RT Protect EDR

Руководство аналитика

Версия 1.0.33 от 30 июня 2026
Разработано компанией АО «РТ-ИБ»

RT Protect

Оглавление

1. Общие положения 8
1.1 Идентификация документа 8
1.2 Аннотация документа 8
1.3 Условные обозначения 9
2. Общие сведения 10
2.1 Общие сведения о Программе 10
2.2 Используемые в графическом интерфейсе иконки 13
3. Описание принципов безопасной работы Программы 24
3.1 Общая информация 24
3.2 Механизмы собственной безопасности агента RT Protect EDR 25
3.3 Компрометация паролей 26
3.4 Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения 26
4. Общие сведения об управлении инцидентами 27
4.1 Общие положения 27
4.2 Действия после возникновения инцидентов 30
4.3 Примеры инцидентов информационной безопасности и их причин 32
4.3.1. Отказ в обслуживании 32
4.3.2. Сбор информации 33
4.3.3. Несанкционированный доступ 35
5. База знаний MITRE ATT&CK 36
5.1 Общие сведения и тактики 36
5.2 Методология анализа киберугроз на основе ATT&CK 41
5.2.1. Идентификация поведения (шаг 1) 41
5.2.2. Получение данных (шаг 2) 42

5.2.3. Создание аналитики (шаг 3) 43
5.2.4. Создание сценария имитации действий злоумышленника (шаг 4) 45
5.2.5. Имитация угрозы (шаг 5) 46
5.2.6. Расследование атаки (шаг 6) 47
5.2.7. Оценка действий (шаг 7) 48
5.3 Вывод по разделу 48
6. Матрица противодействия киберугрозам MITRE D3FEND 50
7. YARA 53
7.1 Общие сведения 53
7.2 Написание YARA-правил 53
7.3 Синтаксис и семантика YARA 55
7.3.1. Комментарии 55
7.3.2. Строки 55
7.3.3. Шестнадцатеричные строки 56
7.3.4. Текстовые строки 58
7.3.5. Строки без учета регистра 59
7.4 Модули YARA, доступные в EDR 60
7.5 Подробнее о правилах 61
8. Общая информация о работе с инцидентами в Программе 62
8.1 Категории аналитиков ИБ 62
8.2 Регистрация инцидентов 62
8.2.1. Алгоритм автоматического создания инцидентов для агентов Linux 63
8.3 Атрибуты инцидентов 63
8.4 Удаление инцидентов 65
9. Модель данных в RT Protect EDR 66
9.1 Общие сведения 66
9.2 События мониторинга сети 80

9.3 События мониторинга файловых операций 83
9.4 События монитора реестра 87
9.5 События журналов 89
9.6 События мониторинга процессов 91
9.7 События мониторинга системы 94
9.8 События пользовательских сессий 95
9.9 События монитора вызовов 97
9.10 События модуля Антишифра 99
9.11 События модуля контроля USB 100
9.12 События статистики 101
9.13 Телеметрия RT Protect EDR 103
10. Ролевая модель 106
10.1 Общая информация 106
10.2 Права, предоставляемые пользователям 107
10.3 Пользователи 113
10.3.1. Изменение параметров учетных записей пользователей 115
10.3.2. Страница профиля пользователя 117
10.3.3. Создание учетной записи пользователя 117
10.3.4. Сброс пароля при входе пользователя в Программу 118
10.3.5. Сообщения пользователю при вводе некорректных значений 118
11. Основные операции в RT Protect EDR 121
11.1 Общая информация 121
11.2 Онлайн-терминал 124
11.2.1. Нативные команды (агенты Windows и Linux) 126
11.2.2. Описание других команд, работающих на агенте Windows (популярные команды интерпретатора и нативные команды) 136
11.2.3. Команды Linux 142
11.3 Операции с профилем пользователя 144

11.4 Расследование инцидентов со страницы «Оповещения» 147
11.5 Работа с деревом процессов 149
11.6 Загрузка и проверка файлов в хранилище 161
11.7 Расследование с «Главной страницы» или страницы «Инциденты» 164
11.7.1. Анализ инцидента 171
11.7.2. PDF-отчет об инцидентах 180
11.7.3. PDF-отчет об инциденте 180
11.8 Принципы работы TI-платформы в RT Protect EDR 181
11.9 Проверка распространенности артефактов TI в агентской сети 186
11.9.1. Ретроспективная проверка артефактов TI 190
11.10 Конфигурирование аналитических правил 192
11.10.1. Индикаторы атак 196
11.10.2. Индикаторы компрометации 233
11.10.3. YARA-правила 245
11.10.4. Журналы 254
11.10.5. Встроенные правила аналитики на агенте 259
11.11 Добавление файлов или программ в список исключений 268
11.11.1. Механизм работы файловых исключений 269
11.11.2. Добавление исключений для файла 275
11.11.3. Исключения для программ 284
11.11.4. Добавление исключений для файла с помощью мастера исключений 296
11.11.5. Добавление исключений для программ в режиме мастера исключений 298
11.12 Добавление сетевых исключений 299
11.12.1. Общая информация 299
11.12.2. Добавление сетевых исключений с помощью мастера исключений 301
11.12.3. Наборы сетевых исключений 301
11.12.4. Страница «Сетевые исключения» 302

11.13 Добавление исключений индикаторов атак 304
11.13.1. Общая информация 304
11.13.2. Наборы исключений индикаторов атак 305
11.13.3. Страница «Исключения индикаторов атак» 306
11.14 Особенности работы Программы с антивирусными средствами сторонних производителей 308
11.14.1. Общая информация 308
11.14.2. Срабатывание антивирусных средств при работе с веб-приложением RT Protect EDR 309
11.14.3. Особенности выполнения действия блокирования для антивирусных решений. 310
11.15 Операции со списком агентов 311
11.16 Операции на странице «Агент» 321
11.16.1. Выполнение операций по реагированию 323
11.16.2. Возврат к нормальному режиму работы после установки агента в режиме «no_driver» 327
11.16.3. Отслеживание изменений состава ПО 328
11.16.4. Настройка конфигураций с наборами 328
11.16.5. Защита на агенте 330
11.16.6. Обновление агента 331
11.16.7. Защита от удаления агента 331
11.16.8. Создание отчета об агенте в формате pdf 332
11.16.9. Просмотр запусков задач для агента 332
11.16.10. Просмотр событий, описывающих состояние агента 333
11.16.11. Просмотр графиков на странице «Агент» 334
11.17 Группы 334
11.18 Конфигурации 335
11.19 Комбинации наборов созданных правил аналитики, исключений и профилей 336
11.20 Уязвимости 337
11.20.1. Формирование отчетности на странице с уязвимостями 341
11.20.2. Распространенность программы с уязвимостью в защищаемой инфраструктуре 342
11.20.3. Изучение сведений об уязвимости 342

11.21 Работа с терминалом (устаревший функционал, оставлен для совместимости с агентами более ранних версий)....346
11.21.1. Общая информация....346
11.21.2. Отправка команд управления на странице «Терминал»....347
11.21.3. Описание команд терминала, реализованных в службе агента....348
11.21.4. Информация в области «Выбор Агента»....358
11.22 Управление задачами....358
11.22.1. Создание сценария....360
11.22.2. Создание задачи....362
11.22.3. Запуск задачи....366
11.23 Реагирование....370
11.23.1. Сценарии реагирования....370
11.23.2. Параметры сценариев реагирования....397
11.24 Просмотр графиков....400
11.24.1. Работа с карточкой графика....401
11.24.2. Ключевые возможности....401
11.24.3. Типичные сценарии....402
11.25 Просмотр файла в разделе Хранилище....402
11.25.1. Создание задач по загрузке архивов....403
11.26 Проактивный поиск угроз....404
11.26.1. Проведение расследований на странице «Активность»....404
11.26.2. Просмотр зашифрованной информации на страницах «Активность», «Инциденты», «Инцидент» и «Процесс»....420
11.26.3. Концепция «Pyramid of Pain»....421
11.27 Обзор событий....422
11.28 Настройка профилей....428
11.28.1. Профиль Антишифра....429

11.28.2. Профили безопасности агента 437
11.28.3. Профили контроля USB 458
11.28.4. Журнал безопасности 464
11.29 Дистрибутивы 469
11.30 Интеграции 470
11.30.1. Интеграция с TI 473
11.30.2. Локальная среда проверки файлов 478
11.30.3. Интеграция с LDAP 478
11.30.4. Интеграция с SIEM (экспорт событий мониторинга) 482
11.30.5. Экспорт событий безопасности 491
11.31 Настройки 494
12. Машинное обучение в Программе 495
12.1 Классификация на сервере 495
12.2 Классификация на агенте 497
12.3 Список компонентов, используемых в модели ИИ 499
13. Создание аналитики на основе MITRE CAR 501
13.1 Общая информация 501
13.2 Пример написания индикатора атаки 501
14. Перечень сокращений 504
15. Перечень терминов и определений 506
16. Заключение 516

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect EDR» Руководство аналитика
Версия документа	Версия 1.0.33 (актуально для версии агента 4.0.0.4000, версии сервера 4.0, фронтенд 3.0.141, бэкенд 1.27.1)
Идентификация программы	RT Protect EDR
Идентификация разработчика	АО «РТ-ИБ»
Уровень доверия	Оценочный уровень доверия 4 (ОУД4) «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772) (с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).)»
Требования по безопасности	«Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла утвержденные приказом ФСТЭК России от 26 февраля 2025 № 58»

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей, осуществляющих функции аналитика (роль с соответствующей группой прав) и взаимодействующих с программой «RT Protect EDR» (далее Программа) с целью обеспечения ИБ.

В документе рассказывается об основных обязанностях аналитика, его возможностях в Программе: основных методах создания аналитических правил, работе с исключениями, профилями Антишифра, безопасности и контроля USB-устройств.

1.3 Условные обозначения

Условные обозначения, применяемые в документе, представлены в таблице 2.

Таблица 2 – Условные обозначения

Обозначение	Описание
ПРОПИСНЫЕ БУКВЫ	Акронимы, аббревиатуры
«Times New Roman»	Названия документов, команд, каталогов, файлов и т.д.
Жирный шрифт	Подписи таблиц, рисунков, названия разделов, подразделов, пунктов и подпунктов, название кнопок меню модуля администрирования Программы
	Обозначения кнопок меню, операций модуля администрирования Программы
Times New Roman/Times New Roman	Перечисление альтернативных вариантов, путь меню, путь файла
 Примечание	Информация, требующая внимания пользователя
 Важно	Информация, связанная с важными конфигурационными настройками и особенностями работы EDR
 Совет	Рекомендации и предположения, которые могут помочь в работе с EDR

2. Общие сведения

2.1 Общие сведения о Программе

RT Protect EDR – это система для обнаружения целенаправленных атак на конечных устройствах. Она обеспечивает быстрое обнаружение вторжений, эффективное автоматическое противодействие, наглядную визуализацию событий и инцидентов, а также сбор цифровых улик и тщательное расследование инцидентов и поиск аномальной активности.

Программа имеет клиент-серверную архитектуру.

Клиентская часть Программы функционирует под управлением ОС согласно следующему списку:

– ОС Windows версий 7 (32 и 64-х битные), 8 (32 и 64-х битные), 8.1 (32 и 64-х битные), 10 (32 и 64-х битные), 11;

– ОС Windows Server 2008 R2, 2012R2, 2012, 2016, 2019, 2022, 2025;

– Различные версии Linux.

Подробная информация о поддерживаемых операционных системах содержится в документе «Руководство администратора RT Protect EDR».

Серверная часть Программы функционирует под управлением ОС Linux (Ubuntu 20.04), а также Astra Linux 1.8.

Обращаться к серверу управления можно в браузерах Google Chrome версии не ниже 92.0.4515.107 и Firefox Browser версии не ниже 83.0.



Примечание

Программа совместима с другими браузерами, однако корректная работа в них не гарантируется. В случае обращения к серверу управления из неподдерживаемого браузера рекомендуется отключать блокировщик рекламы (AdBlock).

Программа предназначена для обработки информации, не являющейся секретной.

Агент спроектирован таким образом, чтобы принимать от сервера правила анализа и другую информацию, необходимую для выявления и реагирования на угрозы. Агент вводит объектную модель и интерфейс взаимодействия с ней по сети.

Посредством интерфейса сервер может передавать на конечные компьютеры правила поведенческого анализа, ставить на контроль различные элементы системы, задавать реакцию на определенные события, а также получать статистику системной активности хоста, собирать, обобщать и при необходимости предоставлять аналитику возможность динамически ее отслеживать.

Технически клиент представляет собой программное средство, устанавливаемое на компьютере конечного пользователя с целью выявления и борьбы с вредоносным ПО и возможными атаками на этот компьютер или инфраструктуру, частью которой он является.

Клиент проводит мониторинг системной активности, чтобы выявлять вредоносное поведение согласно правилам, полученным от сервера поведенческого анализа. Клиент собирает статистику системной активности и периодически отправляет ее на сервер.



Примечание

Все события, регистрируемые на агенте, сохраняются на компьютере, на котором агент установлен и передаются по зашифрованному каналу на сервер в порядке очереди. Если происходит отключение компьютера от сети, то события накапливаются до момента возобновления соединения или до момента переполнения кольцевого буфера, в виде которого организовано хранение событий, где события более старые перезаписываются более новыми при превышении размера буфера. Размер этого буфера составляет до 1 гигабайта памяти и 16 Мб для лог-файлов (по 8 на службу и драйвер). Данные при оптимальной настройке агента, когда количество событий, поступающих от агента в секунду (EPS), равно единице, хранятся до 7 дней отсутствия соединения с сервером. Чем больше eps, тем на меньшее время хватит диска для хранения, поскольку выделенный фиксированный объем будет заполнен быстрее.

При передаче данных используется протокол HTTPS, работающий через шифрованный транспортный механизм TLS. Он обеспечивает защиту от атак, основанных на прослушивании сетевых соединений.

Программа имеет многофункциональный пользовательский интерфейс и предназначена в большей мере для аналитиков и администраторов безопасности.

Программа обеспечивает следующие функции:

– возможность обнаруживать аномалии в работе ОС посредством инструментария индикаторов атак, индикаторов компрометации и других аналитических инструментов;

– предотвращение действий вирусов-шифровальщиков с помощью модуля Антишифр;

– гибкая настройка функций безопасности агента;

– управление USB-устройствами (создание белых и черных списков устройств, ограничение функций устройств, формирование инцидентов на основе заданных событий и т.д.)

– возможность собирать информацию о работе различных подсистем ОС (сетевая, файловая, реестр и т.д.);

– возможность выполнять анализ собранных Программой данных в режиме, близком к реальному масштабу времени;

– обнаружение и предотвращение действия нарушителей в режиме, близком к реальному масштабу времени, на уровне отдельных узлов;

– возможность выполнять анализ собранных данных с целью обнаружения компьютерных вторжений с использованием сигнатурных и эвристических методов;

– возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий файловой активности;

– создание инцидентов на основе событий, поступающих от мониторов активности;

– уведомление пользователей Программы об обнаруженных вторжениях и нарушениях безопасности с помощью отображения соответствующего сообщения;

– автоматизированное обновление базы решающих правил;

– наличие интерфейса администрирования;

– генерация записей аудита для событий, потенциально подвергаемых аудиту;

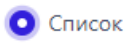
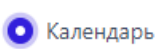
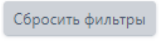
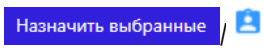
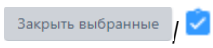
– ограничение доступа к чтению записей аудита;

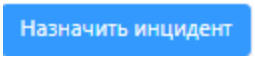
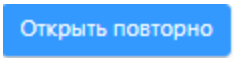
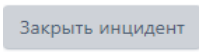
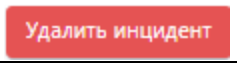
– поиск, сортировка, упорядочение данных аудита.

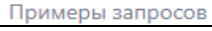
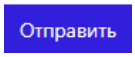
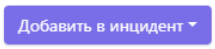
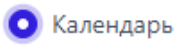
2.2 Используемые в графическом интерфейсе иконки

В таблице 3 представлено значение стандартных иконок, используемых в графическом интерфейсе Программы.

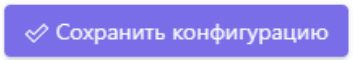
Таблица 3 – Используемые иконки и их назначение

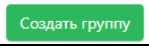
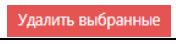
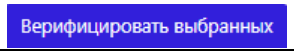
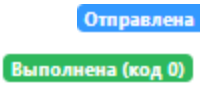
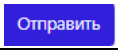
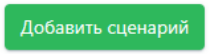
Иконка	Назначение
Иконки верхней панели административного модуля управления на сервере	
	Свернуть/раскрыть боковую панель
	Назначить темную тему оформления страницы
	Назначить светлую тему оформления страницы
	Раскрыть цепочку перехода от главной до открытой страницы
	Перейти на страницу Оповещения
	Перейти на страницу Профиль пользователя (открывается при нажатии ЛКМ на имени профиля)
	Выйти из профиля пользователя (открывается при нажатии ЛКМ на имени профиля)
Иконки страницы «Оповещения»	
	Прочитать выбранные оповещения
	Прочитать все оповещения
	Выбрать оповещение
	Отметить оповещение как прочитанное
Иконки страницы «Пользователи»	
	Заблокировать/разблокировать пользователя
	LDAP-пользователи
Иконки страницы «Инциденты»	
	Выбрать/отменить режим **Список** в настройке периода регистрации инцидента
	Выбрать/отменить режим **Календарь** в настройке периода регистрации инцидента
	Показать графики по динамике инцидентов
	Сбросить все фильтры на странице
	Назначить ответственного за решение выбранного инцидента/назначить инцидент (открыть повторно)
	Закрыть выбранные инциденты

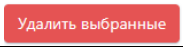
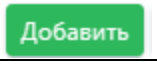
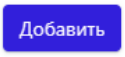
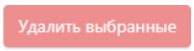
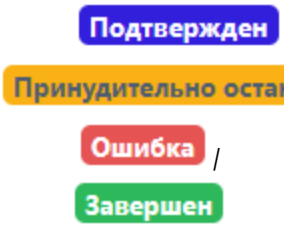
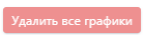
	Выбрать инцидент
	Индикатор активности агента
	Индикатор, сигнализирующий о том, что обнаруженное событие было заблокировано/разрешено
	Индикатор, сообщающий о том, что детектируемое событие является обнаружением (событие с уровнем критичности от среднего и выше)
Иконки страницы «Инцидент»	
	Сохранить файл с отчетом в формате pdf
	Раскрыть дополнительную информацию о событии
	Выбрать событие в инциденте
	Назначить ответственного за решение выбранного инцидента
	Сохранить изменения после редактирования инцидента
	Открыть инцидент повторно (активна, если инцидент закрыт)
	Закрыть инцидент (кнопка активна для новых и назначенных инцидентов)
	Удалить инцидент
	Создание комментария к инциденту
	Кнопки редактирования комментариев
	Индикатор, показывающий критичность события
	Индикатор, сигнализирующий о том, что обнаруженное событие было заблокировано/разрешено
	Создать исключение с помощью мастера исключений
	Исключить выбранные события из инцидента
	Набор по умолчанию
	Индикатор атак
	Иконка показывающая что при создании события артефакт не проверялся TI платформой
	Иконка показывающая что данное событие является онаружением
	Копирование информации в буфер обмена
	Отображение информации в формате JSON

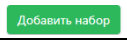
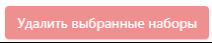
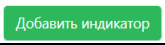
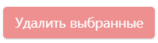
Иконки страницы «Активность»	
	Сбросить значения всех фильтров на странице
	Показать примеры запросов на языке DSL
	Отправить DSL-запрос
	Добавить событие в инцидент
	Выбрать/отменить режим Список в настройке периода регистрации события на сервере
	Выбрать/отменить режим Календарь в настройке периода регистрации события на сервере
	Иконка с предупреждением о том, что DSL-запрос желательно изменить для уменьшения нагрузки на поисковую систему базы данных
	Показать/скрыть график распределения событий
	Раскрыть дополнительную информацию о событии
	Выбрать событие
	Загрузка файла с агента в файловое хранилище сервера
	Копировать в буфер обмена
	Перейти на страницу Процессы и модули для выбранного хеша
	Копирование информации в буфер обмена
	Индикатор, сигнализирующий о том, что обнаруженное событие было заблокировано/разрешено
	Иконка сигнализирующая о том, что вердикт TI – платформы по отношению к артефакту изменился
Иконки страницы «Артефакты TI»	
	Копировать в буфер обмена
	Наборы индикаторов компрометации
	Наборы сетевых исключений
	Наборы исключений для файлов
	Просмотр событий в активности (элемент не присутствует/ присутствует) в событиях активности

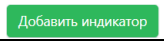
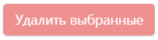
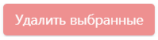
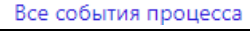
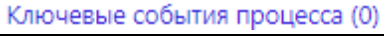
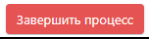
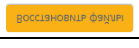
Отправить	Отправить DSL-запрос
Иконки страницы «Агенты»	
Отправить	Отправить DSL-запрос
	Устаревший функционал
	Иконка с предупреждением о том, что DSL-запрос желательно изменить для уменьшения нагрузки на поисковую систему базы данных
	Раскрыть дополнительную информацию об агенте
	Выбрать агента
	Иконка, сигнализирующая о том, что агент функционирует в режиме NO_DRIVER (не работают защитные функции и нет возможности перевести машину с агентом в изоляцию)
	Иконка, информирующая об операционной системе, на которой установлен агент
Активен / Не активен / Защита отключена / Изолирован / Автообновление отключено	Иконки, сообщающие о функциональных состояниях агента
	Открыть терминал для отправки команды выбранному агенту
Добавить в группу	Добавить выбранного агента в группу
	Применить настройки конфигурации
	Исключить выбранного агента из группы
	Удалить выбранного агента
Открытых инцидентов: 3	Перейти на страницу с инцидентами, зарегистрированными на агенте
CSV	Скачать список с информацией об агентах в формате CSV
Сбросить фильтры	Сбросить все фильтры, выставленные на странице Агенты
	Применить конфигурацию
	Изолировать выбранных агентов
	Отменить изоляцию выбранных агентов
	Включить автоматическое обновление выбранных агентов
	Отключить автоматическое обновление выбранных агентов
	Включить защиту на выбранных агентах
	Выключить защиту на выбранных агентах

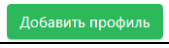
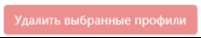
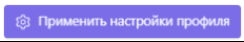
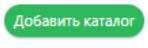
	Зафиксировать состояние ПО выбранных агентов в качестве золотого образа
	Отключить отслеживание соответствия состава ПО выбранных агентов в качестве золотого образа
	Включить защиту от удаления агента
	Отключить защиту от удаления агента
	Выполнить команду на выбранных агентах
	Реагирование для выбранных агентов
	Состав ПО на агенте соответствует составу золотого образа
	Имеются отличия в составе ПО на агенте и золотом образе
	Защита от удаления на агенте включена
	В работе агента имеются проблемы
Иконки страницы «Агент»	
	Сохранить изменения в имени агента
	Иконка состояния агента (активен /не активен)
	Скопировать идентификатор агента в буфер обмена
	Перейти к уязвимостям, найденным на агенте
	Кнопка удаления агента (после удаления агент попадает на верификацию, физически с машина)
	Применить конфигурацию набора или профиля для агента
	Сохранить конфигурацию наборов или профилей для агента
	Переход на страницу наборов или на страницу профилей
	Обновить информацию об установленном ПО на агенте
	Зафиксировать отслеживание золотого образа для агента
	Изменить пароль для удаления агентов при включенной защите от удаления
	Показать пароль для удаления агентов при включенной защите от удаления
	Скопировать в буфер обмена пароль для удаления агентов при включенной защите от удаления
	Раскрыть страницу с графикой отображающей состояние агента (Загрузка ЦП, использование памяти)
	Перейти к набору или профилю агента

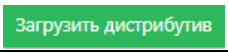
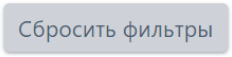
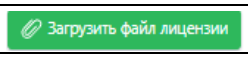
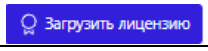
	Перейти к несохраненному набору или профилю агента
	Открыть консоль управления агентом
	Исключить агента из группы
	Изолировать агента/отменить изоляцию агента
	Включить/Выключить функции защиты; Включить/выключить автоматическое обновление агента
	Перейти на страницу зарегистрированных событий агента
	Перейти на страницу зарегистрированных инцидентов агента
	Скачать (краткий/полный) отчет об агенте в формате PDF
Иконки страницы «Группы агентов»	
	Раскрыть состав группы
	Выбрать группу
	Редактировать название группы
	Создать новую группу агентов
	Удалить выбранные группы агентов
Иконки страницы «Конфигурации»	
	Редактировать конфигурацию
	Удалить конфигурацию
	Иконка сигнализирующая что конфигурация является не полной и заданы не все настройки для наборов и профилей
	Создание конфигурации
Иконки страницы «Верификация Агентов»	
	Раскрыть дополнительную информацию о верифицируемом агенте
	Выбрать агента
	Выполнить верификацию выбранных агентов
Иконки страницы «Терминал»	
	Отображение стадии выполнения команды терминала
	Флаг сортировки для выбора только активных агентов
	Прервать выполнение команды
	Отправить команду на исполнение
Иконки страницы «Планировщик задач» вкладка «Сценарии»	
	Добавить сценарий

	Включить выбранные сценарии
	Выключить выбранные сценарии
	Удалить выбранные сценарии
 /	Выключить /Включить сценарий
	Редактировать сценарий
	Удалить сценарий
	Добавить действие при создании сценария
	Выбрать действие для удаления
	Добавить созданный сценарий в список сценариев
Иконки страницы «Планировщик задач» вкладка «Задачи»	
	Задача не будет запущена, т.к. сценарий выключен
	Добавление задачи
	Запустить выбранные задачи
	Включить выбранные задачи
	Выключить выбранные задачи
	Удалить выбранные задачи
	Запустить задачу
	Редактировать задачу
	Удалить задачу
Иконки страницы «Планировщик задач» вкладка «Запуски»	
	Статус запуска
	Завершить выполнение запуска
	Завершить выполнение запуска невозможно
Иконки страницы «Графики»	
	Выбор ширины графика (50% или 100%)
	Флаг сортировки для выбора только активных агентов
	Добавить графики
	Удалить все графики

Иконки страницы «Хранилище»	
	Раскрыть дополнительную информацию о загруженном в хранилище файле
	Выбрать файл
	Скопировать информацию в буфер обмена
	Ссылка на страницу Процессы и модули для выбранного файла
	Открыть отчет TI-платформы (файл является безопасным)
	Открыть отчет TI-платформы (файл неизвестный, не удалось найти информацию о том, является файл безопасным или нет)
	Открыть отчет TI-платформы (информация о файле на платформе отсутствует или не проверялась
	Открыть отчет TI-платформы (файл отмечен платформой как вредоносный)
	Открыть отчет TI-платформы (анализ файла платформой выполняется в текущий момент)
	Просмотреть файл в программе просмотра файлов (в кодировке UTF-8 или в бинарном виде)
	Удалить файл
	Удалить выбранные файлы из хранилища
	Получить ссылку для скачивания файла на машину, с которой осуществляется доступ в модуль администрирования
	Загрузить файл с машины, с которой осуществляется доступ в модуль администрирования
Иконки страницы «Наборы YARA-правил», «Наборы исключений для файлов», «Наборы исключений для программ», «Наборы журналов»	
	Добавить новый набор индикаторов
	Передать все профили агентам
	Удалить выбранные наборы индикаторов
	Не все профили были применены
	Редактировать набор
	Удалить набор индикаторов
	Передать профиль
Иконки страницы «Индикаторы компрометации»	
	Добавить индикатор
	Удалить выбранные индикаторы
	Редактировать индикатор
	Удалить индикатор
	Копировать выбранные элементы в другой набор

	Экспортировать набор в файл
	Импортировать файлы из файла в набор
	Кнопка активации/деактивации правила
	Активировать выбранные элементы
	Деактивировать выбранные элементы
	Скопировать в буфер обмена
	Ссылка на процессы и модули
Иконки страницы «Индикаторы атак»	
	Добавить индикатор
	Удалить выбранные индикаторы
	Редактировать индикатор
	Удалить индикатор
	Копировать выбранные элементы в другой набор
	Экспортировать набор в файл
	Импортировать файлы из файла в набор
	Кнопка активации/деактивации правила
	Перейти на страницу базы знаний MITRE ATT&CK, связанную с индикатором
	Активировать выбранные элементы
	Деактивировать выбранные элементы
Иконки страницы «YARA-правила», «Исключения для файлов», «Исключения для программ», «Журналы»	
	Добавить правило
	Удалить выбранные правила
	Редактировать правило
	Удалить правило
	Копировать выбранные элементы в другой набор
	Экспортировать набор в файл
	Импортировать файлы из файла в набор
	Кнопка активации/деактивации правила
	Быстрый просмотр YARA-правил
Иконки страницы «Процесс»	
	Показать все события процесса
	Показать ключевые события процесса
	Изменить ориентацию дерева процессов
	Убрать информацию о процессе (оставить только дерево процессов)
	Загрузить в область отображения дополнительное количество процессов
	Кнопка «Завершить процесс»
	Кнопка «Восстановить файлы»

	Скопировать данные в буфер обмена
	Загрузить файл в файловое хранилище
	Ссылка на процессы и модули
Общие иконки для поиска и навигации по страницам	
	Выбрать количество отображаемых элементов на странице
	Переместиться на первую страницу списка
	Переместиться на последнюю страницу списка
	Текущая страница списка
	Переместиться на предыдущую страницу списка
	Переместиться на последующую страницу списка
	Номер страницы списка
	Перемещение при горизонтальной прокрутке вправо
	Перемещение при горизонтальной прокрутке влево
	Перемещение при вертикальной прокрутке вверх
	Перемещение при вертикальной прокрутке вниз
	Раскрыть окно краткой информации об элементе
	Скрыть окно краткой информации об элементе
	Сортировать информацию в столбце по убыванию
	Сортировать информацию в столбце по возрастанию
	Удалить параметра фильтрации в поле
Иконки страницы «Профили Антишифра» и «Профили безопасности агента»	
	Профиль не сохранен
	Редактировать профиль
	Удалить профиль
	Передать профиль
	Передать все профили агентам
	Добавить профиль
	Удалить выбранные профили
	Выбрать/отменить выбор строки с названием профиля защиты
Иконки страницы «Профиль Антишифра» и «Профиль безопасности агента»	
	Отключить/включить модуль Антишифра Отключить/включить резервирование
	Применить настройки профиля
	Добавить каталог

	Удалить каталог
	Экспортировать профиль в файл
	Импортировать данные из файла в профиль
	Просмотреть поддерживаемые типы данных для резервирования
	Удалить тип файла из списка для резервирования
	Передать профиль агентам
Иконки страницы «Дистрибутивы»	
	Скачать дистрибутив с сервера управления
	Удалить дистрибутив с сервера управления
	Загрузить дистрибутив на сервер управления
	Сбросить все фильтры выставленные на странице
Иконки страницы «Лицензия»	
	Кнопка загрузки файла лицензии
	Кнопка загрузки лицензии в формате строки

3. Описание принципов безопасной работы Программы

3.1 Общая информация

При использовании Программы должны выполняться следующие меры по защите от несанкционированного доступа к информации:

1) Необходимо соблюдать парольную политику;

2) Пароль не должен включать в себя легко вычисляемые сочетания символов;

3) Личный пароль пользователь не имеет права сообщать никому;

4) При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами;

5) Пароль должен соответствовать следующим требованиям:

– пароль не должен совпадать с именем пользователя или другой персональной информацией или быть слишком похожим на неё;

– пароль должен содержать как минимум 12 символов;

– пароль не может быть одним из широко распространённых паролей;

– пароль не должен состоять только из цифр.



Важно

Если пользователь с ролью **Аналитик** выполнит 4 или более неудачные попытки входа в течение 5 минут, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет администратор Программы или учетная запись будет разблокирована автоматически после завершения временного периода, равного 24 часам.

При эксплуатации Программы запрещено:

– оставлять без контроля незаблокированные программные средства;

– разглашать пароли, выводить пароли на дисплей, принтер или иные средства отображения информации.

Эксплуатация Программы должна осуществляться пользователями, прошедшими проверку на благонадежность и компетентность.

Пользователи Программы должны действовать согласно правилам и процедурам, установленным в настоящем руководстве и внутренних документах организаций, эксплуатирующих Программу.

3.2 Механизмы собственной безопасности агента RT Protect EDR

В агенте RT Protect EDR реализованы следующие механизмы собственной безопасности:

– обязательное наличие привилегий администратора системы для любых штатных действий с агентом (удаление, обновление и т.п.);

– защита файлов и ключей реестра (для ОС Windows), относящихся к агенту;

– парольная защита от удаления агента, управляемая со стороны сервера EDR;

– защита от остановки службы и уничтожения прикладных процессов агента, как штатно, так и посредством известных анти-EDR утилит (backstab и др.);

– контроль целостности кода агента в памяти;

– защита от несанкционированного доступа к функциям компонента ядра агента;

– контроль целостности точек встраивания агента в ОС (и их восстановление при нарушении);

– ограничение межпроцессного взаимодействия с компонентами агента;

– контроль сетевого взаимодействия из прикладных компонентов агента;

– контроль дочерних процессов прикладных компонентов агента;

– контроль модулей, загружаемых в прикладные компоненты агента;

– защита от внедрения стороннего кода в прикладные компоненты агента;

– передача на сервер EDR актуального состояния агента, а также зафиксированных попыток нарушения его работоспособности и выявленных отклонений от штатного функционирования.

По мере развития системы защитные свойства агента RT Protect EDR также совершенствуются, исходя из актуальных угроз. Регулярно проводятся испытания актуальных анти-EDR-решений против агента RT Protect EDR, результатом которых является соответствующее совершенствование защитных механизмов агента.

3.3 Компрометация паролей

Под компрометацией паролей следует понимать следующее:

– физическую утерю носителя с парольной информацией;

– передачу идентификационной информации по открытым каналам связи;

– перехват пароля при распределении идентификаторов;

– сознательную передачу информации постороннему лицу.

При компрометации пароля пользователь обязан незамедлительно оповестить администратора Программы.

3.4 Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения

Настройки (параметры) безопасности доступны только пользователям с ролью **Администратор** и заключаются в возможности управления пользователями Программы.

Пользователям назначаются права и привилегии, необходимые для выполнения ими своих должностных обязанностей (функций).

4. Общие сведения об управлении инцидентами

4.1 Общие положения

Управление инцидентами информационной безопасности (ИБ) обеспечивается в соответствии с ГОСТ Р 59710–2022, ГОСТ Р 59711–2022 и ГОСТ Р 59712–2022.

Под инцидентом ИБ подразумевается непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могло привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации.

Управление инцидентами включает в себя следующие стадии:

– организация деятельности по управлению компьютерными инцидентами;

– обнаружение и регистрация компьютерных инцидентов;

– реагирование на компьютерные инциденты;

– анализ результатов деятельности по управлению компьютерными инцидентами.

Каждый из представленных выше этапов может быть разбит на отдельные подэтапы.

Обнаружение инцидентов ИБ осуществляется в режиме 24x7 за счет выявления событий ИБ или подозрительной активности служб и систем, приложений, программ и оборудования, контролируемых аналитиками.

В качестве событий ИБ и/или подозрительной активности могут рассматриваться, в том числе следующие события:

– уязвимости в системном и/или прикладном ПО;

– трудности и проблемы при работе с ресурсами ИС (нештатное функционирование программных и аппаратных средств ИС, нарушение целостности информации и т.п.).

Основными видами инцидентов ИБ являются:

1) Разглашение конфиденциальной информации, либо угроза такого разглашения;

2) Несанкционированный доступ к конфиденциальной информации со стороны лиц, которые не имеют легального доступа к ресурсам организации;

3) Несанкционированный доступ к ресурсам ИТ-инфраструктуры;

4) Компрометация учетных записей или паролей;

5) Вирусная атака или вирусное заражение;

6) Нарушение или сбой в работе системы резервного копирования.

Аналитик после получения информации о предполагаемом инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных, а также проверку наличия в выявленном событии свидетельств, указывающих на вредоносную активность. Если событие не является инцидентом, аналитик может закрыть его, добавив соответствующий комментарий.

Инциденты информационной безопасности классифицируются согласно таблице 4.

Таблица 4 – Классификация инцидентов ИБ

Типы событий и инцидентов ИБ	Описание	Ответственный за разрешение инцидента
Программно-технические	События и инциденты, связанные с работой программных и аппаратных средств, участвующих в бизнес-процессах, а также связанные с работой средств защиты информации. Программно-технические инциденты в качестве подтипов включают: — несанкционированные подключения и несанкционированный доступ к ресурсам; — атаки из внешних сетей; — вирусные атаки; — неавторизованное использование ресурсов.	Аналитик
Связанные с конфиденциальной информацией	События и инциденты, связанные с несанкционированным доступом или подозрением на доступ к конфиденциальной информации и компрометацией таких данных (или АС, содержащей данные)	Аналитик Администратор

Если инцидент создается аналитиком вручную, то после определения типа инцидента аналитик должен определить его критичность по шкале, приведенной в таблице 5, исходя из следующих сведений:

– информации об инциденте;

– критичности активов, вовлеченных в инцидент;

– прогнозируемой степени влияния инцидента на ключевые свойства активов.

Таблица 5 – Критичность инцидента ИБ

Значение	Качественное значение	Описание
5	Критичный	Инцидент, указывающий на событие, связанное с тем, что система была успешно атакована, затронуты критичные ресурсы. Это может привести к системной компрометации или раскрытию очень важной информации, нарушению работы критических серверов, приводящих к недоступности сервисов и полному непредоставлению услуг. В этом случае планируются и реализуются корректирующие действия.
4	Высокий	Инцидент указывает на событие, последствия которого могут привести к компрометации данных системы. Указанный инцидент должен быть исследован, по нему оперативно принимаются меры, с целью уменьшения риска и снижения вероятности проведения успешной атаки. В этом случае планируются и реализуются корректирующие действия.
3	Средний	Инцидент потенциально может привести к системной компрометации. Возможно применение компенсирующих мер.
2	Низкий	Инцидент символизирует собой низкий риск или предупреждение. В этом случае знание некоторых конфигураций может быть интересным и может потенциально привести к компрометации данных системы. Компенсирующих мер в большинстве случаев не требуется. Риск может быть принят.
1	Информация	Инцидент, связанный с событием, представляющим интерес к системе, но не представляющим угрозу безопасности системы. К ним относятся, как правило, события информационного характера. Компенсирующих мер не требуется. Риск принимается.

Основные цели реагирования на инциденты:

– защитить законные права компании-заказчика или потребителя услуг, предоставляемых производителем Программы;

– минимизировать нарушения порядка работы и повреждения данных информационных и телекоммуникационных систем компании-заказчика или потребителя услуг, предоставляемых производителем Программы;

– восстановить в кратчайшие сроки работоспособность систем компании при нарушении работоспособности в результате инцидента;

– минимизировать последствия нарушения конфиденциальности, целостности и доступности информации в ИС;

– координация реагирования на инцидент;

– подтверждение/опровержение факта возникновения инцидента ИБ;

– быстрое обнаружение и/или предупреждение подобных инцидентов в будущем;

– обеспечить сохранность и целостность доказательств возникновения инцидента;

– создать условия для накопления и хранения точной информации об имевших место инцидентах ИБ, о полезных рекомендациях;

– обучить персонал компании-заказчика или потребителя услуг, предоставляемых производителем Программы, действиям по обнаружению, устранению последствий и предотвращению инцидентов ИБ.

4.2 Действия после возникновения инцидентов

На рисунке 1 представлен примерный порядок реагирования на инцидент информационной безопасности.



Рисунок 1 – Порядок реагирования на инциденты ИБ

План реагирования на инциденты должен содержать пошаговые инструкции к действиям, выполняемым на стадиях обнаружения и регистрации инцидента, а также реагирования на него.

Примерный список действий аналитика применительно к обнаруженному инциденту в системе RT Protect EDR:

– получение первоначальной сводной информации об инциденте: командные строки, артефакты (имена файлов, хеши и доменные имена), сработавшие правила и др. (страница **Инцидент**);

– сетевая изоляция (network containment) хоста (страница **Агент** или **Агенты**);

– завершение процесса (команда в терминале реагирования или кнопка реагирования **Завершить процесс** в дереве процессов на странице **Процесс**);

– загрузка файла или файлов, связанных с инцидентом, в хранилище файлов для последующего изучения (команда в терминале реагирования, кнопка реагирования **Загрузить файл в Хранилище**) рядом с именем файла, раздел **Хранилище**);

– проверка артефактов средствами TI-платформы (производится автоматически или по клику на артефакте);

– формирование правила (в разделах **Индикаторы компрометации**, **Индикаторы атак**, **Исключения для файлов**, **Сетевые исключения**) для последующего предотвращения запуска вредоносного файла или доступа к вредоносному ресурсу;

– формирование исключения в случае ложноположительного срабатывания (вручную в разделе Исключения или с помощью **Мастера создания исключений**);

– ликвидация последствий вредоносной активности – завершение процессов, откат изменений, удаление вредоносных файлов, элементов автозапуска, ключей в реестре (для Windows) и т.п. (терминал реагирования);

– импорт индикаторов компрометации из доверенных источников/от регулирующих органов (раздел Индикаторы компрометации);

– проверка инфраструктуры в реальном времени и сбор триажа (первичная оценка и классификация данных в рамках расследования) с помощью специализированных инструментов (например, RT Retro), посредством команд в терминале реагирования;

– поиск (в том числе ретроспективный) аналогичных событий на других хостах (строка DSL на страницах **Агенты**, **Активность**);

– закрытие инцидента и вывод хоста из сетевой изоляции.

4.3 Примеры инцидентов информационной безопасности и их причин

Инциденты ИБ могут быть преднамеренными или случайными и вызваны как техническими, так и нетехническими средствами.

Их последствиями могут быть такие события, как несанкционированное раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение.

Инциденты ИБ, о которых не было сообщено, но которые были определены как инциденты, расследовать невозможно, и защитных мер для предотвращения повторного появления этих инцидентов применить нельзя.

Ниже приведены некоторые примеры инцидентов ИБ и их причин.

4.3.1. Отказ в обслуживании

Отказ в обслуживании является обширной категорией инцидентов ИБ, имеющих одну общую черту. Подобные инциденты ИБ приводят к неспособности систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

Существует два основных типа инцидентов ИБ, связанных с отказом в обслуживании, создаваемых техническими средствами:

– уничтожение ресурсов;

– истощение ресурсов.

Некоторыми типичными примерами таких преднамеренных технических инцидентов ИБ как отказ в обслуживании являются:

1) Зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

2) Передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;

3) Одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы (замедление их работы, блокирование или разрушение).

Технические инциденты ИБ отказа в обслуживании могут возникать случайно, например, в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения, или преднамеренно, в результате целенаправленной атаки или попадания вредоносной программы в периметр ИС.

Некоторые наиболее распространенные методы скрытого сканирования и идентификации могут приводить к полному разрушению старых или ошибочно сконфигурированных систем или сервисов при их сканировании.

Следует заметить, что многие преднамеренные технические инциденты типа «Отказ в обслуживании» часто инициируются анонимно (источник атаки неизвестен), поскольку злоумышленник обычно не получает информации об атакуемой сети или системе.

4.3.2. Сбор информации

В общих чертах инциденты ИБ «Сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки.

Подобные инциденты ИБ предполагают разведку с целью определения следующей информации:

– наличие цели, получение представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана обменом информации;

– потенциальные уязвимости, которые можно использовать для атаки цели или окружающей ее сетевой среды.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

1) Сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);

2) Отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

3) Зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;

4) Сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например, электронная почта, протокол FTP, сеть и т.д.) и версий программного обеспечения этих сервисов;

5) Сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

В некоторых случаях технический сбор информации расширяется и переходит в несанкционированный доступ, например, если злоумышленник при поиске уязвимости пытается получить несанкционированный доступ.

Обычно это осуществляется автоматизированными средствами взлома, которые не только производят поиск уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

Инциденты, направленные на сбор информации и создаваемые нетехническими средствами, приводят к следующим последствиям:

– прямому или косвенному раскрытию или модификации информации;

– хищению интеллектуальной собственности, хранимой в электронной форме;

– нарушению учетности, например, при регистрации учетных записей;

– неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться следующими факторами:

1) Нарушения физической защиты безопасности, приводящие к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимую информацию, например, ключи шифрования;

2) Неудачно и (или) неправильно конфигурированные операционные системы по причине неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения, что приводит к получению доступа к информации лицами, не имеющими на это разрешения.

4.3.3. Несанкционированный доступ

«Несанкционированный доступ» как тип инцидента включает в себя инциденты, не вошедшие в первые два типа. Этот тип инцидентов состоит из несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети.

Некоторые примеры несанкционированного доступа с помощью технических средств включают в себя:

1) Попытки извлечь файлы с паролями;

2) Атаки переполнения буфера для получения привилегированного доступа к сети (например, на уровне системного администратора);

3) Использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;

4) Попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя или администратора.

Инциденты несанкционированного доступа, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию, или модификации информации, нарушениям учетности или неправильному использованию информационных систем, могут вызываться следующими факторами:

– разрушением устройств физической защиты с последующим несанкционированным доступом к информации;

– неудачной и (или) неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения.

5. База знаний MITRE ATT&CK

5.1 Общие сведения и тактики

Общепризнанной методологией в плане определения возможных действий нарушителя в сфере информационной безопасности является MITRE ATT&CK. Матрица MITRE предоставляет доступ к большому количеству известных тактик, техник и процедур (TTP), с помощью которых злоумышленники могут проводить атаки.

MITRE ATT&CK – это еще и сервис, предоставляющий возможность обмена данными о киберугрозах и средствах защиты, глобально доступная база знаний не только о тактиках и техниках атак на компьютерные системы, но и о технических средствах, с помощью которых злоумышленники могут атаковать ИТ-инфраструктуру, а также о самих злоумышленниках, их группировках и объединениях.

Компания MITRE предоставляет информацию о предпочтительных методах противодействия злоумышленникам как в рамках методологии MITRE ATT&CK, так и в рамках созданной методологии MITRE D3FEND (см. раздел 6).

База знаний ATT&CK используется в качестве основы для разработки конкретных моделей угроз и методологий в частном секторе, в правительстве, а также в сообществе продуктов и услуг кибербезопасности.

ATT&CK открыта и доступна любому физическому лицу или организации для бесплатной работы.

Модель может быть использована, чтобы охарактеризовать враждебное поведение с целью выявить общие черты среди известных атак и деятельности по вторжению в отдельные узлы или комбинации действий, которые злоумышленник может предпринять, чтобы достичь своих целей.

Тактики, техники и процедуры, описанные в ATT&CK, были выбраны на основе наблюдаемых APT-вторжений из публичных источников и включены в модель на необходимом уровне абстракции для определения эффективных мер защиты и поиска соответствий с существующими методами вторжений. Тактики представляют собой высший уровень абстракции в рамках модели ATT&CK.

Тактики – это цели, которые ставит противник в ходе проникновения, то есть тактика показывает, как злоумышленник действует на разных этапах своей операции, каковы цель или задача злоумышленника на определенном шаге. Например, TA0002 Execution – это тактика злоумышленника, который пытается запустить вредоносный код на атакуемой машине.

Техника – это то, как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, технологии, код, эксплойты, утилиты и т. д. В качестве примера можно рассмотреть T1059.001 PowerShell – использование PowerShell при атаке.

Процедура – это то, как техника выполняется и для чего. Например, вредоносная программа, используя PowerShell, скачивает загрузчик, который, в свою очередь, загружает фреймворк Cobalt Strike для попытки запуска на удаленных хостах. В этот момент происходит объединение техники и тактики.

Ниже перечислены тактики MITRE ATT&CK для корпоративных систем, с которыми чаще всего сталкиваются аналитики ИБ в корпоративных структурах:

1) «Разведка» (Reconnaisense);
2) «Сбор ресурсов» (Resource Development);
3) «Первоначальный доступ» (Initial Access);
4) «Выполнение» (Execution);
5) «Закрепление» (Persistence);
6) «Повышение привилегий» (Privilege Escalation);
7) «Уклонение от защиты» (Defense Evasion);
8) «Доступ к учетным данным» (Credential Access);
9) «Исследование» (Discovery);
10) «Перемещение внутри периметра» (Lateral Movement);
11) «Сбор» (Collection);
12) «Управление и контроль» (Command and Control);
13) «Эксфильтрация» (Exfiltration);
14) «Воздействие» (Impact).

«Разведка» – целью тактики является сбор злоумышленником информации, которую возможно использовать при проведении дальнейших вредоносных атак. Информация может включать в себя детали об управлении, инфраструктуре или личную информацию о персонале атакуемой организации. Подобные детали могут быть использованы в других фазах жизненного цикла атаки, к примеру, при получении первоначального доступа или для продвижения в фазе разведки.

«Сбор ресурсов» – целью тактики является сбор злоумышленниками ресурсов, которые могут быть использованы при проведении атак. Под ресурсами здесь понимаются элементы инфраструктуры, учетные записи или компьютерные мощности жертвы. Эти ресурсы могут быть использованы злоумышленниками при развитии атаки в других фазах ее жизненного цикла, например, использование купленного домена для поддержки тактики «Управление и контроль» или использование почтовых аккаунтов для фишинга как часть тактики «Первоначальный доступ».

«Первоначальный доступ» – целью тактики является проникновение злоумышленника в сетевой контур жертвы для создания точки входа внутри контура, чтобы в дальнейшем расширить присутствие, получив доступ к дополнительным учетным данным или службам удаленного доступа.

«Выполнение» – целью тактики является запуск злоумышленником вредоносного кода на локальной или удаленной системе. Часто техники, с помощью которых запускается вредоносный код, группируются с техниками из других тактик, чтобы достичь большего, например, исследования сети или кражи данных.

Для наглядности можно привести такой пример: злоумышленник использует утилиту удаленного доступа, чтобы запустить Powershell-скрипт, который обнаруживает удаленные системы.

«Закрепление» – целью тактики является сохранение точки для развития атаки, под этим подразумевается любой доступ, действие или изменение конфигурации системы, которое дает злоумышленнику постоянное присутствие в этой системе. Злоумышленникам часто необходимо поддерживать доступ к системе из-за прерываний: перезапуск системы, потеря учетных данных или другие сбои. В качестве примеров можно привести замену или воровство легального кода или добавление кода, автоматически загружаемого при перезапуске системы.

«Повышение привилегий» – целью тактики является повышение злоумышленником уровня разрешений в атакуемой системе или сетевой инфраструктуре. Обычным для тактики является использование уязвимостей, ошибок в конфигурациях и слабостей системы.

Примеры повышения привилегий:

– уровень System/root;

– локальный администратор;

– учетная запись пользователя с доступом как у администратора;

– учетная запись пользователя с доступом к специализированной системе или пользователя, выполняющего определенные специфичные функции.

Техники, использующие «Повышение привилегий», часто перекрываются техниками тактики «Закрепление», так как особенности операционных систем, позволяющие злоумышленнику в ней закрепиться, могут применяться при наличии у него повышенных привилегий.

«Уклонение от защиты» – целью тактики является действия злоумышленника, направленные на уклонение от обнаружения. Техники, используемые для уклонения от защиты, включают в себя удаление или выключение программ, осуществляющих защиту, или использование доверенных процессов для скрытия и маскировки вредоносных программ.

«Доступ к учетным данным» – целью тактики является кража учетных данных: логинов и паролей. Техники, используемые здесь, включают в себя регистрацию действий пользователя с помощью keylogger или сброса (дампинга) учетных данных. Использование легитимных учетных данных дает возможность злоумышленникам скрываться от обнаружения и получать доступ к большему количеству аккаунтов.

«Исследование» – целью тактики является исследование злоумышленником инфраструктуры жертвы, то есть сбор информации о системе и внутренней сети. Такой метод позволяет злоумышленнику решить, как лучше действовать внутри периметра жертвы, понять, что можно контролировать и что позволит получить наибольшую выгоду.

«Перемещение внутри периметра» – целью тактики является продвижение злоумышленника внутри периметра жертвы. «Перемещение внутри периметра» включает в себя техники, позволяющие злоумышленнику получить доступ и управление удаленными системами в сети, в том числе с помощью установки собственного инструмента для получения удаленного доступа.

«Сбор» – целью тактики является сбор данных, способствующих достижению целей злоумышленников. «Сбор» использует техники идентификации и сбора информации, которую в дальнейшем чаще всего требуется переместить из целевой сети в подконтрольную злоумышленнику инфраструктуру, то есть выполнить так называемую эксфильтрацию данных. Примерами таких методов атак являются захват экрана (screenshot) и захват ввода клавиатуры.

«Управление и контроль» – целью тактики является связь злоумышленника со скомпрометированными системами для их управления. Чтобы избежать обнаружения, злоумышленники

обычно стараются скрыть свои действия за нормальным, обычным сетевым трафиком. Примеры включают использование законных протоколов (HTTP и подобных им) для передачи C&C-информации.

«Эксфильтрация» – целью тактики является кража данных злоумышленником, то есть вывод этих данных за периметр жертвы. Чаще всего после сбора нужных данных злоумышленники их упаковывают, чтобы избежать детектирования во время перемещения данных. Техники эксфильтрации включают транспортировку данных по C2-каналам и их альтернативам и могут подразумевать ограничение размера передаваемых данных.

«Воздействие» – целью тактики являются манипуляции или вмешательство в работу ИТ-инфраструктуры жертвы, или уничтожение систем и данных инфраструктуры. Техники влияния используются для достижения конечных целей злоумышленника.

Общий вид матрицы с тактиками представлен на рисунке 2.

Enterprise tactics

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Рисунок 2 – Общий вид матрицы ATT&CK

На этом уровне матрица ATT&CK очень похожа на другие модели угроз, которые описывают жизненный цикл противника.

Разница между ATT&CK и другими моделями заключается в ее объеме.

Категории тактик применимы от одной индивидуальной системы конечных точек к другой, так как противник перемещается по сети. В то же время модель жизненного цикла кибератаки требует учитывать больший диапазон действий в соответствии с жизненным циклом атакующего.

Тактики в модели ATT&CK также описывают враждебный процесс передвижения по корпоративной сети.

В качестве дополнения в информации об угрозах специалистом по безопасности (аналитиком) могут быть использованы описания из банка данных угроз безопасности информации, предоставляемого ФСТЭК.

5.2 Методология анализа киберугроз на основе ATT&CK

В качестве примера использования методологии MITRE ATT&CK при анализе киберугроз рассмотрим этапы анализа, применяемые в компании MITRE. Компания MITRE использует методы ATT&CK для создания, развития и ревизии аналитической информации об угрозах.

Методология, основанная на ATT&CK, включает в себя следующие шаги:

1) Идентификация поведения;
2) Получение данных;
3) Создание аналитики;
4) Создание сценария имитации действий злоумышленника;
5) Имитация угрозы;
6) Расследование атаки;
7) Оценка действий.

5.2.1. Идентификация поведения (шаг 1)

Процесс создания аналитики начинается с идентификации поведения злоумышленников. Чтобы приоритизировать поведение злоумышленников, необходимо ответить на четыре вопроса.

Какое поведение является самым распространенным?

Приоритизация тактик, техник и процедур, чаще всего используемых злоумышленниками, может оказать существенное влияние на безопасность. Способность различать серьезные угрозы позволяет организации сосредоточиться на нужных тактиках и техниках, представленных в ATT&CK.

Какие действия имеют наибольшее влияние?

Организации должны определить, какие техники и тактики ATT&CK могут иметь наибольшее влияние на их инфраструктуру. Это влияние может принимать формы физического разрушения элементов инфраструктуры, потери информации, компрометации системы или других негативных последствий.

Для какого поведения есть доступные данные?

Для поведения, по которому уже есть доступные данные, создавать аналитические решения проще и дешевле, чем для поведения, которое еще нужно обнаружить, или по которому еще нужно создать или развернуть инфраструктуру для сбора данных.

Какое поведение следует детектировать как вредоносное?

Разбор поведения злоумышленников, а не легитимных источников наиболее полезен для защищающей стороны, потому что приводит к меньшему числу ложноположительных результатов.

5.2.2. Получение данных (шаг 2)

На этапе подготовки к созданию аналитики организация должна принять решение, какие данные необходимо обнаружить, собрать и сохранить, чтобы на основе этих данных разработать аналитику.

Для этого необходимо определить, какие данные уже были собраны инструментами обнаружения и механизмами логирования. Во многих случаях правила и установки, по которым собираются данные, нуждаются в корректировке, иногда для сбора определенных данных требуется поменять инструменты и механизмы.

Обнаружение на конечных точках

Многие компании полагаются на обнаружение вредоносной активности с внешней стороны защищаемого периметра сети из-за относительной легкости развертывания инструментов детектирования. Это ограничивает наблюдение только входящим и исходящим трафиком, при этом от защищающей стороны часто ускользают события, происходящие внутри защищаемого периметра.

При использовании подобного подхода защищающая сторона полагается на захват и разбор сетевого трафика, брандмауэры, проксирование, системы обнаружения сетевых вторжений, другие системы сетевого анализа или блокирующие системы.

Если злоумышленник способен проникнуть внутрь защищаемого периметра и сохранить способность осуществлять тактику «Контроль и Управление» будучи незамеченным системами обнаружений сетевых вторжений, то защищающая сторона может не заметить его активность внутри сети.

Учитывая наличие возможности для злоумышленника использовать легитимные веб-сервисы и защищенные криптографией коммуникации, которые позволяют проходить сетевое обнаружение, действия внутри периметра становится отследить особенно сложно.

Обнаружение на конечных точках должно основываться на идентификации действий после компрометации, так как информация о действиях атакующего внутри периметра имеет большую ценность.

Без обнаружения сетевых событий на конечных точках, таких как старт процесса или новое сетевое соединение, практически невозможно обнаруживать большую часть атак, описанных в матрице, если нет конкретных знаний об атакующем, например, используемой инфраструктуре и протоколах.

Другой подход, основанный на обнаружении индикаторов компрометации на конечных точках или сборе снимков состояния системы, также может привести к невозможности обнаружить действия злоумышленника, прошедшего внешний периметр. Периодический сбор данных с конечных точек может привести к тому, что злоумышленник выполнит действия, компрометирующие систему в промежутках между итерациями сбора информации.

В качестве примера можно рассмотреть внедрение вредоносной программы RAT в легитимный процесс explorer.exe, который был осуществлен злоумышленником в промежутке между двумя сканированиями. В таком случае снимок состояния системы не покажет внедрения RAT в процесс.

5.2.3. Создание аналитики (шаг 3)

Когда у организации есть инструменты детектирования и сбора данных, она может приступить к созданию аналитики.

Создание аналитики требует наличия программной и аппаратной платформы, а также специалистов, которые могут с ними работать.

Исследователи MITRE выделяют следующие типы аналитики в методологии ATT&CK:

«Поведенческая аналитика» – целью аналитики является обнаружение специфического поведения злоумышленника, к примеру, создание новой службы Windows. При этом, поведение может и не быть вредоносным. Такое поведение необходимо сравнивать с техниками модели ATT&CK.

«Операционная аналитика» – целью аналитики является обнаружение того, что происходит внутри сетевого периметра в конкретный момент. Анализ не всегда должен быть направлен на то, чтобы генерировать инциденты, связанные с вредоносной активностью. Иногда большую пользу может принести анализ общего состояния периметра.

Такая аналитика может быть особенно полезна при определении состояния текущего «здоровья» защищаемой инфраструктуры.

«Поиск аномалий» – целью аналитики является обнаружение подозрительного поведения, отличного от нормы, к примеру, выполнение процессов, ранее в системе не выполнявшихся. Как и в случае операционной аналитики, предметом интереса анализа могут быть не только атаки.

«Форензика» – такая аналитика применяется при расследовании инцидентов. Чтобы быть наиболее полезной, форензика требует определенного уровня внедрения. К примеру, если аналитик находит событие сброса учетных данных на одном хосте, запуск аналитики может выявить всех пользователей, учетные данные которых были скомпрометированы.

Защищающая команда может использовать в работе все типы аналитики для внедрения в текущую деятельность. В качестве примера подобного объединения можно рассмотреть такой сценарий:

1) Специалисту SOC-центра приходит оповещение о создании запланированной задачи с помощью удаленного доступа (поведенческая аналитика);

2) После просмотра оповещения от скомпрометированной машины аналитик использует аналитические инструменты поиска отклонений в работе служб на этом хосте, в ходе чего выясняется, что незадолго до создания задачи на хосте была создана новая служба (поиск аномалий);

3) После обнаружения подозрительной службы аналитик использует инструменты, которые показывают все дочерние процессы службы, изучая которые он выясняет, что на хосте запущен RAT, после этого аналитик просматривает все дочерние процессы, запущенные RAT-ом и выясняет, что он запустил PowerShell (форензика);

4) После получения данных о вредоносном поведении на одном хосте, аналитик проверяет другие удаленные соединения в сети, которые были выполнены с этого хоста, детализируя тем самым все окружение, которое могло быть атаковано вредоносной программой (операционная аналитика).

5.2.4. Создание сценария имитации действий злоумышленника (шаг 4)

Традиционное тестирование на проникновение концентрируется на определенной цели, чаще всего в таком сценарии «красная команда» пытается взять под контроль критически важные системы атакуемой сети. В этом случае команда ограничена выбранной целью и может не учитывать множество дополнительных возможностей при поиске уязвимостей, не связанных с этой целью.

Подход MITRE к имитации действий злоумышленника отличается от традиционного подхода тем, что в процессе определения уязвимостей члены «красной команды» копируют поведение определенной группы или множества известных групп, чтобы протестировать специфические зоны защищаемой сети. В этом случае тесты, имитирующие действия злоумышленников, могут быть проведены быстрее и в более сфокусированном режиме, чем тесты тестирования на проникновение, выполняемого в полном объеме.

После появления новых инструментов и методов обнаружения, и укреплении их позиций среди специалистов по кибербезопасности, исследователи сосредотачиваются на способах их обхода, равно как и злоумышленники. Сценарии, имитирующие поведение злоумышленников, должны создаваться с осознанием этой идеи, а также понимания того, что у злоумышленника всегда могут быть специфические цели, например, доступ к информации, составляющей государственную тайну.

Во время выполнения тестов для «красной команды» можно назначать определённые цели, но действия ее специалистов должны быть сосредоточены на том, как они собираются достичь этой цели, и не важно, будет ли она достигнута.

В этом случае «синяя команда» сможет провести полное тестирование защищаемой сети против наиболее вероятных техник, применяемых злоумышленниками.

Создание сценария

Для создания сценария может потребоваться план, который должна разработать «белая команда» на основе знаний об инструментах и возможностях «красной» и «синей команды». План может быть основой для полного сценария поведения злоумышленников и включать следующие детали:

1) Аналитика детектирования и защитные возможности, которые необходимо протестировать;

2) Поведение, которое злоумышленники будут использовать;

3) Примерный план с последствиями действий, которые нужно предпринять, чтобы подтвердить возможности защиты;

4) Системные, сетевые или другие ресурсы, необходимые для проведения тестирования.

Сценарий имитации действий злоумышленника не обязательно должен быть подробным сценарием. Он должен быть достаточно подробным, чтобы дать «красной команде» направление, в котором нужно подтвердить тестируемые защитные возможности. При этом сценарий должен быть и достаточно гибким, чтобы «красная команда» могла изменять свои действия по необходимости и применять тестовые вариации, которые еще неизвестны «синей команде». В момент, когда «синяя команда» становится достаточно компетентной, чтобы предотвратить известные угрозы, у «красной команды» должна быть свобода действий для выхода за рамки чистой имитации.

В этом ей должна помочь «белая команда», которая может решить, какое еще поведение может быть протестировано, не уведомляя «синюю команду» о возможных действиях «красной команды».

В таком сценарии «белая команда» также сохраняет возможность свободно сообщать «красной команде» детали о защищаемой инфраструктуре, чтобы в полной мере протестировать меры обнаружения против последовательности действий злоумышленников.

5.2.5. Имитация угрозы (шаг 5)

После создания сценария действий злоумышленника и аналитики «красная команда» выполняет те действия, которые «белая команда» определила в качестве необходимых для проведения тестирования. Имитация угрозы позволяет специалистам по информационной безопасности проверить эффективность разработанных мер.

«Белая команда» наряду с владельцами проверяемой сетевой инфраструктуры должна координировать процесс имитации угрозы, чтобы предупредить и предотвратить возможные негативные последствия такой активности.

5.2.6. Расследование атаки (шаг 6)

Для тестирования аналитики в условиях, приближенных к реальным, полезно включать в «синюю команду» аналитиков, разработавших применяемую аналитику. Это позволяет им понять, как она работает, и какие изменения необходимо внести, чтобы сделать аналитику лучше.

С другой стороны, включение специалистов, не участвовавших в процессе разработки, тоже может быть полезным. Тестирование в таком ключе позволяет понять, является ли аналитика, задействованная в тестировании, интуитивно понятной для любого пользователя, и не является ли успех «синей команды» следствием институциональных знаний аналитиков (т.е. комбинации опыта, организационных и личных знаний специалистов).

Процесс тестирования аналитики в основном начинается с выявления «синей командой» какого-либо индикатора активности «красной команды», чаще всего такой точкой входа становится поведенческая аналитика. После нахождения такого индикатора, необходимо для проведения дальнейшего расследования подключать аналитику следующих типов: форензику, операционную, исследующую аномалии.

«Синяя команда» при расследовании атаки «красной команды» должна собрать значительные объемы информации по следующим направлениям:

1) Вовлеченные/Скомпрометированные хосты;
2) Скомпрометированные учетные записи;
3) Задачи и цели;
4) Используемые тактики и техники;

Вовлеченные/Скомпрометированные хосты – это список конечных точек, на которых было зафиксировано подозрительное поведение. Эта информация критически важна для того, чтобы справиться с инцидентом.

Одним из ключевых факторов успеха «синей команды» является способность выявить все скомпрометированные учетные записи внутри защищаемой сети. Если это сделать не получается, то «красная команда» или реальный злоумышленник смогут восстановить доступ к сети, используя другие векторы атаки.

«Синяя команда» должна выявлять цели и задачи, которые ставит перед собой «красная команда», а также информацию о том, были эти цели достигнуты или нет. Такая информация требует значительного объема данных, чтобы можно было говорить о намерениях «красной команды» объективно.

Очень важно определить тактики и техники ATT&CK, которые были задействованы «красной командой», чтобы на основе этого знания улучшить работу по защите инфраструктуры. Таким знанием может быть информация о неправильной конфигурации сети или информация о технике ATT&CK, которую «синяя команда» еще не умеет выявлять с помощью своей аналитики.

5.2.7. Оценка действий (шаг 7)

После завершения тестирования «белая команда» вместе с членами «красной» и «синей команды» анализирует предпринятые с обеих сторон действия. Это позволяет собрать важную информацию о том, насколько успешны были защитные действия «синей команды» против атакующих действий «красной команды».

С помощью такой информации «синяя команда» может улучшить свою аналитику и выявить поведение злоумышленников, для которого им нужно создать или установить новые инструменты обнаружения, или собрать новые данные, или создать новую аналитику.

5.3 Вывод по разделу

Метод разработки аналитики на основе ATT&CK – мощный инструмент для защиты ИТ-инфраструктуры, который используется, чтобы создавать и поддерживать возможность обнаружения и устранения угроз специалистами ИБ по всему миру. Он базируется на пяти основных принципах:

– детектирование после компрометации;

– фокус на анализе поведения;

– основан на модели угроз;

– итеративность;

– создание аналитики в реальных условиях.

Обнаружение с использованием этих методов не зависит от типичных заведомо неисправных IOC или внешних уведомлений о нарушениях в сети и может привести к быстрому обнаружению компрометации сети путем обнаружения использованных противником приемов, описанных в модели ATT&CK.

База знаний MITRE ATT&CK постоянно развивается, поэтому информация о тактиках, техниках и их количестве может изменяться со временем и описанное в настоящем документе не всегда будет совпадать с текущим состоянием матрицы ATT&CK.

6. Матрица противодействия киберугрозам MITRE D3FEND

MITRE D3FEND представляет собой матрицу противодействия киберугрозам, граф знаний, который используется в качестве методологии уменьшения потенциальной поверхности атаки.

Подобно матрице MITRE ATT@CK она содержит тактики и техники, только уже не те, что используются злоумышленниками для нанесения вреда инфраструктуре атакуемого, а те, что помогают эту инфраструктуру защитить (см. рис. 3).

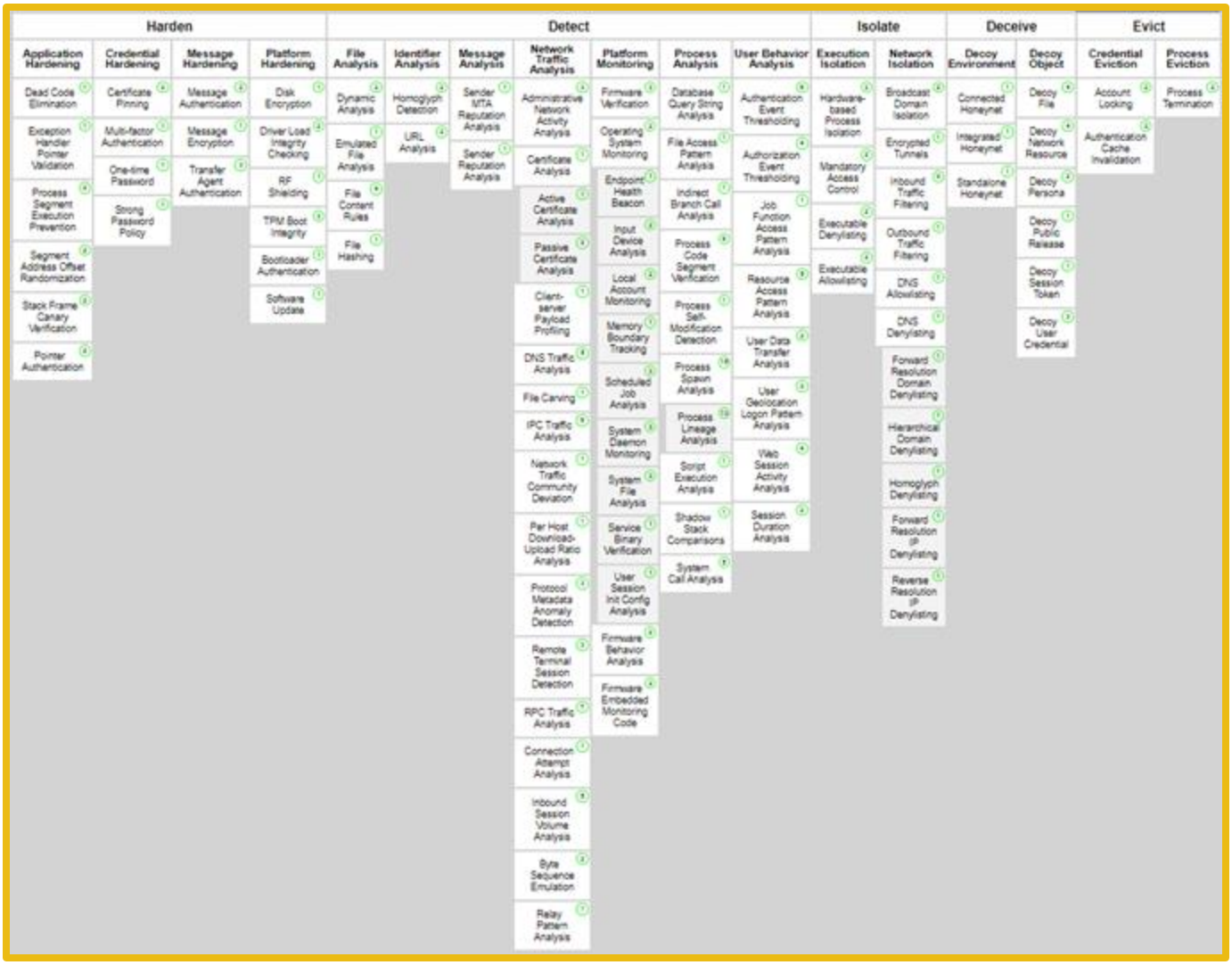


Рисунок 3 – Тактики и техники MITRE D3FEND (версия 0.9.3-BETA-1)

В самом простом смысле D3FEND представляет собой каталог техник противодействия киберугрозам и связей этих техник с техниками атак. На данный момент все используемые техники противодействия киберугрозам распределены по пяти тактикам.

«Закрепление» – целью тактики является увеличение альтернативной стоимости совершения вредоносных действий для злоумышленника. «Укрепление» отличается от тактики «Обнаружение» тем, что применяется в момент жизненного цикла ИТ-инфраструктуры, когда она еще не функционирует онлайн или пока не выполняет оперативные задачи. Основными техниками являются:

– программное укрепление;

– укрепление учетных данных;

– укрепление почтовой инфраструктуры;

– укрепление платформы.

«Обнаружение» – целью тактики является обнаружение действий злоумышленника по получению доступа к защищаемой ИТ-инфраструктуре. Основными техниками являются:

– анализ файлов;

– анализ идентификаторов;

– анализ почтовых сообщений;

– анализ сетевого трафика;

– мониторинг программного обеспечения и устройств;

– анализ процессов;

– анализ поведения пользователей.

«Изоляция» – целью тактики является создание логических или физических барьеров в защищаемой инфраструктуре, которые снижают возможности злоумышленников в части расширения доступа к данным и элементам инфраструктуры.

Основными техниками являются:

– изоляция выполнения;

– сетевая изоляция.

«Обман» – целью тактики является разрешение злоумышленнику получения доступа к окружению, которое контролирует атакуемый. Основными техниками являются:

– приманка в виде окружения;

– приманка в виде объекта.

«Удаление» – целью тактики является удаление злоумышленника и его активности из защищаемой инфраструктуры. Основными техниками являются:

– удаление скомпрометированных учетных данных;

– уничтожение вредоносных процессов.

7. YARA

7.1 Общие сведения

YARA в Программе – это инструмент матчинга сведений о подозрительных и вредоносных файлах и событиях, имеющихся в базе данных Программы или TI-платформы, с файлами и событиями, обнаруживаемыми на машинах с агентами.

Инструмент помогает аналитику искать и классифицировать вредоносные экземпляры на основе сигнатурного анализа. Утилита выполняет анализ на основе формальных YARA-описаний (правил).



Важно

YARA-правила применяются только к исполняемым файлам (PE) или к файлам с активным содержимым (если активны соответствующие опции в профиле безопасности). В случае с YARA-матчингом под запуском PE-файлов подразумевается исполнение программ, загрузка динамических библиотек (или драйверов) для исполнения их кода. Для файлов с активным содержимым (файлы с любыми расширениями, указанными в профиле безопасности агента, например, с расширениями PDF, PS1, PSM1 и т.д.), анализ по YARA-правилам выполняется при любом открытии файлов, когда осуществляется доступ к их содержимому.

7.2 Написание YARA-правил

Правила YARA легко писать и понимать. Синтаксис напоминает язык C.

Простейшее правило, которое можно написать для YARA:

```
rule
{
   condition:
      false
}
```

Каждое правило в YARA начинается с ключевого слова или идентификатора правила rule, за которым следует значение идентификатора.

Идентификаторы должны соответствовать тем же лексическим соглашениям языка программирования C, они могут содержать любой буквенно-цифровой символ и символ подчеркивания, но первый символ не может быть цифрой. Идентификаторы правил чувствительны к регистру и не могут превышать 128 символов.

Следующие ключевые слова зарезервированы и не могут использоваться в качестве идентификатора: all, and, any, ascii, at, condition, contains, entrypoint, false, filesize, fullword, for, global, in, import, include, int8, int16, int32, int8be, int16be, int32be, matches, meta, nocase, not, or, of, private, rule, strings, them, true, uint8, uint16, uint32, uint8be, uint16be, uint32be, wide, xor

Правила обычно состоят из двух разделов:

– определение строк (strings definition);

– условие (condition).

Раздел определения строк может быть опущен, если правило не полагается на какую-либо строку, но всегда требуется раздел condition.

В разделе strings определяются строки, которые будут частью правила. Каждая строка имеет идентификатор, состоящий из символа $, за которым следует последовательность буквенно-цифровых символов и подчеркиваний. Эти идентификаторы могут использоваться в разделе условий для ссылки на соответствующую строку. Строки могут быть определены в текстовой или шестнадцатеричной форме, как показано в следующем примере:

```
rule ExampleRule
{
   strings:
      $my_text_string = "text here"
      $my_hex_string = {E2 34 A1 C8 23 FB}
   condition:
      $my_text_string or $my_hex_string
}
```

Текстовые строки заключаются в двойные кавычки, как и в языке C. Шестнадцатеричные строки заключаются в фигурные скобки и состоят из последовательности шестнадцатеричных чисел, которые могут

отображаться как с пробелами, так и без. В шестнадцатеричных строках нельзя использовать десятичные числа.

Раздел условия (condition) – это место, в котором прописывается логика правила. Этот раздел должен содержать логическое выражение, указывающее, при каких обстоятельствах файл или событие удовлетворяет правилу или нет.

7.3 Синтаксис и семантика YARA

7.3.1. Комментарии

Можно добавлять комментарии к правилам YARA, как если бы это был исходный файл C.

Поддерживаются как однострочные, так и многострочные комментарии в стиле C.

```
/*
   This is a multi-line comment ...
*/
rule CommentExample   // ... and this is single-line comment
{
   condition:
      false  // just a dummy rule, don't do this
}
```

7.3.2. Строки

В YARA есть три типа строк:

– шестнадцатеричные строки;

– текстовые строки;

– регулярные выражения.

Шестнадцатеричные строки используются для определения необработанных последовательностей байтов, в то время как текстовые строки и регулярные выражения полезны для определения частей разборчивого текста.

Текстовые строки и регулярные выражения также могут использоваться для представления необработанных байтов с помощью управляющих последовательностей.

7.3.3. Шестнадцатеричные строки

Шестнадцатеричные строки допускают три специальные конструкции, которые делают их более гибкими:

– подстановочные знаки;

– переходы (или прыжки);

– альтернативы.

Подстановочные знаки – это заменители, которые можно вставить в строку, указав, что некоторые байты неизвестны и должны соответствовать чему угодно.

Один из знаков заменителей – это вопросительный знак (?).

Ниже представлен пример шестнадцатеричной строки с подстановочными знаками:

```
rule WildcardExample
{
   strings:
      $hex_string = {E2 34 ?? C8 A? FB}
   condition:
      $hex_string
}
```

Как показано в примере, подстановочные знаки являются полубайтами, что означает, что можно определить только один полубайт байта и оставить другой неизвестным.

Подстановочные знаки полезны при определении строк, содержимое которых может варьироваться, но известна длина блоков переменных.

В некоторых случаях может потребоваться определить строки с фрагментами переменного содержания и длины.

В таких ситуациях можно использовать прыжки вместо подстановочных знаков:

```
rule JumpExample
```

```
{
   strings:
      $hex_string = {F4 23 [4-6] 62 B4}
   condition:
      $hex_string
}
```

В приведенном выше примере есть пара чисел, заключенных в квадратные скобки и разделенных дефисом, это прыжок. Этот переход указывает на то, что любая произвольная последовательность от 4 до 6 байтов может занимать позицию перехода. Любая из следующих строк будет соответствовать шаблону:

F4 23 01 02 03 04 62 B4;

F4 23 00 00 00 00 00 62 B4;

F4 23 15 82 A3 04 45 22 62 B4.

Любой прыжок [XY] должен соответствовать условию 0 <= X <= Y. Начиная с YARA 2.0 ограничений для X и Y нет.

Допустимые прыжки:

FE 39 45 [0-8] 89 00;

FE 39 45 [23-45] 89 00;

FE 39 45 [1000-2000] 89 00.

Недопустимый прыжок:

FE 39 45 [10-7] 89 00.

Если нижняя и верхняя границы равны, можно написать одно число в скобках, например, FE 39 45 [6] 89 00.

Вышеупомянутая строка эквивалентна следующим строкам:

FE 39 45 [6-6] 89 00;

FE 39 45 ?? ?? ?? ?? ?? ?? 89 00.

Начиная с YARA 2.0 также можно использовать неограниченные прыжки:

FE 39 45 [10-] 89 00;

FE 39 45 [-] 89 00.

Первый означает [10-бесконечность], второй означает [0-бесконечность].

Также существуют ситуации, в которых можно указать разные альтернативы для данного фрагмента шестнадцатеричной строки. В таких ситуациях можно использовать синтаксис, напоминающий регулярное выражение, добавив знак альтернативы |:

```
rule AlternativesExample1
{
   strings:
      $hex_string={F4 23 (62 B4 | 56) 45}
   condition:
      $hex_string
}
```

Это правило будет соответствовать любому файлу, содержащему F42362B445 или F4235645.

Можно задать более двух альтернатив. Фактически, нет никаких ограничений на количество и длину альтернативных последовательностей, которые можно указать:

```
rule AlternativesExample2
{
   strings:
      $hex_string = {F4 23 (62 B4 | 56 | 45 ?? 67) 45}
   condition:
      $hex_string
}
```

В этом примере строки, содержащие подстановочные знаки, разрешены как часть альтернативных последовательностей.

7.3.4. Текстовые строки

Как показано в предыдущих разделах, текстовые строки обычно определяются следующим образом:

```
rule TextExample
```

```
{
   strings:
      $text_string = "foobar"
   condition:
      $text_string
}
```

Это простейший случай: строка в кодировке ASCII с учетом регистра. Однако текстовые строки могут сопровождаться некоторыми полезными модификаторами, которые изменяют способ интерпретации строки. Эти модификаторы добавляются в конце определения строки и разделяются пробелами.

Текстовые строки могут содержать следующее подмножество управляющих последовательностей, доступных в языке C (см. таблицу 6).

Таблица 6 – Последовательности в текстовых строках

Символ	Описание
\"	Двойная кавычка
\\	Обратная косая черта
\r	Возврат каретки (переход курсора к левому краю текстового поля)
\t	Горизонтальная табуляция
\n	Перевод строки
\xdd	Любой байт в шестнадцатеричной системе счисления

Во всех версиях YARA до 4.1.0 текстовые строки принимали любые символы Unicode независимо от их кодировки. Эти символы интерпретировались YARA как необработанные байты, и поэтому конечная строка фактически определялась форматом кодировки, используемым текстовым редактором. Исходное намерение всегда заключалось в том, чтобы строки YARA были только ASCII, а YARA 4.1.0 начал выдавать предупреждения о не-ASCII символах в строках. Это ограничение не распространяется на строки в разделе метаданных или в комментариях.

7.3.5. Строки без учета регистра

Текстовые строки в YARA по умолчанию чувствительны к регистру, однако можно перевести строку в режим без учета регистра, добавив модификатор nocase в конце определения строки:

```
rule CaseInsensitiveTextExample
{
   strings:
      $text_string = "foobar" nocase
   condition:
      $text_string
}
```

С модификатором nocase, строка *foobar* будет соответствовать *Foobar*, *FOOBAR* и *fOoBaR*. Этот модификатор можно использовать вместе с любым модификатором, кроме base64 и base64wide.

7.4 Модули YARA, доступные в EDR

Модули позволяют расширить возможности YARA, позволяют определить структуры данных и функции, которые могут использоваться в правилах для выражения более сложных условий. В RT Protect EDR доступны следующие модули YARA:

1) Time;
2) Math;
3) PE;
4) Hash;
5) Dotnet;
6) ELF.

Time – модуль позволяет использовать временные условия в правилах YARA. Содержит функцию **now()**. Функция возвращает целое число – количество секунд с 1 января 1970 года.

Math – модуль позволяет вычислять определенные значения из частей файла и создавать сигнатуры на основе этих результатов. Содержит функции **entropy(offset, size)**, **entropy(string)**, **monte_carlo_pi(offset, size)**, **monte_carlo_pi(string)**, **serial_correlation(offset, size)**, **serial_correlation(string)**, **mean(offset, size)**, **mean(string)**, **deviation(offset, size, mean)**, **deviation(string, mean)**, **in_range(test, lower, upper)**, **max(int, int)**, **min(int, int)**.

PE – модуль позволяет создавать детализированные правила для исполняемых файлов с помощью атрибутов и функций формата PE-файла. Подробная информация о формате PE-файла содержится в

документации Microsoft. Модуль содержит множество атрибутов, функций и переменных, подробно можно ознакомиться в документации YARA.

Hash – модуль позволяет вычислять хеши (MD5, SHA1, SHA256) из частей файла и создавать сигнатуры на основе этих хешей. Содержит функции **md5(offset, size)**, **md5(string)**, **sha1(offset, size)**, **sha1(string)**, **sha256(offset, size)**, **sha256(string)**, **checksum32(offset, size)**, **checksum32(string)**.

Dotnet – модуль позволяет создавать детализированные правила для файлов .NET с помощью атрибутов и функций формата файлов .NET. Подробно можно ознакомиться в документации YARA.

ELF – модуль ELF во многом схож с модулем PE, но предназначен для работы с ELF-файлами. Этот модуль предоставляет доступ к большинству полей, присутствующих в заголовке ELF.

7.5 Подробнее о правилах

Для ознакомления с исчерпывающей информацией по особенностям написания правил в утилите YARA можно перейти по ссылке (документация YARA).

8. Общая информация о работе с инцидентами в Программе

8.1 Категории аналитиков ИБ

Роли аналитиков могут быть заданы администратором в разделе **Пользователи и роли**. Подразумевается, что можно создать роль с любым набором прав, что дает большую гибкость при назначении ролей пользователям.

Аналитик – основной функцией специалиста является реагирование на инциденты, генерируемые Программой в режиме реального времени. После получения уведомления о создании инцидента аналитик решает, представляет ли событие или события, помещенные в инцидент, угрозу для защищаемой инфраструктуры и в соответствии с этим заключением предпринимает дальнейшие действия. Чаще всего специалист такого плана будет работать с угрозами известными, обнаруженными Программой на основе анализа файловых, бесфайловых, сетевых и других угроз.

8.2 Регистрация инцидентов

Под инцидентом в общем смысле понимается событие в защищаемой информационной системе, требующее реакции персонала ИБ. Применительно к разработанной системе инцидент – это контейнер событий, формирующих подозрительную активность, и набор связанных атрибутов (название, описание, временной интервал активности, ответственный аналитик, критичность, статус и др.).

Способы регистрации инцидентов:

1) Автоматическое создание на основе наборов с аналитическими правилами или внутренними алгоритмами;

2) Создание инцидента вручную при проведении ретроспективных расследований.

Автоматическое создание инцидента проводится на основе правил и алгоритмов, в том числе и средствами машинного анализа. Инцидент выступает в качестве контейнера для событий, идентифицированных на стороне агента как подозрительные или вредоносные. Инцидент создается при обнаружении событий, критичность которых находится на уровне **Средняя** или выше.

В дальнейшем такой инцидент может обогащаться событиями, в том числе более низкой критичности, в течение восьми часов после создания инцидента. Если инцидент взят в работу, то его наполнение событиями останавливается.

Логика объединения событий в инциденты определяется агентом за счет назначения событиям идентификатора корреляции, что позволяет объединять в один инцидент события группы процессов, имеющих отношение «родитель-потомок». В инцидент также могут объединяться события с разных агентов по какому-либо артефакту, например, по модулю-инициатору операции или домену, к которому обращаются агенты.

Независимо от того, какое действие было выбрано для события или событий, ставших основой для создания инцидента, ему присваивается статус **Новый**. Для дальнейшей работы с инцидентом аналитику на странице **Инциденты** следует нажать кнопку **Назначить инцидент** ( ) в поле **Статус** и в открывшемся окне назначить ответственного за инцидент, после чего сохранить его в новом статусе. В случае ложноположительного срабатывания аналитику необходимо нажать кнопку **Закрыть инцидент** ( ). Для информативности необходимо писать комментарии при закрытии и назначении инцидента, для этого предусмотрены поля ввода в окнах **Назначение инцидентов** и **Закрытие инцидента**.



Совет

Ручное создание инцидента производится аналитиком согласно проведенному им анализу с использованием всех реализованных в системе возможностей. Первичное создание инцидента в ручном режиме следует выполнять из раздела **Активность**.

8.2.1. Алгоритм автоматического создания инцидентов для агентов Linux

Для событий, у которых в качестве ОС указана Linux, автодополняемый инцидент формируется на основе полей **platform** и **rul**, где первое – это ОС Linux, а второе – это правило, на основе которого создается событие.

8.3 Атрибуты инцидентов

Инцидент имеет следующие атрибуты:

1) Внутренний сквозной порядковый номер (*#8219*);

2) Название;

3) Время регистрации;

4) Время действия (от начального события до конечного);

5) Группа/имя агента;

6) Критичность:

– «Информация»;

– «Низкая»;

– «Средняя»;

– «Высокая»;

– «Критичная»;

7) Ответственный;

8) Количество событий, входящих в инцидент (является ссылкой на просмотр событий на странице **Активность**);



Совет

При большом количестве событий в инциденте необходимо использовать фильтры на странице **Активность** и DSL-запросы для поиска нужной информации внутри инцидента.

9) Статус:

– «Новый»;

– «Назначен»;

– «Закрыт».

Сразу после создания инцидент получает инкрементный глобальный номер, сгенерированное автоматически название, отражающее суть инцидента, описание, статус **Новый**. Для перевода инцидента из статуса **Новый** в статус **Назначен** необходимо нажать кнопку Назначить инцидент, после чего в окне **Назначение инцидента** выбрать ответственного за его решение и нажать кнопку **Сохранить**.

В случае создания инцидента вручную ответственным за его решение назначается аналитик, создавший инцидент.

Под статусом **Назначен** подразумевается, что ответственный за инцидент сотрудник взял инцидент в работу и проводит расследование. Состояние инцидента **Закрыт** означает, что аналитик обработал события инцидента и закрыл его. Инцидент может открываться повторно, для этого необходимо в закрытом инциденте нажать кнопку **Открыть повторно** или нажать кнопку  (**Назначить инцидент (открыть повторно)**) на странице **Инциденты**.

Критичность инцидента, созданного автоматически, устанавливается равной максимальной критичности события-обнаружения, на основе которого создан инцидент.

8.4 Удаление инцидентов

Чтобы удалить инциденты, необходимо выбрать их на странице **Инциденты** и нажать кнопку **Удалить выбранные**. Инциденты обычно удаляются в том случае, если работа по ним уже давно закончена или инцидент явно не соответствует статусу инцидента. Операция удаления также доступна на странице **Инцидент**. Чтобы выполнить операцию, необходимо нажать кнопку **Удалить инцидент**.



Примечание

Вместе с инцидентом удаляются события, входящие в этот инцидент.

9. Модель данных в RT Protect EDR

9.1 Общие сведения

События, зарегистрированные агентом, отправляются на сервер в формате JSON. Отправка событий с агента осуществляется блоками. Каждый блок содержит заголовок и массив событий разного типа. Каждое событие включает в себя 2 набора полей – общий набор и набор, специфичный для определенного вида события. Полный список полей событий и их JSON-представления, которые могут быть применены для написания DSL-запросов или индикаторов атак, представлен в таблице 7.

Таблица 7 – Общий список полей событий

Назначение	Тип данных	JSON	Подсистема
Тип события	enum	t	Общая
Время регистрации события	timestamp	time	Общая
Действие, связанное с событием	enum	act	Общая
Причина предпринятого действия	enum	rsn	Общая
Правило, относящееся к событию	string	rul	Общая
Идентификатор техники/тактики MITRE	string	mitre	Общая
Критичность (уровень важности) события	enum	svrt (по умолчанию: 0)	Общая
Уникальный идентификатор процесса	int (индекс в массиве GUID'ов)	uuid	Общая
Уникальный идентификатор группы процессов	int (индекс в массиве GUID'ов)	hid	Общая
Уникальный идентификатор корреляции событий	string (индекс в массиве GUID'ов)	cid	Общая
Идентификатор процесса на агентской системе	unsigned	pid	Общая
Идентификатор родительского процесса на агентской системе	unsigned	ppid	Общая
Полное имя исполняемого файла процесса	string MANGLED	app	Общая
Командная строка процесса	string	cmdl	Общая
Номер сессии, в которой работает процесс на агентской системе	unsigned	sess (по умолчанию: 0)	Общая
SID пользователя, создавшего процесс	string	sid	Общая
Издатель ЭП исполняемого файла процесса	string	app_sgnr	Общая
Имя пользователя, запустившего процесс	string	usr	Общая
Домен (имя компьютера) пользователя, запустившего процесс	string	dom	Общая
Подтип события	enum	st	Общая

Назначение	Тип данных	JSON	Подсистема
Поведенческие признаки процесса (первая группа)	uint64	rf0	Общая
Поведенческие признаки процесса (вторая группа)	uint64	rf1	Общая
Флаги исполняемого файла процесса	int64	exclf	Общая
Исключения для программ, назначенные процессу	string	excls	Общая
Синтетическое событие (принимает значения true или false)	int (0/1)	syn	Общая
Версия события	unsigned	efmt	Общая
Протокол	enum	proto	Сеть
Признак работы по IPv6 (принимает значения true или false)	int (0/1)	ipv6	Сеть
Уникальный идентификатор сетевого потока	string (индекс в массиве GUID'ов в текстовой форме)	fluuid	Сеть
Идентификатор сетевого потока	int64	flow	Сеть
Отправка или прием (принимает значения true или false)	int (0/1)	out	Сеть
Размер полезных данных (payload) сетевого пакета	int64	size	Сеть
Имя хоста, соответствующее удаленному IP-адресу	string	host	Сеть
Тип DNS-запроса	enum	dnsq_t	Сеть
Статус DNS-запроса	unsigned	dnsq_s	Сеть
Результат DNS-запроса	string	dnsq_r	Сеть
Имя хоста из DNS-запроса	string	dnsq_h	Сеть
Идентификатор транзакции DNS-обмена	unsigned	dns_trx	Сеть
Имя хоста (server_name) из сообщения SSL Client Hello	string	ssl_h	Сеть
Удаленный IP-адрес	string	r_ip	Сеть
Удаленный порт	unsigned	r_p	Сеть
Локальный IP-адрес	string	l_ip	Сеть
Локальный порт	unsigned	l_p	Сеть
Исключение для удаленного IP-адреса	unsigned	r_ip_excl	Сеть
Исключение для имени хоста, соответствующего удаленному IP-адресу	unsigned	h_excl	Сеть
Исключение для имени хоста в запросе	unsigned	rqh_excl	Сеть
Тип ICMP-сообщения	unsigned (код или мнемоника)	icmp_t	Сеть
Код ICMP-сообщения	unsigned (код или мнемоника)	icmp_c	Сеть
Имя хоста в индикаторе компрометации	string	ioc_h	Сеть

Назначение	Тип данных	JSON	Подсистема
Флаги сетевого события	unsigned	netf	Сеть
Общий размер исходящих данных за время жизни подключения, байт	uint64	o_sz	Сеть
Общий размер входящих данных за время жизни подключения, байт	uint64	i_sz	Сеть
Время жизни подключения, в 100-наносекундных интервалах	uint64	lt	Сеть
Полное имя файла	string MANGLED	name	Файлы, Защита данных
Время создания файла	timestamp	crtime	Файлы, Процессы
Время последнего изменения файла	timestamp	chtime	Файлы, Процессы
Размер файла	int64	fsize	Файлы, Процессы
Тип файла	enum	ftype	Файлы, Процессы
Атрибуты файла	unsigned	attr	Файлы, Процессы
SHA-1 файла	string	sha1	Файлы, Процессы
MD5 файла	string	md5	Файлы, Процессы
SHA-256 файла	string	sha256	Файлы, Процессы
Imphash файла	string	imphash	Файлы, Процессы
Электронная подпись файла	string	sgnr	Файлы, Процессы
Статус электронной подписи файла	enum	sgnr_s	Файлы, Процессы
Признак доверенной электронной подписи файла	int (-/1)	sgnr_t	Файлы, Процессы
Оригинальное имя файла	string	ofn	Файлы, Процессы
Компания-издатель файла	string	fcomp	Файлы, Процессы
Версия файла	string	fver	Файлы, Процессы
Описание файла	string	fdesc	Файлы, Процессы
Продукт, к которому относится файл	string	fprod	Файлы, Процессы

Назначение	Тип данных	JSON	Подсистема
Тип упаковщика файла	string	pack	Файлы, Процессы
Файл находится в "белом" списке	int (-/1)	fwhite	Файлы, Процессы
Исключение для файла по хешу	string	fh_excl	Файлы, Процессы
Исключение для файла по имени	string	fn_excl	Файлы, Процессы
Файл расположен в директории автозапуска (принимает значения true или false)	int (0/1)	arun	Файлы
Новое имя файла	string MANGLED	fnew	Файлы, Защита данных
Файл был заменен (принимает значения true или false)	int (0/1)	owrt	Файлы
Предыдущее время создания файла	timestamp	old_t	Файлы
Новое время создания файла	timestamp	new_t	Файлы
Файл содержит атрибут "скрытый" (принимает значения true или false)	int (0/1)	hdn	Файлы
Файл содержит атрибут "системный" (принимает значения true или false)	int (0/1)	sys	Файлы
Операция совершается над альтернативным потоком данных файла (принимает значение только true)	int (-/1)	ads	Файлы
Для файла была создана резервная копия (принимает значение только true)	int (-/1)	save	Файлы
Доступ на удаление (принимает значение только true)	int (-/1)	delete	Файлы
Доступ на чтение (принимает значение только true)	int (-/1)	read	Файлы
Доступ на модификацию (принимает значение только true	int (-/1)	modify	Файлы
Обмен именами (принимает значение только true) (поле доступно только в ОС Linux)	int (-/1)	nxchg	Файлы
Имя альтернативного потока данных файла	string	strm	Файлы
SID предыдущего владельца файла	string	own_old	Файлы
Домен предыдущего владельца файла	string	own_old_dom	Файлы
Имя предыдущего владельца файла	string	own_old_usr	Файлы
Предыдущий владелец файла был задан по умолчанию	int (-/1)	own_old_def	Файлы
SID нового владельца файла	string	own_new	Файлы

Назначение	Тип данных	JSON	Подсистема
Домен нового владельца файла	string	own_new_dom	Файлы
Имя нового владельца файла	string	own_new_usr	Файлы
Новый владелец файла был задан по умолчанию	int (-/1)	own_new_def	Файлы
SID предыдущей основной группы владельца файла	string	grp_old	Файлы
Домен предыдущей основной группы владельца файла	string	grp_old_dom	Файлы
Имя предыдущей основной группы владельца файла	string	grp_old_usr	Файлы
Предыдущая основная группа владельца файла была задана по умолчанию	int (-/1)	grp_old_def	Файлы
SID новой основной группы владельца файла	string	grp_new	Файлы
Домен новой основной группы владельца файла	string	grp_new_dom	Файлы
Имя новой основной группы владельца файла	string	grp_new_usr	Файлы
Новая основная группа владельца файла была задана по умолчанию	int (-/1)	grp_new_def	Файлы
Предыдущий DACL файла	string	dacl_old	Файлы
Предыдущий DACL файла был задан по умолчанию	int (-/1)	dacl_old_def	Файлы
Новый DACL файла	string	dacl_new	Файлы
Новый DACL файла был задан по умолчанию	int (-/1)	dacl_new_def	Файлы
Предыдущий SACL файла	string	sacl_old	Файлы
Предыдущий SACL файла был задан по умолчанию	int (-/1)	sacl_old_def	Файлы
Новый SACL файла	string	sacl_new	Файлы
Новый SACL файла был задан по умолчанию	int (-/1)	sacl_new_def	Файлы
Предыдущая мандатная метка файла	unsigned	mlbl_old	Файлы
Предыдущая маска мандатной метки файла	unsigned	mlbl_old_mask	Файлы
Новая мандатная метка файла	unsigned	mlbl_new	Файлы
Новая маска мандатной метки файла	unsigned	mlbl_new_mask	Файлы
Код оповещения	enum	detect	Сеть, Файлы, Процессы, Реестр
Полное имя исполняемого модуля–инициатора операции	string MANGLED	who	Файлы, Процессы, Реестр
Идентификатор нити–инициатора операции	unsigned	whotid	Файлы,

Назначение	Тип данных	JSON	Подсистема
			Процессы, Реестр
Стартовый адрес нити–инициатора операции	uint64	whoaddr	Файлы, Процессы, Реестр
Флаги исполняемого модуля-инициатора операции	uint64	whof	Файлы, Процессы, Реестр
Исключения для программ, назначенные инициатору операции	string	who_excls	Сеть, Файлы, Процессы, Реестр
Стек вызовов операции	string	trace	Процессы
Командная строка родительского процесса	string	cmdlp	Процессы
Электронная подпись родительского процесса	string	sgnrp	Процессы
Командная строка прародителя (grand parent)	string	cmdlg	Процессы
Рабочий каталог процесса	string MANGLED	wdir	Процессы
Уровень защиты процесса	unsigned	prot	Процессы
Уровень доверия (integrity level) процесса	unsigned	integ	Процессы
Время создания процесса	timestamp	when	Процессы
Уникальный идентификатор родительского процесса	int (индекс в массиве GUID'ов)	parent	Процессы
Уникальный идентификатор процесса-создателя	int (индекс в массиве GUID'ов)	caller	Процессы
Идентификатор процесса-инициатора операции	unsigned	cpid	Процессы
Полное имя процесса-инициатора операции	string MANGLED	cpath	Процессы
Код завершения процесса	unsigned	code	Процессы
Уникальный идентификатор целевого процесса	int (индекс в массиве GUID'ов)	targ	Процессы
Полное имя целевого процесса	string MANGLED	tpath	Процессы
Идентификатор целевого процесса	unsigned	tpid	Процессы
Флаги образа целевого процесса	uint64	targf	Процессы
Поведенческие признаки целевого процесса (первая группа)	uint64	trf0	Процессы
Поведенческие признаки целевого процесса (вторая группа)	uint64	trf1	Процессы
Имя модуля целевой нити	string	tmod	Процессы
Имя функции целевой нити	string	tfunc	Процессы
Полное имя файла образа	string MANGLED	path	Процессы
Флаги нити	unsigned	tf	Процессы

Назначение	Тип данных	JSON	Подсистема
Флаги операции загрузки образа	unsigned	ldf	Процессы
Флаги образа	int64	imgf	Процессы
Базовый адрес образа	int64	base	Процессы
Размер образа	unsigned	isize	Процессы
Идентификатор целевой нити	unsigned	tid	Процессы
Стартовый адрес целевой нити	int64	taddr	Процессы
Запрашиваемые права	unsigned	dsrd	Процессы
Предоставленные права	unsigned	grnt	Процессы
Новый уровень защиты процесса	int	prot1	Процессы
Новая командная строка	string	cmdl1	Процессы
Идентификатор контейнера целевого процесса (только для агентов Linux)	string	container	Процессы
AMSI: имя содержимого	string	amsi_cname	Процессы
AMSI: содержимое	string	amsi_data	Процессы
AMSI: имя приложения	string	amsi_appname	Процессы
AMSI: ссылка на скачивание зарезервированного содержимого	string	amsi_blink	Процессы
Локальная сессия (принимает значения true или false)	int (0/1)	local	Сессии
Номер сессии	unsigned	sess_id	Сессии
Тип дистанционного управления	unsigned (опционально)	sess_opt	Сессии
Тип сессии	unsigned (опционально)	sess_proto	Сессии
Имя оконной станции	string	win_stn	Сессии
Имя клиента	string (опционально)	sess_cl	Сессии
IP-адрес клиента	string (опционально)	sess_claddr	Сессии
Имя пользователя	string (опционально)	sess_usr	Сессии
Имя домена\компьютера	string (опционально)	sess_dom	Сессии
Путь ключа	string	key	Реестр
Имя значения	string	val_n	Реестр
Тип данных значения	enum	val_t	Реестр
Размер данных значения	unsigned	val_s	Реестр
Данные значения	string	val_d	Реестр
Новое имя ключа	string	new	Реестр
Имя файла-источника загружаемой в реестр информации	string MANGLED	src	Реестр
Имя файла, в который записываются данные из реестра	string MANGLED	dst	Реестр
Ключ/значение относится к категории автозапуска (принимает значение только true)	int (-/1)	asep	Реестр

Назначение	Тип данных	JSON	Подсистема
WMI: Тип события	enum	wmi	Система: WMI
WMI: Путь	string	wmi_pth	Система: WMI
WMI: SID пользователя	string	wmi_sid	Система: WMI
WMI: Пространство имен	string	ns	Система: WMI
WMI: Путь до исполняемого файла	string MANGLED	exe_path	Система: WMI
WMI: Имя файла	string MANGLED	fname	Система: WMI
WMI: Имя фильтра событий	string	wmi_nm	Система: WMI
WMI: Строка запроса	string	qstr	Система: WMI
WMI: Имя файла скрипта	string MANGLED	scrfname	Система: WMI
WMI: Текст скрипта	string	scrtxt	Система: WMI
WMI: Имя источника	string MANGLED	sname	Система: WMI
WMI: SMTP	string	smtp	Система: WMI
WMI: Фильтр	string	flt	Система: WMI
WMI: Потребитель	string	cnsm	Система: WMI
WMI:Идентификатор процесса клиента	unsigned (по умолчанию 0)	wmi_clpid	Система: WMI
WMI: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	wmi_cluuid	Система: WMI
WMI: Время создания процесса клиента	timestamp	wmi_cltime	Система: WMI
WMI: Командная строка процесса клиента	string	wmi_clcmdl	Система: WMI
WMI: Локальный запрос (принимает значение только true)	int (-/1)	wmi_local	Система: WMI
WMI: Идентификатор созданного процесса	unsigned	wmi_crpid	Система: WMI
WMI: Уникальный идентификатор созданного процесса	int (индекс в массиве GUID'ов)	wmi_cruuid	Система: WMI
WMI: Время создания созданного процесса	timestamp	wmi_crtime	Система: WMI
WMI: Командная строка созданного процесса	string	wmi_crcmdl	Система: WMI
WMI: Имя машины, выполнившей запрос	string	wmi_cl	Система: WMI
WMI: FQDN машины, выполнившей запрос	string	wmi_clfqdn	Система: WMI
WMI: Имя пользователя клиента, выполнившего запрос	string	wmi_usr	Система: WMI
WMI: Имя домена клиента, выполнившего запрос	string	wmi_dom	Система: WMI
WMI: Имя вызываемого метода	string	wmi_mthd	Система: WMI
Новое время	timestamp	new_stime	Система: Изменение системного времени

Назначение	Тип данных	JSON	Подсистема
Предыдущее время	timestamp	prev_stime	Система: Изменение системного времени
Причина завершения	unsigned	sht	Система: Завершение работы
Уровень	unsigned	e_lvl	Журналы
Дополнительные данные	JSON object	e_ex	Журналы
Описание событий	string (опционально)	e_msg	Журналы
Блок информации **winlogbeat**	JSON object	winlog	Журналы
RPC: UUID интерфейса	int (индекс в массиве GUID'ов)	rpc_id	Вызовы: RPC
RPC: Номер процедуры	unsigned	rpc_opnum	Вызовы: RPC
RPC: Имя процедуры	string	rpc_opname	Вызовы: RPC
RPC: Протокол	unsigned	rpc_proto	Вызовы: RPC
RPC: Сервис аутентификации	unsigned	rpc_authsvc	Вызовы: RPC
RPC: Конечная точка	string	endp	Вызовы: RPC
RPC: Сетевой адрес	string (опционально)	n_addr	Вызовы: RPC
RPC: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	c_uuid	Вызовы: RPC
RPC: PID процесса клиента	unsigned	c_pid	Вызовы: RPC
RPC: Исполняемый файл процесса клиента	string MANGLED	c_path	Вызовы: RPC
RPC: Уникальный идентификатор процесса сервера	int (индекс в массиве GUID'ов)	s_uuid	Вызовы: RPC
RPC: PID процесса сервера	unsigned	s_pid	Вызовы: RPC
RPC: Исполняемый файл процесса сервера	string MANGLED	s_path	Вызовы: RPC
Количество открытий/созданий файлов с последующими обращениями к ним	unsigned	cf_ac	Защита файлов
Количество открытых файлов из защищаемых каталогов	unsigned	cf_oc	Защита файлов
Количество созданных процессом файлов после активации мониторинга	unsigned	cf_cc	Защита файлов
Количество удалённых файлов в защищаемых каталогах	unsigned	si_dc	Защита файлов
Количество переименованных файлов в защищаемых каталогах	unsigned	si_rc	Защита файлов
Количество перемещённых файлов в защищаемые каталоги	unsigned	si_mi	Защита файлов
Количество перемещённых файлов из защищаемых каталогов	unsigned	si_mo	Защита файлов

Назначение	Тип данных	JSON	Подсистема
Количество файлов из защищаемых каталогов, которые только читали	unsigned	ro_fc	Защита файлов
Количество файлов из защищаемых каталогов, в которые только писали	unsigned	wo_fc	Защита файлов
Количество файлов из защищаемых каталогов, которые читали и писали	unsigned	rw_fc	Защита файлов
Среднее значений файловой энтропии по чтению	unsigned	pr_re	Защита файлов
Среднее значений файловой энтропии по записи	unsigned	pr_we	Защита файлов
Правило блокировки процесса	unsigned	pr_lr	Защита файлов
Реакция модуля на идентификацию шифровальщика	unsigned	pr_ra	Защита файлов
Количество файлов с нарушенной целостностью	unsigned	a_fcc	Защита файлов
Количество файлов с превышенной энтропией	unsigned	a_eoc	Защита файлов
Количество расширений файлов, из которых читали	unsigned	exrac_	Защита файлов
Количество расширений файлов, в которые писали	unsigned	exwac_	Защита файлов
Количество уникальных расширений файлов, из которых только читали	unsigned	exurac	Защита файлов
Количество уникальных расширений файлов, в которые только писали	unsigned	exuwac	Защита файлов
Категории файлов, к которым осуществлялся доступ	unsigned	gf_am	Защита файлов
Категории файлов, из которых производилось чтение	unsigned	gf_rm	Защита файлов
Категории файлов, в которые производилась запись	unsigned	gf_wm	Защита файлов
Категории файлов, которые удалялись	unsigned	gf_dm	Защита файлов
Группа, к которой относится файл	unsigned	gf_ai	Защита файлов
Тип контролируемого устройства	unsigned	usb_dt	Контроль USB-устройств
Класс устройства	unsigned	usb_dc	Контроль USB-устройств
Подкласс устройства	unsigned	usb_dsc	Контроль USB-устройств
Идентификатор производителя	unsigned	usb_vid	Контроль USB-устройств
Идентификатор продукта	unsigned	usb_pid	Контроль USB-устройств

Назначение	Тип данных	JSON	Подсистема
Номер интерфейса	unsigned (опционально)	usb_mi	Контроль USB-устройств
Серийный номер	string	usb_sn	Контроль USB-устройств
Наименование производителя	string	usb_mr	Контроль USB-устройств
Наименование продукта	string	usb_pt	Контроль USB-устройств
Имя модуля, который был запущен с носителя	string	usb_exec	Контроль USB-устройств



Примечание

(-/1) в таблице обозначает, что событие можно будет найти в DSL-запросе, только если такое событие придет в базу данных, то есть будет содержать значение **true**.

Типы событий представлены в таблице 8.

Таблица 8 – Типы событий (t)

Код типа	Описание типа
0	Сеть
1	Файлы
2	Реестр
3	Журналы
4	Процессы
5	Система
6	Сессии
7	Вызовы
8	Защита файлов
9	Контроль USB

Поля общей части событий представлены в таблице 9.

Таблица 9 – Поля общей части событий

Назначение	JSON	Тип
Тип события	t	unsigned
Время регистрации события (в формате UTC)	time	timestamp

Назначение	JSON	Тип
Действие, связанное с событием (0 – блокировать, 1 – разрешить, 2 – продолжить наблюдение)	act (по умолчанию – 2)	unsigned
Причина предпринятого действия	rsn	unsigned
Правило, относящееся к событию	rul	string
Идентификатор техники/тактики MITRE	mitre	string
Критичность (уровень важности) события	**svrt** (по умолчанию – 0)	unsigned
Уникальный идентификатор процесса	uuid	int (индекс в массиве GUID'ов)
Уникальный идентификатор группы процессов	hid	string (индекс в массиве GUID'ов)
Уникальный идентификатор корреляции событий	cid	string (индекс в массиве GUID'ов)
Идентификатор процесса на агентской системе	pid	unsigned
Идентификатор родительского процесса на агентской системе	ppid	unsigned
Полное имя (вместе с путем) исполняемого модуля процесса	app	string MANGLED
Командная строка процесса	cmdl	string (index string 2650+)
Номер сессии, в которой работает процесс на агентской системе	**sess** (по умолчанию – 0)	unsigned
SID пользователя, запустившего процесс	sid	string
Издатель ЭП исполняемого файла процесса	app_sgnr	string
Имя пользователя, запустившего процесс	usr	string
Домен (имя компьютера) пользователя, запустившего процесс	dom	string
Подтип события (интерпретируется в зависимости от типа)	st	unsigned
Поведенческие признаки процесса (первая группа)	rf0	uint64
Поведенческие признаки процесса (вторая группа)	rf1	uint64
Флаги исполняемого файла процесса	exclf	uint64
Синтетическое событие (0 или 1)	syn	int (0/1)
Версия события	efmt	unsigned

В поле **time** передается UTC-время регистрации события. Система построена таким образом, что в штатной ситуации в пределах одного агента не бывает событий с одинаковым значением поля **time**. Если события зарегистрированы в одно и то же время, то между ними вносится временной сдвиг, который для последующих событий компенсируется за счет естественного течения времени.

В поле **svrt** (severity) передается критичность события.

Критичность события может принимать следующие значения:

1) **NORMAL** (код 0, значение по умолчанию) — информация ("зеленый", нет угрозы);
2) **GUARDED** (код 1) – низкая/пограничная ("серый", малой степени вероятная угроза);
3) **ELEVATED** (код 2) – средняя/повышенная ("синий", средней степени вероятная угроза);
4) **HIGH** (код 3) – высокая ("оранжевый", вероятная угроза);
5) **SEVERE** (код 4) – критичная ("красный", максимальной степени вероятная угроза).



Примечание

Критичность также можно трактовать следующим образом: NORMAL – телеметрия, GUARDED – информирующие обнаружения (informational alerts), ELEVATED+ – обнаружения (alerts). Предполагается, что аналитик работает преимущественно с обнаружениями, редко обращаясь к информирующим обнаружениям и крайне редко – к телеметрии.

В поле **act** (action) передается действие, предпринятое в связи с событием. Это может быть одно из трех значений:

BLOCK (код 0) – блокирование. Означает, что в контексте события сработала какая-то логика («черный» список, эвристическое правило, политика и т.п.), и в результате то или иное действие было заблокировано. При этом поля **rsn** (reason – причина) и **rul** (правило) будут содержать информацию, определяющую, почему принято блокирующее решение.

ALLOW (код 1) – разрешение. Означает, что в контексте события сработала какая-то логика («белый» список, эвристическое правило, политика и т.п.) и в результате то или иное действие было разрешено. Поля **rsn** и **rul** в этом случае содержат информацию, показывающую, почему принято разрешающее решение.

MORE_PROCESSING (код 2, значение по умолчанию, т.е. непосредственно в теле события этот код не передается) – трактуется по-разному в зависимости от контекста. В контексте события телеметрии означает, что никакого действия, связанного с событием, не предпринято. В контексте обнаружения (alert) код 2 означает, что логика обнаружения не предписывает никакого действия, кроме фиксации самого факта обнаружения – обнаруженная активность не блокируется, что не отменяет самого факта ее обнаружения. Для события телеметрии поля **rsn** и **rul**, как правило (но необязательно), не заполняются, а для события-обнаружения поле

rul содержит правило, идентифицирующее обнаружение. И тогда поле **rsn**, как и в других случаях, содержит причину, по которой установлена такая реакция на обнаружение.

Поле **mitre** заполняется, если событие соответствует какой-то технике/тактике MITRE. Одно событие может соответствовать сразу нескольким элементам MITRE, в этом случае техники/тактики перечисляются через запятую, например, «T1490, T1047/001».

Поля **pid**, **ppid**, **uuid**, **app**, **sess**, **usr**, **dom** определяют приложение (процесс), ассоциированный с событием. Поле **pid** содержит системный ID процесса, **ppid** – системный ID его родителя, **uuid** – индекс элемента в массиве **uuids** заголовка блока событий (см. выше), определяющий внутренний уникальный ID процесса (предназначен для внутреннего использования), **app** – полное имя файла процесса вместе с путем, **sess** (session) – номер сессии процесса (по умолчанию 0), **usr** (user) – имя пользователя, от имени которого работает процесс, **dom** (domain) – домен/имя компьютера пользователя, от имени которого запущен процесс.

Поля **rf0**, **rf1** определяют поведенческий профиль процесса. Поле **rf0** – это runtime-флаги процесса (первая группа); **rf1** – runtime-флаги процесса (вторая группа). Флаги в явном виде не отображаются, а используются для удобочитаемого представления поведенческого профиля процесса. Поведенческие признаки процесса могут меняться от события к событию сообразно с поведением процесса в системе.

Поле **st** определяет подтип события в рамках определенной подсистемы.

Поле **app**, а также другие поля событий, в которых присутствуют пути, могут быть декорированы (mangled). Декорация заключается в замене известного префикса пути его кодом. У декорированных путей в начале следует один или несколько компонентов, кодирующих заранее определенные подстроки, затем следует недекорированный остаточный путь.

Поле **syn** устанавливается в 1, если событие, которое в обычной ситуации отражает реально имеющую место активность агента, в данном конкретном случае является синтезированным, т.е. исскуственным. Например, если агентский модуль деактивируется, то он публикует синтетические события завершения процессов системы, за которыми он наблюдает и для которых были отправлены события старта процесса. И наоборот, при запуске агентского модуля "на лету" сразу после установки (или его активации после деактивации), когда в системе уже работают те или иные процессы, агент публикает синтетические события создания этих процессов. Это позволяет сохранять целостную картину состояния агентской системы с точки зрения административного модуля в разных сценариях работы агента.

Поле **efmt** (версия события) содержит номер сборки агента, который сформировал данное событие.

Предусматривается 2 схемы декорирования (см. таблицы 10 и 11).

Таблица 10 – Декорируются стандартные префиксы путей

Путь	Заменяется на
\Device\HarddiskVolume1\Windows	*0
\Device\HarddiskVolume1\Windows\System32\	*1
\Device\HarddiskVolume1\Windows\SysWOW64\	*2
\Device\HarddiskVolume1\Program Files\	*3
\Device\HarddiskVolume1\Program Files (x86)\	*4
\Device\HarddiskVolume1\ProgramData\Microsoft\	*5

Пример: \device\harddiskvolume1\windows\system32\kernel32.dll декорируется в *1\kernel32.dll.

Таблица 11 – Декорирование первых 2-х компонент пути

Путь	Заменяется на
\Device\HarddiskVolumeX\	?X\
\Device\HarddiskVolumeX\Windows\	?X*0\
\Device\HarddiskVolumeX\Windows\System32\	?X*1\
\Device\HarddiskVolumeX\Windows\SysWOW64\	?X*2\
\Device\HarddiskVolumeX\Program Files\	?X*3\
\Device\HarddiskVolumeX\Program Files (x86)\	?X*4\
\Device\HarddiskVolumeX\ProgramData\Microsoft\	?X*5\

X - символ 0-9.

Пример: \device\harddiskvolume5\programdata\microsoft\Office\AssetLibrary.ico декорируется в ?5*5\Office\AssetLibrary.ico.

Синтаксис декорирования таков, что при обратном декорировании позволяет однозначно идентифицировать схему декорирования.

9.2 События мониторинга сети

При любых сетевых взаимодействиях и проверках, которые осуществляются между агентом и удаленным компьютером, будь то матчинг индикаторов атак, индикаторов компрометации, в сетевых

исключениях и т.д. важен прежде всего удаленный хост, его имя, IP-адрес и порт, то есть на него идет основное внимание в момент сетевого соединения.

Подтипы событий (**st**) и их текстовые описания представлены в таблице 12.

Таблица 12 – События монитора сети

Код события	Имя события	Описание
0	Сеть: Исходящее подключение	Исходящее подключение к удаленному хосту (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
1	Сеть: Входящее подключение	Входящее подключение к порту **l_p** от удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
16	Сеть: Завершение сетевого подключения	Завершение исходящего подключения к удаленному хосту заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto** или 2. Завершение входящего подключения к порту l_p от удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
2	Сеть: Отправка	Отправка **size** байт на удаленный хост (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
3	Сеть: Прием	Прием **size** байт на порт **l_p** от удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
5	Сеть: DNS запрос	DNS-запрос **dnsq_t** к удаленному хосту (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) на имя **dnsq_h** размером **size** байт
11	Сеть: DNS-ответ	DNS-ответ со статусом dnsq_s на запрос dnsq_t к удаленному хосту на имя **dnsq_h** размером **size** байт, результат – **dnsq_r** (ответ может не выводиться)
13	Сеть: Входящий DNS запрос	DNS-запрос **dnsq_t** от **%remote_endpoint%** на имя **dnsq_h** размером **size** байт
14	Сеть: Исходящий DNS-ответ	DNS-ответ со статусом **dnsq_s** на запрос **dnsq_t** от **%remote_endpoint%** на имя **dnsq_h** размером **size** байт, результат: **dnsq_r** (ответ может не выводиться)
6	Сеть: SSL HELLO	SSL HELLO (**ssl_h**) с удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) размером **size** байт
7	Другие обнаружения*	Расшифровка кода **detect**
8	Обнаружение: срабатывание индикатора компрометации*	Срабатывание индикатора компрометации при сетевом взаимодействии с удаленным хостом (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p)**
10	Сеть: Открытие локального порта на прием (LISTEN)	Открытие локального порта **l_p** на прием
15	ICMP-сообщение	ICMP-сообщение типа icmp_t (код icmp_c)

События, отмеченные значком * отправляются на сервер только в формате обнаружений (st>50), **%remote_endpoint%** заменяется на **host (r_ip:r_p)** если заполнено поле **host**, иначе на **r_ip:r_p**.

Поля сетевых событий представлены в таблице 13.

Таблица 13 – Поля сетевых событий

Назначение	JSON	Тип
Полное имя исполняемого модуля–инициатора операции	who	string MANGLED
Идентификатор нити–инициатора операции	whotid	unsigned
Стартовый адрес нити–инициатора операции	whoaddr	uint64
Флаги исполняемого модуля–инициатора операции	whof	uint64
Исключения для программ, назначенные инициатору операции	who_excls	string
Стек вызовов операции	trace	string
Номер протокола 6 – TCP, 17 – UDP, 1 – ICMP, 58 – ICMPv6	proto	unsigned
Признак работы по IPv6 (принимает значения true или false)	ipv6	int (0/1)
Идентификатор сетевого потока (служебное значение, позволяет группировать события, относящиеся к одному сетевому потоку)	flow	int64
Уникальный идентификатор сетевого потока	fluuid	string (индекс в массиве GUID'ов в текст. форме)
Отправка (1) или прием (0)	out	int (0/1)
Размер полезных данных (payload) сетевого пакета	size	int64
Имя хоста, соответствующее удаленному IP	host	string
Тип DNS запроса: 0x1 – A, 0x5 – CNAME, 0x1C – AAAA, 0x0F – MX, 0x21 – SRV, 0x0C – PTR, 0x41 HTTPS. Остальные типы запросов выводятся кодом (2 байта), пример: 0x0002	dnsq_t	unsigned
Имя хоста из DNS-запроса	dnsq_h	string
Статус DNS-запроса	dnsq_s	unsigned
Результат DNS-запроса	dnsq_r	string
Идентификатор транзакции DNS-обмена	dns_trx	unsigned
Имя хоста (server_name) из SSL Client Hello сообщения	ssl_h	string
Удаленный IP-адрес	r_ip	string
Удаленный порт	r_p	unsigned
Локальный IP-адрес	l_ip	string
Локальный порт	l_p	unsigned
Флаги сетевого события	netf	unsigned
Исключение для удаленного IP-адреса	r_ip_excl	string
Исключение для имени хоста, соответствующего удаленному IP-адресу	h_excl	string
Исключение для имени хоста в запросе	rqh_excl	string
Код обнаружения	detect	unsigned
Тип ICMP-сообщения	icmp_t	unsigned

Назначение	JSON	Тип
Код ICMP-сообщения	icmp_c	unsigned
Имя хоста в индикаторе компрометации	loc_h	string
Общий размер исходящих данных за время жизни подключения, байт	o_sz	uint64
Общий размер входящих данных за время жизни подключения, байт	i_sz	uint64
Время жизни подключения, в 100-наносекундных интервала	lt	uint64

Тип DNS-запроса — это параметр в DNS-сообщении, который указывает, какую именно информацию хочет получить клиент (например, браузер) от DNS-сервера. Проще говоря, это вопрос, который клиент задает DNS-серверу. Вопросы бывают разные: «Какой IP-адрес у этого домена?», «Какой почтовый сервер его обслуживает?» и так далее. Тип запроса как раз и определяет, какой именно вопрос задается.

SSL ClientHello — это первое и одно из самых важных сообщений в процессе установления безопасного (шифрованного) соединения по протоколу SSL (например, когда вы заходите на сайт по HTTPS), в процессе которого выполняются следующие шаги:

1) Приветствие с сервером;

2) Сообщение о своих возможностях (версии протокола, шифры);

3) Просьба об установлении безопасного соединения для конкретного сайта;

4) Начало процесса генерации уникальных ключей шифрования для текущего сеанса.

ICMP (Internet Control Message Protocol) — это вспомогательный протокол в составе сетевого стека TCP/IP. Его главная задача — обмен служебной информацией между сетевыми устройствами (маршрутизаторами, серверами, обычными хостами) для диагностики проблем и управления передачей данных.

9.3 События мониторинга файловых операций

Подтипы событий (**st**) мониторинга файловых операций и их текстовые описания представлены в таблице 14.

Таблица 14 – События мониторинга файловых операций

Код события	Имя события	Описание
0	Файлы: Создан новый файл	Создан новый файл **name**
1	Файлы: Файл переименован	Файл **name** переименован в **fnew**

Код события	Имя события	Описание
2	Файлы: Удален файл	Удален файл **name**
3	Файлы: У файла изменен атрибут или время создания	У файла **name** [установлен/снят атрибут "системный" (если присутствует **sys**, **sys** = 0, то снят, **sys** = 1 - установлен)], [установлен атрибут "скрытый" (если присутствует **hdn**)], [изменено время создания с **old_t** на **new_t** (если присутствуют **old_t** и **new_t**)]
4	Файлы: Другие обнаружения*	<Описание кода **detect**>
7	Файлы: Файл был модифицирован	Файл **name** был модифицирован (запись файла)
8	Файлы: Файл был прочитан	Файл **name** был прочитан
12	Файлы: Прямой доступ к тому на чтение	Прямой доступ к диску (тому) **name** на чтение
13	Файлы: Прямой доступ к тому на запись	Прямой доступ к диску (тому) **name** на запись
14	Файлы: Создан именованный канал	Создан именованный канал **name**
15	Файлы: Подключение к именованному каналу	Подключение к именованному каналу **name**
16	Файлы: Обнаружение: доступ к файлу	Доступ к файлу **name**
17	Файлы: Обнаружение: срабатывание индикатора компрометации для файла*	Срабатывание индикатора компрометации для файла **name**
19	Файлы: Обнаружение: файл классифицирован как вредоносный (ML на агенте)*	Файл **name** классифицирован как вредоносный (ML на агенте)
20	Файлы: Обнаружение: файл классифицирован как вредоносный (Yara-правила)*	Файл **name** классифицирован как вредоносный (Yara-правила)
22	Файлы: Создан альтернативный поток для файла	Создание альтернативного поток **strm** для файла **name**
23	Файлы: Создан файл с потенциально аткивным содержимым	Создан файл **name** с потенциально активным содержимым
24	Файлы: Модифицирован файл с потенциально активным содержимым	Модифицирован файл **name** с потенциально активным содержимым

События, отмеченные значком *, отправляются на сервер только в формате обнаружений (st>50).

Поля событий мониторинга файловой системы представлены в таблице 15.

Таблица 15 – Поля событий мониторинга файловой системы

Назначение	JSON	Тип
Полное имя исполняемого модуля-инициатора операции	who	string MANGLED
Идентификатор нити-инициатора операции	whotid	unsigned
Стартовый адрес нити-инициатора операции	whoaddr	uint64
Флаги исполняемого модуля-инициатора операции	whof	uint64
Исключения для программ, назначенные инициатору операции	who_excls	string
Стек вызовов операции	trace	string
Полное имя файла	name	string MANGLED

Время создания файла	crtime	timestamp
Время последнего изменения файла	chtime	timestamp
Размер файла	fsize	int64
Тип файла	ftype	enum
Атрибуты файла	attr	unsigned
SHA-1 файла	sha1	string
MD5 файла	md5	string
SHA-256 файла	sha256	string
Imphash файла	imphash	string
Электронная подпись файла	sgnr	string
Статус электронной подписи файла	sgnr_s	enum
Оригинальное имя файла	ofn	string
Компания-издатель файла	fcomp	string
Версия файла	fver	string
Описание файла	fdesc	string
Продукт, к которому относится файл	fprod	string
Файл находится в белом списке	fwhite	int (-/1)
Тип упаковщика файла	pack	string
Файл расположен в директории автозапуска	arun	int (-/1)
Новое имя файла	fnew	string MANGLED
Файл был заменен	owrt	int (-/1)
Время создания файла до изменения атрибутов	old_t	timestamp
Время создания файла после изменения атрибутов	new_t	timestamp
Файл содержит атрибут "скрытый"	hdn	int (0/1)
Файл содержит атрибут "системный"	sys	int (0/1)
Операция совершается над альтернативным потоком данных файла	ads	int (-/1)
Код обнаружения	detect	unsigned
Доступ на удаление	delete	int (-/1)
Доступ на чтение	read	int (-/1)
Доступ на модификацию	modify	int (-/1)
Обмен именами (доступен только в Linux)	nxchg	int (-/1)
Имя альтернативного потока данных файла	strm	string
Исключение для файла по хешу	fh_excl	string
Исключение для файла по имени	fn_excl	string
SID предыдущего владельца файла	own_old	string
Домен предыдущего владельца файла	own_old_dom	string
Имя предыдущего владельца файла	own_old_usr	string
Предыдущий владелец файла был задан по умолчанию	own_old_def	int (-/1)
SID нового владельца файла	own_new	string
Домен нового владельца файла	own_new_dom	string

Имя нового владельца файла	own_new_usr	string
Новый владелец файла был задан по умолчанию	own_new_def	int (-/1)
SID предыдущей основной группы владельца файла	grp_old	string
Домен предыдущей основной группы владельца файла	grp_old_dom	string
Имя предыдущей основной группы владельца файла	grp_old_usr	string
Предыдущая основная группа владельца файла была задана по умолчанию	grp_old_def	int (-/1)
SID новой основной группы владельца файла	grp_new	string
Домен новой основной группы владельца файла	grp_new_dom	string
Имя новой основной группы владельца файла	grp_new_usr	string
Новая основная группа владельца файла была задана по умолчанию	grp_new_def	int (-/1)
Предыдущий DACL файла	dacl_old	string
Предыдущий DACL файла был задан по умолчанию	dacl_old_def	int (-/1)
Новый DACL файла	dacl_new	string
Новый DACL файла был задан по умолчанию	dacl_new_def	int (-/1)
Предыдущий SACL файла	sacl_old	string
Предыдущий SACL файла был задан по умолчанию	sacl_old_def	int (-/1)
Новый SACL файла	sacl_new	string
Новый SACL файла был задан по умолчанию	sacl_new_def	int (-/1)
Предыдущая мандатная метка файла	mlbl_old	unsigned
Предыдущая маска мандатной метки файла	mlbl_old_mask	unsigned
Новая мандатная метка файла	mlbl_new	unsigned
Новая маска мандатной метки файла	mlbl_new_mask	unsigned

Поле **ftype** принимает следующие значения, представленные в таблице 16.

Таблица 16 – Значение поля ftype

Значение	Описание
2	PE
3	Active content
4	PowerShell script

Если было получено значение, отсутствующее в таблице, отображается только его значение (например, **Тип файла: 1**).

Поле **sgnr_s** (статус электронной подписи) событий мониторинга файлов и процессов может принимать следующие значения:

– 0 (нет подписи);

– 1 (есть подпись);

– 2 (неизвестно).



Примечание

Список всех возможных атрибутов файлов для ОС Windows содержится в документации Microsoft.

Альтернативный поток данных файла (ADS) – это специальная возможность файловой системы NTFS в Windows, позволяющая хранить дополнительную информацию в виде отдельного скрытого «потока» внутри обычного файла.

DACL (Discretionary Access Control List) — это список управления доступом, который определяет, кто и какие действия может выполнять с объектом (файлом, папкой, разделом реестра и т.д.) в операционных системах Windows.

SACL (System Access Control List) — это список управления доступом для аудита, который определяет, какие попытки доступа к файлу или папке нужно регистрировать в журнале событий Windows (Event Log).

Мандатная метка файла — это специальный атрибут, который присваивается файлу для определения уровня его секретности (конфиденциальности) и категорий информации, которые он содержит. В отличие от прав доступа (как в DACL), которые определяются владельцем файла, мандатная метка назначается системой или администратором безопасности и является принудительной. Пользователь не может по своему желанию изменить её или проигнорировать.

9.4 События монитора реестра

Подтипы событий (**st**) мониторинга реестра и их текстовые описания представлены в таблице 17.

Таблица 17 – Подтипы событий мониторинга реестра

Код события	Имя события	Описание
0	Реестр: Создан новый ключ	Создан новый ключ **key**
1	Реестр: Удален ключ	Удален ключ **key**
2	Реестр: в значение ключа записаны данные	В значение **val_n** ключа **key** записаны данные **val_d** (тип: **val_t**, размер: **val_s**)
3	Реестр: Удалено значение ключа	Удалено значение **val_n** ключа **key**

Код события	Имя события	Описание
4	Реестр: Ключ переименован	Ключ **key** переименован в **new**
5	Реестр: Ключ восстановлен из файла	Ключ **key** восстановлен из файла **src**
6	Реестр: Данные ключа заменены файлом	Данные ключа **key** заменены файлом **src**
7	Реестр: Другие обнаружения*	Описание поля **detect**

События, отмеченные значком *, отправляются на сервер только в формате обнаружений (st>50).

Поля событий монитора реестра представлены в таблице 18.

Таблица 18 – Поля событий мониторинга реестра

Назначение	JSON	Тип
Полное имя исполняемого модуля-инициатора операции	who	string MANGLED
Идентификатор нити-инициатора операции	whotid	unsigned
Стартовый адрес нити-инициатора операции	whoaddr	uint64
Флаги исполняемого модуля-инициатора операции	whof	uint64
Исключения для программ, назначенные инициатору операции	who_excls	string
Стек вызовов операции	trace	string
Путь ключа реестра	key	string
Имя значения	val_n	string
Тип данных значения: 1 – REG_SZ; 2 – REG_EXPAND_SZ; 3 – REG_BINARY; 4 – REG_DWORD; 5 – REG_DWORD_BE; 6 – REG_LINK; 7 – REG_MULTI_SZ; 8 – REG_RES_LIST; 9 – REG_FULL_RES_DESC; 10 – REG_RES_REQ_LIST; 11 – REG_QWORD	val_t	unsigned
Размер данных значения	val_s	unsigned
Данные значения	val_d	string
Новое имя ключа	new	string
Имя файла-источника загружаемой в реестр информации	src	string MANGLED
Ключ/значение относится к категории автозапуска	asep	int (-/1)
Код обнаружения	detect	unsigned

Поле **asep** принимает значение **true**.

Autostart Extensibility Points (ASEP) — это механизмы в операционных системах (в частности, Windows), которые позволяют программам, службам, драйверам или скриптам автоматически запускаться при загрузке системы, входе пользователя или выполнении определенных условий. Они играют ключевую роль в обеспечении функциональности и удобства, но также представляют значительный риск для информационной безопасности, поскольку часто используются злоумышленниками для закрепления вредоносного ПО в системе.

9.5 События журналов

Подтипы событий журналов и их текстовые описания представлены в таблице 19.

Таблица 19 – Подтипы событий журналов (st)

Код события	Имя события	Описание
0	WINLOGBEAT_EVENT	Событие журнала
1	FILEBEAT_EVENT	Строка лог-файла

Поля событий журнала и их текстовые описания представлены в таблице 20.

Таблица 20 – Поля событий журнала (st=0)

Назначение	JSON	Тип
Подтип события	st	unsigned
Уровень (возможно значение: Критическая ошибка = 1, Ошибка = 2, Предупреждение = 3, Информация = 4, Подробно = 0 или 5)	e_lvl	unsigned
Дополнительные данные (выводятся в поле карточки событий в JSON-формате)	e_ex	string (опционально)
Описание события	e_msg	string (опционально)
ID события	e_id	unsigned
ID провайдера	e_prv_id	unsigned (индекс в массиве GUID'ов) (опционально)
Провайдер	e_prv	string
Имя канала	e_chn	string
Событие в формате winlogbeat (см. winlogbeat), является JSON-объектом	winlog	JSON-объект

События формата winlogbeat могут принимать значения, представленные в таблице 21.

Таблица 21 – События winlogbeat

Поле	Тип	Расшифровка
winlog.api	keyword	Тип API
winlog.event_id	keyword	Идентификатор события
winlog.activity_id	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор действия
winlog.related_activity_id	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор действия, которому было передано управление
winlog.computer_name	keyword (опционально)	Имя компьютера
winlog.keywords	keyword (опционально)	Ключевые слова

Поле	Тип	Расшифровка
winlog.channel	keyword (опционально)	Имя канала
winlog.record_id	keyword	Номера записи
winlog.opcode	keyword (опционально)	Код операции
winlog.provider_guid	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор провайдера
winlog.provider_name	keyword (опционально)	Имя провайдера
winlog.process.pid	long (опционально)	Идентификатор процесса
winlog.task	keyword (опционально)	Имя задачи
winlog.time_created	date (опционально) (ISO 8601)	Дата и время создания события
winlog.process.thread.id	long (опционально)	Идентификатор нити
winlog.user.identifier	keyword (опционально)	SID пользователя
winlog.user.name	keyword (опционально)	Имя пользователя
winlog.event_data	json_object (опционально) (набор полей отличаются от провайдера к провайдеру, все поля должны иметь тип: keyword)	Поля события
winlog.user_data	json_object (опционально) (набор полей отличаются от провайдера к провайдеру, все поля должны иметь тип: keyword)	Пользовательские поля события



Примечание

Подробное логирование предоставляет максимальную видимость процессов в системе, но требует значительных ресурсов, поэтому желательно его включать для критических компонентов, например, Windows Defender, сетевых служб, это позволит грамотно использовать ресурсы системы.

Описание полей события строки лог-файла (**st = 1**) представлено в таблице 22.

Таблица 22 – Поля события строки лог-файла

Назначение	JSON	Тип
Строка log-файла	message	string
Блок информации filebeat	log	JSON-объект

События формата filebeat могут принимать значения, представленные в таблице 23

Таблица 23 – События формата filebeat

Поле	Тип	Расшифровка
log.offset	long	Смещение строки в лог-файле
log.file.path	string	Имя лог-файла

9.6 События мониторинга процессов

Подтипы событий и их текстовые описания представлены в таблице 24.

Таблица 24 – Подтипы событий мониторинга процессов и их тестовые описания

Код события	Имя события	Описание
0	Процессы: Загрузка драйвера	Загрузка драйвера **path**
1	Процессы: Старт процесса	Старт процесса командой **cmdl** из **cpath** (**cpid**), нить = **whotid** (из модуля **who**)
2	Процессы: Завершение процесса	Завершение процесса с кодом **code**
3	Процессы: Загрузка образа	Загрузка образа **path**
6	Процессы: Доступ к процессу	Доступ к процессу **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd-grnt**}, нить=**whotid** (из модуля **who**)
7	Процессы: Создание нити в стороннем процессе	Создание нити **tid** в процессе **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
13	Процессы: Обнаружение: подмена командной строки*	Подмена командной строки с **cmdl1** на **cmdl**
16	Процессы: Обнаружение: изменение системной защиты процесса*	Изменение системной защиты процесса с **prot** на **prot1**
18	Процессы: Доступ к нити процесса	Доступ к нити **tid** процесса **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd-grnt**}, нить = **whotid** (из модуля **who**)
20	Процессы: Загрузка образа в сторонний процесс	Загрузка образа **path** в процесс **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
23	Процессы: Другие обнаружения*	Описание кода **detect**
22	Уведомление модуля Antimalware Scan Interface Windows	Уведомление модуля Antimalware Scan Interface Windows: содержимое **amsi_cname** размером **fsize**, хеш sha256

События, отмеченные значком *, отправляются на сервер только в формате обнаружений (st>50).

Поля событий мониторинга процессов представлены в таблице 25.

Таблица 25 – Поля событий мониторинга процессов

Назначение	JSON	Тип
Полное имя исполняемого модуля–инициатора операции	who	string MANGLED
Идентификатор нити–инициатора операции	whotid	unsigned

Назначение	JSON	Тип
Стартовый адрес нити–инициатора операции	whoaddr	uint64
Флаги исполняемого модуля–инициатора операции	whof	uint64
Исключения для программ, назначенные инициатору операции	who_excls	string
Командная строка родительского процесса	cmdlp	string
Электронная подпись родительского процесса	sgnrp	string
Командная строка прародителя (grand parent)	cmdlg	string
Рабочий каталог процесса	wdir	string MANGLED
Уровень защиты процесса	prot	unsigned
Уровень доверия (integrity level) процесса	integ	unsigned
Время создания процесса	when	timestamp
Уникальный идентификатор родительского процесса	parent	unsigned (индекс в массиве GUID-ов)
Уникальный идентификатор процесса-создателя	caller	unsigned (индекс в массиве GUID-ов)
Идентификатор процесса-инициатора операции	cpid	unsigned
Полное имя процесса-инициатора операции	cpath	string MANGLED
Код завершения процесса	code	unsigned
Уникальный идентификатор целевого процесса	targ	unsigned
Полное имя целевого процесса	tpath	string MANGLED
Идентификатор целевого процесса	tpid	unsigned
Флаги образа целевого процесса	targf	uint64
Поведенческие признаки целевого процесса (первая группа)	trf0	uint64
Поведенческие признаки целевого процесса (вторая группа)	trf1	uint64
Стек вызовов операции	trace	string
Полное имя файла образа	path	string MANGLED
Флаги операции загрузки образа	ldf	unsigned
Флаги образа	imgf	uint64
Базовый адрес образа	base	uint64
Размер образа	isize	unsigned
Идентификатор целевой нити	tid	unsigned
Имя модуля целевой нити	tmod	string
Имя функции целевой нити	tfunc	string
Стартовый адрес целевой нити	taddr	uint64
Флаги операции с нитью	tf	unsigned
Запрашиваемые права	dsrd	unsigned (32 бита)
Предоставленные права	grnt	unsigned (32 бита)
Новый уровень защиты процесса	prot1	int
Новая командная строка процесса	cmdl1	string
Размер файла	fsize	int64

Назначение	JSON	Тип
Тип файла	ftype	enum
SHA-1 файла	sha1	string
MD5 файла	md5	string
SHA-256 файла	sha256	string
Imphash файла	imphash	string
Электронная подпись файла	sgnr	string
Статус электронной подписи	sgnr_s	enum
Тип упаковщика файла	pack	string
Атрибуты файла	attr	unsigned
Время создания файла	crtime	timestamp
Время последней записи файла	chtime	timestamp
Оригинальное имя файла	ofn	string
Компания-издатель файла	fcomp	string
Версия файла	fver	string
Описание файла	fdesc	string
Продукт, к которому относится файл	fprod	string
Файл находится в "белом" списке	fwhite	int (-/1)
Код обнаружения	detect	unsigned
Исключение для файла по хешу	fh_excl	string
Исключение для файла по имени	fn_excl	string
AMSI: имя содержимого	amsi_cname	string
AMSI: содержимое	amsi_data	string
AMSI: имя приложения	amsi_appname	string
AMSI: ссылка на скачивание зарезервированного содержимого	amsi_blink	string

Поле **integ** (уровень доверия процесса) событий мониторинга процессов может принимать следующие значения:

– 0 (нет);

– 1 (низкий);

– 2 (средний);

– 3 (высокий);

– 4 (системный);

– 5 (защищенный).

9.7 События мониторинга системы

Подтипы событий (st) мониторинга системы представлены в таблице 26.

Таблица 26 – Подтипы событий мониторинга системы

Код события	Имя события	Описание
0	Система: WMI	Событие подсистемы WMI
2	Система: Изменение системного времени	Изменение системного времени
3	Завершение работы	Событие, связанное с завершением работы ОС

События мониторинга систем с кодом события 0 (WMI) представлены в таблице 27.

Таблица 27 – Поля мониторинга системы (код события 0)

Назначение	JSON	Тип
WMI: Тип события (создание = 0, удаление = 1, изменение = 2)	wmi	integer
WMI: SID пользователя	wmi_sid	string
WMI: Пространство имен	ns	string
WMI: Путь до исполняемого файла	exe_path	string MANGLED
WMI: Имя файла	fname	string MANGLED
WMI: Имя фильтра событий	wmi_nm	string
WMI: Строка запроса	qstr	string
WMI: Имя файла скрипта	scrfname	string MANGLED
WMI: Текст скрипта	scrtxt	string
WMI: Имя источника	sname	string MANGLED
WMI: Путь	wmi_pth	string
WMI: SMTP	smtp	string
WMI: Фильтр	flt	string
WMI: Потребитель	cnsm	string
WMI: Идентификатор процесса клиента	wmi_clpid	unsigned
WMI: Уникальный идентификатор процесса клиента	wmi_cluuid	int
WMI: Время создания процесса клиента	wmi_cltime	timestamp (UTC)
WMI: Командная строка процесса клиента	wmi_clcmdl	string
WMI: Локальный запрос (0 или 1, по умолчанию 1)	wmi_local	int (0/1)
WMI: Идентификатор созданного процесса	wmi_crpid	unsigned
WMI: Уникальный идентификатор созданного процесса	wmi_cruuid	int (индекс в массиве GUID'ов)
WMI: Время создания созданного процесса	wmi_crtime	timestamp (UTC)

Назначение	JSON	Тип
WMI: Командная строка созданного процесса	wmi_crcmdl	string
WMI: Имя машины, выполнившей запрос	wmi_cl	string
WMI: FQDN машины, выполнившей запрос	wmi_clfqdn	string
WMI: Имя пользователя клиента, выполнившего запрос	wmi_usr	string
WMI: Имя домена клиента, выполнившего запрос	wmi_dom	string
WMI: Имя вызываемого клиента	wmi_mthd	string



Важно

До ОС Windows 10 и Windows Server 2019, WMI-провайдер не предоставляет информацию о созданном процессе в WMI-запросе, соответственно, информация о созданном процессе будет отсутствовать в событии.

Пример строки события представлен в таблице 28.

Таблица 28 – События WMI

Подтип события	Описание
0	[Система] Зарегистрирован WMI-компонент с возможностью автозапуска по пути **wmi_pth**
1	[Система] Удален WMI-компонент с возможностью автозапуска по пути **wmi_pth**
2	[Система] Модифицирован WMI-компонент с возможностью автозапуска по пути **wmi_pth**

Системное время изменяется с **prev_stime** (предыдущее системное время) на **new_stime** (новое системное время).

Поле **sht** событий мониторинга системы может принимать следующие значения событий:

– 1 (штатное завершение работы компьютера);

– 2 (штатный переход компьютера в состояние сна или гибернации);

– 3 (штатная остановка агента).

9.8 События пользовательских сессий

Подтипы событий и их текстовые описания представлены в таблице 29.

Таблица 29 – Подтипы событий пользовательских сессий

Код события	Имя события	Описание
1	Сессии: Создание пользовательской сессии	Создание **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
2	Сессии: Завершение пользовательской сессии	Завершение **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
3	Сессии: Подключение к пользовательской сессии	Подключение к **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
4	Сессии: Отключение от пользовательской сессии	Отключение от **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
5	Сессии: Выполнен вход пользователя	Выполнен **%type2%** вход пользователя **sess_dom\sess_usr (sess_id)**
6	Сессии: Выполнен выход пользователя	Выполнен **%type2%** выход сессии пользователя **sess_dom\sess_usr (sess_id)**
7	Сессии: Блокирование сессии пользователя	Блокирование **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
8	Сессии: Разблокирование сессии пользователя	Разблокирование **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
9	Сессии: Изменен статус удаленного управления сессии пользователя	Изменен статус удаленного управления сессии пользователя **sess_dom\sess_usr (sess_id)**



Примечание

Обозначение **%type%** заменяется на «локальной», если тип сессии **local**, в противном случае заменяется на «дистанционной». Обозначение **%type2%** заменяется на «локальный», если тип сессии local, иначе заменяется на «дистанционный».

Параметр **sess_opt** (тип дистанционного управления) может принимать одно из значений, указанных в таблице 30.

Таблица 30 – Типы дистанционного управления

Значение	Описание
0	Дистанционное управление отключено
1	Пользователь имеет полный контроль над сеансом пользователя с разрешения локального пользователя
2	Пользователь имеет полный контроль над сеансом пользователя, разрешение локального пользователя не требуется
3	Пользователь может просматривать сеанс удаленно с разрешения локального пользователя, удаленный пользователь не может активно управлять сеансом

4	Пользователь может удаленно просматривать сеанс, но не может активно управлять сеансом, разрешение локального пользователя не требуется

Параметр **sess_proto** (тип дистанционного управления) принимает следующие значения:

– 0 (консольная сессия);

– 2 (RDP-сессия).

Поля событий мониторинга сессий представлены в таблице 31.

Таблица 31 – Поля мониторинга сессий

Назначение	JSON	Тип
Локальная сессия	local	int (0/1)
Номер сессии	sess_id	unsigned
Тип дистанционного управления	sess_opt	unsigned (опционально
Тип сессии	sess_proto	unsigned (опционально)
Имя оконной станции	win_stn	string (опционально)
Имя клиента	sess_cl	string (опционально)
IP-адрес клиента	sess_claddr	string (опционально)
Имя пользователя	sess_usr	string (опционально)
Имя домена/компьютера	sess_dom	string (опционально)

Анализ шаблонов поведения может помочь аналитикам заметить отклонения, которые указывают на активность злоумышленников: необычное время активности пользователей, многократный подбор учетных данных и другие аномалии в поведении пользователей.

9.9 События монитора вызовов

Подтипы событий монитора вызовов представлены в таблице 32.

Таблица 32 – Подтипы событий монитора вызовов

Код события	Имя события	Описание
0	Вызовы: RPC	RPC (remote procedure call)

События монитора вызовов (RPC-вызовы) представлены в таблице 33.

Таблица 33 – Поля монитора вызовов (RPC вызовы)

Назначение	JSON	Тип
RPC: UUID интерфейса	rpc_id	unsigned (индекс в массиве GUID-ов)
RPC: Номер процедуры	rpc_opnum	unsigned
RPC: Имя процедуры	rpc_opname	string (опционально)
RPC: Протокол	rpc_proto	unsigned (опционально)
RPC: Сервис аутентификации	rpc_authsvc	unsigned (опционально)
RPC: Конечная точка	endp	string (опционально)
RPC: Сетевой адрес	n_addr	string (опционально)
RPC: Уникальный идентификатор процесса клиента	c_uuid	unsigned (индекс в массиве GUID-ов)
RPC: PID процесса клиента	c_pid	integer
RPC: Исполняемый файл процесса клиента	c_path	string MANGLED
RPC: Уникальный идентификатор процесса сервера	s_uuid	unsigned (индекс в массиве GUID-ов) (опционально)
RPC: PID процесса сервера	s_pid	integer (опционально)
RPC: Исполняемый файл процесса сервера	s_path	string MANGLED (опционально)

Поле **rpc_proto** принимает следующие значения:

1 – TCP;

2 – Named Pipes;

3 – LRPC;

4 – HTTP.

Поле **rpc_authsvc** принимает следующие значения:

0x09 – Negotiate;

0x0A – NTLM;

0x0E – SChannel;

0x10 – Kerberos;

0x14 – Kernel.

В поле **Описание** таблицы событий на странице **Активность**, если **n_addr** пустой или не задан, выводится сообщение в виде:

[Вызовы] Процесс **c_path (c_pid)** выполнил удаленный вызов процедуры **endp** по интерфейсу **rpc_id** в процессе **s_path (s_pid)**.

Если **n_addr** задан, тогда выводится сообщение в виде:

[Вызовы] Процесс **c_path (c_pid)** выполнил удаленный вызов процедуры **n_addr:endp** по интерфейсу **rpc_id** в процессе **s_path (s_pid)**.

9.10 События модуля Антишифра

Подтипы событий и их текстовые описания представлены в таблице 34.

Таблица 34 – Подтипы событий модуля Антишифра

Код события	Имя события	Описание
0	Защита файлов: Заблокирован вредоносный процесс	Заблокирован вредоносный процесс
1	Создана резервная копия файла	Создана резервная копия файла **name**

Поля событий модуля защиты от вирусов-шифровальщиков представлены в таблице 35.

Таблица 35 – Поля событий модуля Антишифра

Назначение	JSON	Тип
Количество открытий/созданий файлов с последующими обращениями к ним	cf_ac	unsigned
Количество открытых файлов из защищаемых каталогов	cf_oc	unsigned
Количество созданных процессом файлов после активации мониторинга	cf_cc	unsigned
Количество удалённых файлов в защищаемых каталогах	si_dc	unsigned
Количество переименованных файлов в защищаемых каталогах	si_rc	unsigned
Количество перемещённых файлов в защищаемые каталоги	si_mi	unsigned
Количество перемещённых файлов из защищаемых каталогов	si_mo	unsigned
Количество файлов из защищаемых каталогов, которые только читали	ro_fc	unsigned
Количество файлов из защищаемых каталогов, в которые только писали	wo_fc	unsigned
Количество файлов из защищаемых каталогов, которые читали и писали	rw_fc	unsigned
Среднее значений файловой энтропии по чтению	pr_re	unsigned
Среднее значений файловой энтропии по записи	pr_we	unsigned
Правило блокировки процесса	pr_lr	unsigned
Реакция модуля на идентификацию шифровальщика	pr_ra	unsigned
Количество файлов с нарушенной целостностью	a_fcc	unsigned
Количество файлов с превышенной энтропией	a_eoc	unsigned
Количество расширений файлов, из которых читали	exrac_	unsigned
Количество расширений файлов, в которые писали	exwac_	unsigned
Количество уникальных расширений файлов, из которых только читали	exurac	unsigned
Количество уникальных расширений файлов, в которые только писали	exuwac	unsigned
Категории файлов, к которым осуществлялся доступ	gf_am	unsigned
Категории файлов, из которых производилось чтение	gf_rm	unsigned

Назначение	JSON	Тип
Категории файлов, в которые производилось запись	gf_wm	unsigned
Категории файлов, которые удалялись	gf_dm	unsigned

Энтропия файла в контексте информационной безопасности — это статистическая мера неопределенности или случайности данных, содержащихся в файле. Она измеряет, насколько непредсказуемы или хаотичны байты, из которых состоит файл.

Низкая энтропия (от 0 до 4) характерна для структурированных данных (тексты, логи, XML, несжатые исполняемые файлы), а высокая энтропия (6-8 и более) типична для случайных данных (зашифрованные файлы, сжатые архивы, упакованные исполняемые файлы, медиафайлы)

9.11 События модуля контроля USB

Тип события – **Контроль USB** (**t**:9 в DSL). Подтипы событий (**st**) и их текстовые описания представлены в таблице 36.

Таблица 36 – Подтипы событий модуля контроля USB

Код события	Имя события	Описание
0	Устройство USB подключено	Подключено устройство **usb_mr usb_pt** MI_**usb_mi**
1	Устройство USB отключено	Отключено устройство **usb_mr usb_pt** MI_**usb_mi**
2	Зафиксирована запрещенная попытка чтения	Заблокировано чтение с устройства **usb_mr usb_pt** MI_**usb_mi**
3	Зафиксирована запрещенная попытка записи	Заблокирована запись на устройство **usb_mr usb_pt** MI_**usb_mi**
4	Зафиксирована запрещенная попытка выполнения управляющего запроса	Заблокировано конфигурирование устройства **usb_mr usb_pt** MI_**usb_mi**
5	Зафиксирована запрещенная попытка запуска исполняемого кода	Заблокирован запуск исполняемого файла **usb_exec** с накопителя **usb_mr usb_pt**
6	Статистика чтения/записи данных	usb_mr usb_pt usb_mi : прочитано usb_cr байт, записано usb_cw байт

Поля событий модуля контроля USB указаны в таблице 38.

Таблица 37 – События модуля контроля USB

Назначение	Тип	JSON
Тип контролируемого устройства	uint8	usb_dt

Класс устройства USB	uint8	usb_dc
Подкласс устройства USB	uint8	usb_dsc
Идентификатор производителя (VID)	uint16	usb_vid
Идентификатор продукта (PID)	uint16	usb_pid
Номер интерфейса (MI)	uint8	usb_mi
Серийный номер устройства	string	usb_sn
Наименование производителя	string	usb_mr
Наименование продукта	string	usb_pt
Имя модуля, который был запущен с носителя	string	usb_exec
Количество прочитанных байтов	uint64	usb_cr
Количество записанных байтов	uint64	usb_cw
Общее количество прочитанных байтов	uint64	usb_tr
Общее количество записанных байтов	uint64	usb_tw

9.12 События статистики

Поля событий статистики указаны в таблице 38.

Таблица 38 – События статистики

Назначение	Тип	JSON
Загрузка процессора	unsigned	cpu_load
Загрузка памяти	unsigned	mem_load
Количество процессов	unsigned	processes
Количество нитей	unsigned	threads
Количество открытых описателей	unsigned	handles
Объем прочитанных с диска данных в секунду	int64	disk_read
Объем записанных на диск данных в секунду	int64	disk_write
Объем переданных данных по сети в секунду	int64	net_send
Объем принятых данных по сети в секунду	int64	net_recv
Время регистрации событий (UTC)	timestamp	time
Временная зона	string	timezone
Признак нахождения в режиме network containment	int(0/1)	net_locked
Общее количество сетевых соединений	unsigned	connections
Состояние функций защиты (0 –включены, 1 – выключены)	int(0/1)	disabled
Время последнего обновления аналитики по наборам	json_object	config_time
Причина завершения работы	unsigned	shutdown
Парольная защита от удаления агента (1 – включена, 0 –выключена)	int(0/1)	protect
Количество системных ошибок	unsigned	sys_errs

Назначение	Тип	JSON
Количество прикладных ошибок	unsigned	app_errs
Максимальная скорость отправки событий (Кбит/сек)	unsigned	netlimit
Загрузка процессора службой агента	unsigned	svc_cpu_load
Использование памяти службой (Мбайт) агента	unsigned	svc_mem_usage
Использование памяти драйвером (Мбайт) агента	unsigned	drv_mem_usage
Загрузка процессора драйвером агента	unsigned	drv_cpu_load
Загрузка процессора монитором процессов	unsigned	drv_pm_load
Загрузка процессора монитором сетевых соединений	unsigned	drv_net_load
Загрузка процессора монитором файловых операций	unsigned	drv_fs_load
Загрузка процессора монитором реестра	unsigned	drv_reg_load
Загрузка процессора механизмом проверки индикаторов атак/исключений	unsigned	drv_ioa_load
Выборка самых тяжеловесных индикаторов атак	json_object	ioa_util
Выборка самых тяжеловесных исключений	json_object	excl_util
Максимальная скорость отправки событий (Кбит/сек)	unsigned	netlimit
Режим работы агента	unsigned	mode
Количество блокировок реагирования по командным строкам	unsigned	cmdl_locks
Количество файловых блокировок реагирования	unsigned	file_locks
Количество сетевых блокировок реагирования	unsigned	net_locks

Поле **shutdown** может принимать следующие значения:

1) 0 – агент работает в штатном режиме;

2) 1 – штатное завершение работы компьютера;

3) 2 – штатный переход компьютера в состояние сна или гибернации;

4) 3 – штатная остановка агента.

DSL-запросы по статистике срабатывают, если в поле **Источник события** на странице **Активность** выбран источник **Статистика**.

Поле **ioa_util** является json_object-ом, свойствами которого являются идентификаторы индикаторов атак, а значениями базисные пункты (сотые доли процента) от общего времени проверки индикаторов атак, начиная с момента получения индикаторов агентом. Содержит максимум десять пар значений для самых тяжеловесных индикаторов. Данное поле может отсутствовать, если индикаторы не загружены на агенте, или их проверка не осуществлялась по каким-либо причинам. Поле **excl_util** аналогично **ioa_util**, только его свойствами являются идентификаторы исключений.

9.13 Телеметрия RT Protect EDR

Категории функций телеметрии, которые возможно обнаружить с помощью RT Protect EDR представлены в таблице 39.

Таблица 39 – Телеметрия RT Protect EDR

Категория функций телеметрии	Подкатегория	Реализация в RT Protect EDR
Процессы	Создание процесса	Да
	Завершение процесса	Да
	Доступ к процессу	Да
	Загрузка образа/библиотеки	Да
	Создание нити в стороннем процессе	Да
	Активность, связанная с подменой процесса	Да
Файлы	Создание файла	Да
	Открытие файла	Реализовано только для файлов с потенциально активным содержимым
	Удаление файла	Да
	Модификация файла	Да
	Переименование файла	Да
Активность, связанная с учетной записью пользователя	Создание локальной учетной записи	Доступно с помощью журнала Windows
	Модификация локальной учетной записи	Доступно с помощью журнала Windows
	Удаление локальной учетной записи	Доступно с помощью журнала Windows
	Вход в учетную запись	Да
	Выход из учетной записи	Да
Сетевая активность	TCP-соединение	Да
	UDP-соединение	Да
	URL	В данный момент не реализовано
	DNS-запрос	Да
	Загрузка файла	Реализовано только для файлов, загруженных с помощью браузеров и их компонентов
Хеш-алгоритмы	MD5	Да
	SHA	Да

Категория функций телеметрии	Подкатегория	Реализация в RT Protect EDR
	IMPHASH	В данный момент не реализовано
Активность реестра	Создание ключа/значения	Да
	Модификация ключа/значения	Да
	Удаление ключа/значения	Да
Активность, связанная с планировщиком задач	Создание задачи	Реализовано с помощью индикатора атак
	Модификация задачи	Реализовано с помощью индикатора атак
	Удаление задачи	Реализовано с помощью индикатора атак
Службы	Создание службы	Реализовано с помощью индикатора атак
	Модификация службы	Реализовано с помощью индикатора атак
	Удаление службы	Реализовано с помощью индикатора атак
Активность драйвера/модуля	Загрузка драйвера	Да
	Модификация драйвера	В данный момент не реализовано
	Выгрузка драйвера	В данный момент не реализовано
Операции с устройствами	Монтирование виртуального диска	В данный момент не реализовано
	Размонтирование USB-устройства	Да (при включении модуля USB)
	Монтирование USB-устройства	Да (при включении модуля USB)
Другие релевантные события	Модификация групповых политик	В данный момент не реализовано
Активность, связанная с именованными каналами	Создание именованного канала	Да
	Соединение с именованным каналом	Да
Системные операции EDR	Запуск агента	Да
	Остановка агента	Да
	Установка агента	В данный момент не реализовано
	Удаление агента	В данный момент не реализовано
	Агент keep-alive	Да
	Ошибки агента	Да
WMI активность	WmiEventConsumerToFilter	Да

Категория функций телеметрии	Подкатегория	Реализация в RT Protect EDR
	WmiEventConsumer	Да
	WmiEventFilter	Да
Активность BIT JOBS	Активность BIT JOBS	Реализовано с помощью индикатора атак
Активность PowerShell	Активность блока сценариев	Реализовано с помощью индикатора атак

10. Ролевая модель

10.1 Общая информация

При развертывании сервера в Программе формируется пользователь с администраторскими правами, который может создавать группы прав для других пользователей, назначая для них произвольный набор прав. Соответственно, аналитик может обладать произвольным набором прав. Аналитику может быть назначена произвольная роль или несколько ролей, каждая из которых подразумевает определенный набор функций.

В разделе **Пользователи и роли** на вкладке **Роли** администратор может создать группу прав и добавить в нее пользователей, которые будут наделены соответствующими выбранной роли правами. При нажатии кнопки **Создать роль** администратору необходимо выбрать в открывшемся окне, какие права будут назначены группе пользователей. Обязательным при назначении роли является определение ее имени. После назначения всех прав, необходимых для выбранной роли, администратору следует нажать кнопку **Создать**.

На вкладке **Роли** администратор может выполнить следующие операции с ролью:

1) Редактировать роль ();

2) Назначить роль пользователям ();

3) Отозвать роль у пользователей ();

4) Удалить роль ();

5) Удалить выбранные роли (чтобы это сделать, необходимо выбрать роли для удаления и нажать кнопку **Удалить выбранные**).

10.2 Права, предоставляемые пользователям

В списке доступных для назначения прав представлены права, описанные в таблице 40.

Таблица 40 – Список прав, назначаемых пользователям

Право пользователя		Описание
Пользователи		
Доступ к разделу Пользователи и роли		**Обязательное право.** Отсутствие данного права делает разделы «Пользователи и роли» недоступным для пользователя. Если обязательное право будет не выбрано, то дочерние права будут недоступны.
	Создание учетных записей пользователей	Данное право зависит от обязательного права «Доступ к разделу пользователи и роли». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. При отсутствии данного права у пользователя отключается возможность регистрации новых пользователей в системе. При этом доступность других операций определяется отдельными правами. При наличии данного права пользователю автоматически добавляются права управления учетными записями и правами пользователей.
	Управление учетными записями пользователей	Данное право зависит от обязательного права «Доступ к разделу пользователи и роли». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Также данное право зависит от права «Создание учетных записей пользователей». При включенном праве «Создание учетных записей пользователей», данное право будет автоматически включено и заблокировано для изменений.
	Управление правами пользователей	Данное право зависит от обязательного права «Доступ к разделу пользователи и роли». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Также данное право зависит от права «Создание учетных записей пользователей». При включенном праве «Создание учетных записей пользователей», данное право будет автоматически включено и заблокировано для изменений.

Право пользователя	Описание
Изменение пароля своей учетной записи	При отсутствии данного права у пользователя пропадает возможность сброса пароля своей УЗ. В таком случае пароль ему может сменить другой пользователь, имеющий право управления пользователями.
Планировщик задач	
Управление планировщиком задач	Основное право. При включенном основном праве, дочерние права автоматически будут включены и заблокированы для изменений.
Включение/выключение сценариев и задач	Данное право зависит от права «Управление планировщиком задач». При включенном праве «Управление планировщиком задач», данное право автоматически будет включено и заблокировано для изменений.
Использование сценариев реагирования	Данное право зависит от права «Управление планировщиком задач». При включенном праве «Управление планировщиком задач», данное право автоматически будет включено и заблокировано для изменений.
Реагирование	
Право доступа к терминалу реагирования	При отсутствии данного права следующие возможности становятся недоступными: - открытие live-сессии с агентом; - API «старого» терминала.
Право доступа к файлам, загруженным с агентов	При отсутствии данного права у пользователя отключается возможность тем или иным способом получать содержимое и имена файлов, загруженных в Хранилище с агентов, включая скачивание одного файла или нескольких (в виде архива) файлов, получение ссылки на скачивание, просмотр, отправка в TI. Также исключается возможность удаления файлов, загруженных с агентов, из Хранилища. При этом сохраняется возможность полноценной работы с пользовательскими файлами, т.е. с файлами, предназначенными для скачивания с сервера (вкладка «Загрузка файлов в Хранилище»). В разделе «Хранилище»: - исключаются вкладки Файлы с агентов и «Задачи по загрузке архивов». В разделе «Планировщик задач»: - исключается возможность работы с файлами, загруженными в рамках задачи.
Журнал безопасности	
Доступ к журналу безопасности	Обязательное право. Если обязательное право не выбрано, то дочерние права будут недоступны.

Право пользователя	Описание
	При отсутствии данного права у пользователя блокируется возможность любого доступа к журналу безопасности. Раздел «Журнал безопасности» исключается целиком из интерфейса. При наличии данного права в дополнение к нему подразумевается наличие списка (вектора) типов событий, которые доступны пользователю в разделе «Журнал безопасности».
Управление журналом безопасности	Зависит от обязательного права «Доступ к журналу безопасности». При включенном обязательном праве данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Выбор событий, регистрируемых в журнале безопасности	Зависит от обязательного права «Доступ к журналу безопасности». При включенном обязательном праве данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Диагностическая информация	
Диагностика системы	При отсутствии данного права у пользователя отключается функционал предоставления статуса «здоровья» сервера и агента (check-engine), а также пропадает возможность выборки агентов по фильтру Проблемный. Возможность найти проблемных агентов иными способами (например, через DSL) не зависит от данного права.
Обновление агентов	
Управление обновлением ПО Агентов	При отсутствии права следующий функционал отключается (кнопки и переключатели скрываются или переходит в read-only режим, текстовые поля переходят в read-only режим): — загрузка, скачивание, удаление дистрибутивов обновления агентского ПО; — изменение параметра автообновления агента. На странице **Агенты** отсутствует переключатель **Автообновление**. На странице **Дистрибутивы** отсутствуют: - кнопка **Загрузить** дистрибутив; - столбец **Управление** в таблице дистрибутивов.
Агенты	

Право пользователя	Описание
Управление агентами	При отсутствии права следующий функционал отключается (кнопки и переключатели скрываются или переходят в read-only режим, текстовые поля переходят в read-only режим): – изменение имени агента; – изменение критичности агента; – изменение группы агента; – создание, удаление, редактирование групп агентов; – возможность верификации и удаления (деверификации) агентов; – управление защитой агента; – управление золотым образом агента; – управление защитой от удаления агента; – изменение описания агента. **Страница Агент:** – Имя агента; – Критичность агента; – кнопка **Удалить агента**; – переключатель **Защита**; – кнопка **Управление** в блоке **Золотой образ**; – переключатель **Защита от удаления**; – управление группой агента; – блок **Описание агента**. **Страница Агенты:** – кнопки управления группами агентов; – кнопка удаления агентов; – кнопки управления изоляций, защитой, защитой от удаления, золотым образом; – кнопка изменения критичности агента. **Страница Группы:** – кнопка **Создать группу**; – кнопка **Удалить выбранные**; – столбец **Управление в таблице групп** (редактирование, удаление). **Страница Верификация:** – кнопка **Верифицировать выбранных**.
Интеграции	

Право пользователя	Описание
Настройка интеграции с TI	Данное право подразумевает возможность изменения настройки интеграции с TI в разделе **Интеграции**.
Настройка интеграции с локальной средой проверки файлов	Данное право подразумевает возможность изменения настройки интеграции с локальной средой проверки файлов в разделе **Интеграции**.
Настройка интеграции с LDAP	Данное право подразумевает возможность изменения настройки интеграции с LDAP в разделе **Интеграции.**
Настройка экспорта событий журнала безопасности	Данное право зависит от обязательного права «Доступ к журналу безопасности». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Данное право подразумевает возможность изменения настройки экспорта событий в разделе **Интеграции.**
Настройка экспорта событий мониторинга	Данное право подразумевает возможность изменения настройки интеграции с SIEM для экспорта событий мониторинга в разделе **Интеграции**.
Аналитика	
Доступ к аналитике	**Обязательное право.** Если обязательное право будет не выбрано, то дочерние права будут недоступны. При отсутствии данного права пользователю становятся недоступны любые операции модификации, касающиеся аналитики, исключений, профилей и конфигураций. В части аналитики (т.е. ИА, ИК, YARA и Журналы) и профилей USB и Антишифра «закрываются» операции чтения содержимого наборов (профилей), а соответствующие одноименные разделы при этом полностью исключаются из интерфейса. При этом все же остается доступным вызов set перечисления наборов, необходимый для визуализации бейджа набора (имя, признак TI и т.д.) в конфигурации агента на странице Агент и др. местах. Также в режиме «только чтение» остаются доступными исключения (всех типов) и профиль безопасности агента. При наличии данного права у пользователя все разделы аналитики, исключений и профилей становятся доступны, при этом для исключений допускаются операции модификации, а аналитика и профили работают в режиме «только чтение» - доступность операций модификации определяется другими правами. Логика выключения данного функционала уже заложена у нас в роли Оператора поиска угроз и включает в себя следующее: - из сайд бара исключается раздел Аналитика (Исключения и Профили остаются доступными);

Право пользователя	Описание
	- возможность перехода на недоступные элементы аналитики (ИА, ИК, YARA-правила) исключается (страницы Активность, Инциденты, Инцидент, Обзор событий, возможно еще где-то, нужно все места найти). При этом сохраняется возможность перехода к исключениям; - раздел Конфигурации сохраняется, но работает в режиме «только чтение»; - на странице Агент блок Конфигурации также работает в режиме «только чтение»; - со страницы Агенты также убирается возможность применения конфигурации; - в раскрывашке агента на странице Агенты убираются ссылки на разделы аналитики и профилей.
Управление наборами и конфигурациями	Зависит от обязательного права «Доступ к аналитике». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Изменение аналитики и профилей	При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Включение/выключение элементов аналитики	При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Также данное право зависит от права «Изменение аналитики и профилей». При включенном праве «Изменение аналитики и профилей» данное право автоматически будет включено и заблокировано для изменений.
Инциденты	
Управление инцидентами	При наличии данного права весь раздел Инциденты работает без ограничений. При этом право ограниченного управления инцидентами включено автоматически. При отсутствии данного права управление инцидентами регулируется правом ограниченного доступа к инцидентам – либо в режиме оператора поиска угроз (если право есть), согласно существующей схеме ограничений для этой роли, либо в режиме «только чтение» (если права нет).
Ограниченное управление инцидентами	Зависит от права «Управление инцидентами». При включенном основном праве, данное право автоматически будет включено и заблокировано для изменений. При отсутствии данного права, пользователю запрещены какие-либо модифицирующие действия с инцидентами. Раздел Инциденты и карточка инцидента работают в режиме «только чтение».

Право пользователя	Описание
Лицензия	
Управление лицензией	При отсутствии данного права отключается возможность загрузки новой лицензии в разделе **Лицензия**. Доступ к просмотру параметров текущей лицензии не ограничивается.

10.3 Пользователи

В разделе **Пользователи и роли** во вкладке **Пользователи** администратор может просматривать информацию о пользователях, создавать и удалять учетные записи пользователей, назначать пользователям определенную роль и исключать пользователей из роли, а также изменять параметры учетных записей пользователей. Во вкладке **Пользователи** показана информация обо всех зарегистрированных в Программе пользователях.

Данные о пользователях представлены в табличном виде.

Таблица содержит следующие поля:

1) Имя пользователя;
2) Последнее время входа;
3) Имя;
4) Фамилия;
5) Email;
6) Роль;
7) Статус;
8) Управление.

Имя пользователя – содержит логин, под которым пользователь зарегистрирован в Программе. Если пользователь является LDAP-пользователем, то помечается значком  . При этом LDAP-пользователь может быть связан с пользователем EDR. Такой пользователь сможет войти как под учетной записью, созданной в разделе **Пользователи**, так и с учетными данными LDAP-пользователя.

Последнее время входа – содержит дату и время последнего входа пользователя.

Имя – содержит имя, которое пользователь указал при регистрации.

Фамилия – содержит фамилию, которую пользователь указал при регистрации.

Email – электронный почтовый адрес, указанный пользователем при регистрации.

Роли – указаны роли с наборами прав.

Статус и **Управление** – в указанных полях содержатся кнопки для изменения параметров учетных записей пользователей.

В верхней части окна над таблицей содержатся строки для поиска пользователей по параметрам фильтрации:

– Показывать по;

– Имя пользователя (логин);

– Имя;

– Фамилия;

– Email;

– Роль пользователя;

Каждая строка таблицы содержит информацию о роли пользователя и дополнительную информацию о сессиях пользователя, для ее просмотра необходимо нажать ЛКМ на значок ›. В случае, если у пользователя были активные сессии, они будут показаны ниже строки. По умолчанию отображается только последняя сессия (рис. 4).

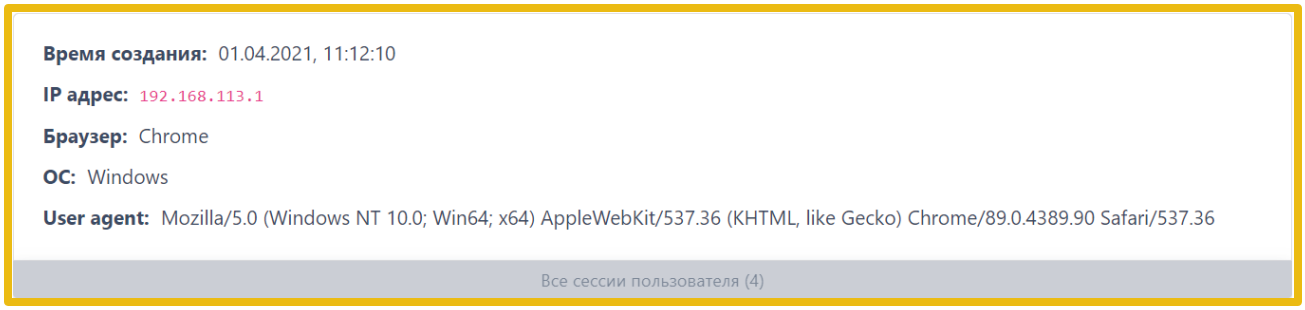


Рисунок 4 – Информация о сессиях пользователя

Для раскрытия данных по всем сессиям следует нажать кнопку **Все сессии пользователя**. В окне сессии отображается информация по следующим параметрам: **Время создания**, **IP адрес**, **Браузер**, **ОС** и **User agent**.

Время создания – дата и время входа в учетную запись пользователя для выбранной сессии.

IP адрес – ip-адрес устройства, с которого был выполнен вход пользователя для выбранной сессии.

Браузер – браузер, из которого был выполнен вход в Программу для выбранной сессии.

ОС – операционная система, под управлением которой выполнялся запуск браузера для входа в Программу.

User agent – в поле отображается наименование браузера, с помощью которого выполняется взаимодействие с агентом.

10.3.1. Изменение параметров учетных записей пользователей

Пользователь с соответствующими правами может управлять параметрами учетных записей пользователей.

Два поля таблицы с учетными записями пользователей содержат дополнительные кнопки для управления параметрами учетных записей: **Статус** и **Управление**.

В поле **Статус** находятся кнопки **Заблокировать/Разблокировать пользователя** , с помощью которых уполномоченный пользователь может временно запретить или разрешить обычному пользователю работать с Программой. Опция блокирования неприменима по отношению к своей учетной записи. Процесс блокирования пользователя защищен от случайных нажатий необходимостью подтверждать действие блокирования/разблокирования в отдельном окне.

После подтверждения операции в нижней части основного окна Программы появляется сообщение **Пользователь разблокирован/заблокирован**.

В поле **Управление** находятся кнопки **Редактировать пользователя** ( ), **Потребовать смену пароля при следующем входе** ( ), **Привязать LDAP-пользователя** ( ) или изменить настройки привязки и **Удалить пользователя** ( ).

При нажатии кнопки **Редактировать пользователя** открывается окно, в котором можно изменить имя и фамилию пользователя, а также адрес электронной почты. Для сохранения и применения измененных параметров необходимо нажать кнопку **Сохранить**.

При нажатии кнопки **Потребовать пароль при следующем входе** ( ) в строке с определенным пользователем открывается окно подтверждения операции. После подтверждения при последующем входе в Программу этого пользователя будет выведено окно смены пароля (рис. 5). Пароль должен соответствовать правилам добавления пароля. После сохранения нового пароля пользователь сможет войти в Программу с этим паролем.

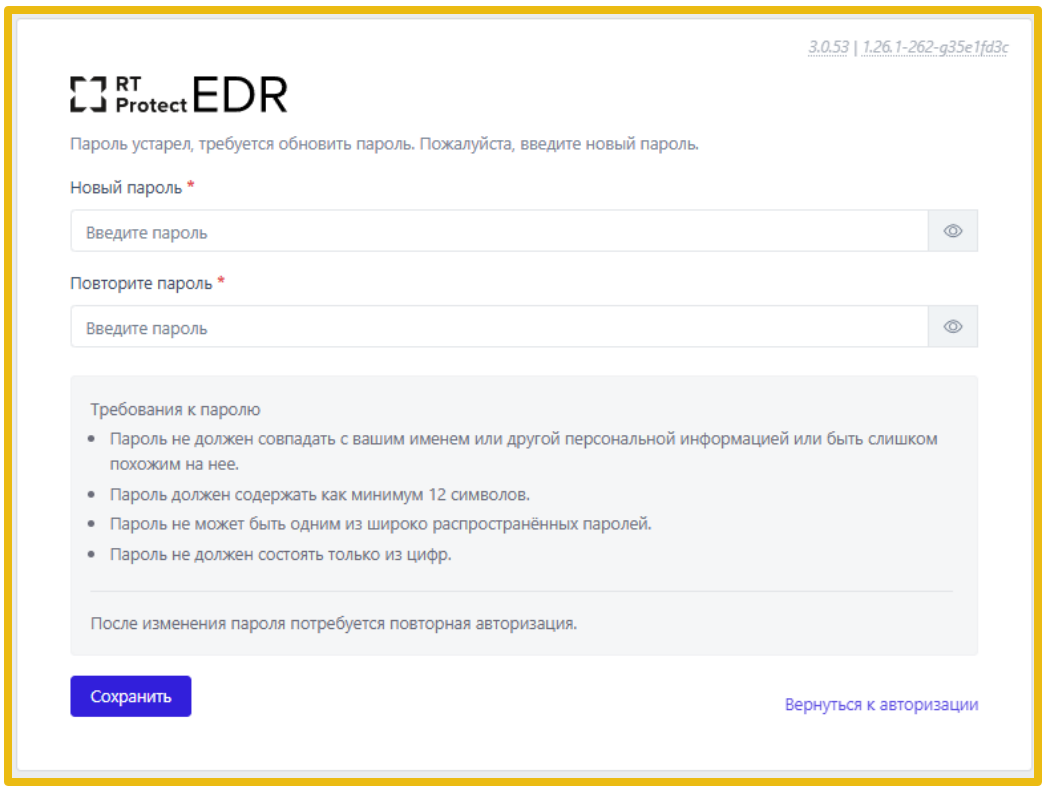


Рисунок 5 – Окно смены пароля пользователя

Для привязки LDAP-пользователя к пользователю EDR администратору необходимо нажать кнопку **Привязать LDAP-пользователя** ( ) в поле **Управление** во вкладке **Пользователи** и в открывшемся окне ввести логин LDAP-пользователя, которого необходимо привязать к пользователю EDR. Связанность пользователей обозначает, что данные между конкретным пользователем LDAP и конкретным пользователем EDR будут синхронизированы.

При нажатии кнопки **Удалить пользователя** ( ) открывается окно, в котором для удаления учетной записи выбранного пользователя следует нажать кнопку **Подтвердить**.

Чтобы добавить роль для одного или нескольких пользователей, необходимо выбрать этих пользователей ( ), после чего нажать кнопку **Назначить роль пользователям** ( ). Откроется окно, в котором необходимо определить роль для выбранных пользователей и нажать кнопку **Добавить**.

Чтобы исключить пользователей из роли, необходимо выбрать этих пользователей ( ), после чего нажать кнопку **Исключить пользователей из роли** . Откроется окно, в котором следует выбрать роль, из которой далее исключить пользователей, после чего нажать кнопку **Применить**.

Чтобы переназначить роли пользователям, необходимо выбрать этих пользователей ( ), после чего нажать кнопку **Переназначить роли пользователям** ( ). Откроется одноименное окно, в котором необходимо выбрать одну или несколько ролей. Выбранные роли заменят текущую роль или роли пользователя.

10.3.2. Страница профиля пользователя

Кликнув по имени пользователя на странице **Пользователи и роли**, можно открыть страницу с профилем пользователя, на которой выполняются различные операции, пересекающиеся функционально с операциями на странице **Пользователи и роли**.

10.3.3. Создание учетной записи пользователя

В нижней части панели администрирования находится кнопка **Создать пользователя**. При нажатии кнопки открывается окно **Создать пользователя**.

Для добавления пользователя необходимо заполнить в окне **Создать пользователя** следующие поля:

– Имя пользователя;

– Адрес электронной почты;

– Имя;

– Фамилия;

– Новый пароль;

– Повторите пароль.

Для завершения регистрации нового пользователя следует заполнить все поля ввода. В поле ввода **Адрес электронной почты** необходимо ввести адрес электронной почты вида login@domain. Для того, чтобы отобразить/скрыть символы, вводимые в поля **Новый пароль** и **Повторите пароль** следует нажать кнопки / .

В нижней части окна приведены правила формирования пароля:

– пароль не должен совпадать с именем пользователя или другой персональной информацией или быть слишком похожим на неё;

– пароль должен содержать как минимум 12 символов;

– пароль не может быть одним из широко распространённых паролей;

– пароль не должен состоять только из цифр.

Для подтверждения значений, установленных для новой учетной записи пользователя, необходимо нажать кнопку Создать. После создания учетной записи пользователя можно назначить ему роль во вкладке **Роли**.

10.3.4. Сброс пароля при входе пользователя в Программу

При входе пользователя в Программу можно выполнить операцию сброса пароля. В этом случае на электронную почту, указанную при регистрации аккаунта будет отправлено письмо, содержащее ссылку на окно восстановления пароля. Эта операция может быть выполнена в случае, если пользователь забыл свой пароль. Необходимо обратить внимание на то, что у пользователя должны быть соответствующие права на сброс пароля (право изменения пароля своей учетной записи). После перехода по ссылке на сброс пароля откроется окно, в котором необходимо ввести новый пароль и подтвердить его.

10.3.5. Сообщения пользователю при вводе некорректных значений

При вводе уполномоченным пользователем некорректных данных в полях окон **Редактировать пользователя** и **Создать пользователя** Программа выводит сообщения об ошибках.

Если пользователь оставляет в указанных выше окнах хотя бы одно пустое поле ввода, то выводится сообщение (рис. 6). Такое же сообщение выводится во всех полях, требующих ввода информации.



Рисунок 6 – Сообщение о пустом поле ввода

При написании в поле ввода **Имя пользователя** значения имени пользователя, идентичного уже сохраненному в Программе, выводится сообщение о том, что пользователь с таким именем уже существует (рис. 7).

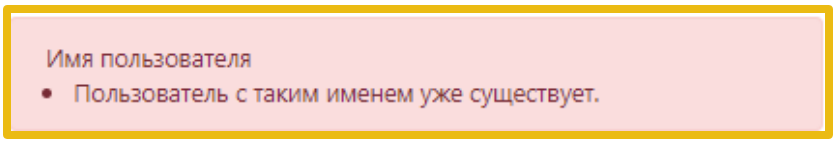


Рисунок 7 – Сообщение о совпадении имени пользователя

При вводе пользователем некорректного адреса электронной почты в поле ввода **Email** в нижней части окна **Редактировать пользователя** или **Создать пользователя** выводится сообщение о необходимости ввода правильного адреса электронной почты (рис. 8).

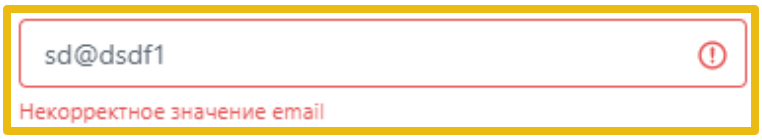


Рисунок 8 – Сообщение о неправильном адресе электронной почты

Если введенный пароль не соответствует одному или нескольким указанным требованиях к паролю правилам, то в нижней части окна появится сообщение, в котором будет указано нарушенное при создании пароля правило (рис. 9).

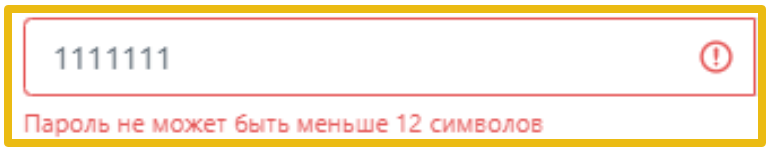


Рисунок 9 – Предупреждающее сообщение при вводе некорректного пароля

При вводе отличных друг от друга значений в поля **Новый пароль** и **Повторите пароль** в нижней части полей ввода появится сообщение о несовпадении введенных паролей (рис. 10).



Рисунок 10 – Сообщение о несовпадении паролей

При восстановлении пароля по ссылке после ввода пользователем некорректных значений в поля **Введите новый пароль** и **Повторите пароль** в окне **Сброс пароля** будут отображаться сообщения, идентичные указанным выше (рис. 11).

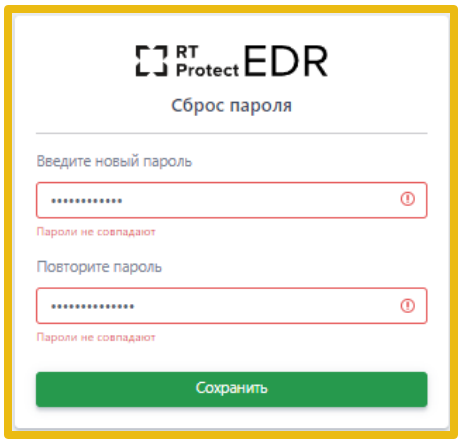


Рисунок 11 – Ввод некорректных значений при сбросе пароля

Сообщения об ошибках, которые выдает Программа при вводе некорректных значений пароля, будут идентичны тем, которые могут возникнуть при вводе пароля и его подтверждения в окне **Создать пользователя.**

Важно

Если пользователь Программы выполнит 4 или более неудачных попыток входа в течение 5 минут, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет администратор Программы или учетная запись будет разблокирована автоматически после завершения временного периода, равного 24 часам.

---

11. Основные операции в RT Protect EDR

11.1 Общая информация

Основной задачей работы Программы является обнаружение вредоносной активности в защищаемой инфраструктуре и нахождение аномалий в генерируемом агентами потоке событий с последующим созданием инцидентов и реагированием на эти события. Инциденты – это контейнеры для событий, обнаруженных на защищаемых конечных точках Программой или аналитиками и определённых ими как аномальная или вредоносная активность. Такие события определяются как несущие угрозу или потенциально угрожающие защищаемой инфраструктуре.

В большинстве случаев аналитику приходится иметь дело с инцидентами, которые формируются в Программе автоматически в момент обнаружения на агенте событий, соответствующих уровню критичности **Средняя** или выше. Кроме автоматического создания инцидента, в Программе предусмотрено создание инцидента аналитиком вручную, когда аналитик добавляет в инцидент произвольное количество событий, которые он считает проявлением вредоносной активности.



Примечание

Подавляющая часть инцидентов в Программе формируются на основе аналитических правил (индикаторы атак, YARA-правила, индикаторы компрометации, встроенные правила на агенте), вердиктов модели машинного обучения, а также в результате получения для артефактов (хеши, IP-адреса и домены) вердиктов от TI-платформы.

Просмотр информации об инциденте и входящих в него событиях осуществляется аналитиком на следующих страницах:

1) **Главная страница** – на странице отображается динамика инцидентов по критичности, распределение инцидентов по критичности, показаны данные о наиболее распространенных за период правилах, в соответствии с которыми были созданы инциденты, и другая важная информация;

2) **Активность** – на странице отображается вся доступная информация о событиях, происходящих на компьютере с установленным агентом;

3) **Оповещения** – на странице отображаются краткие отчеты обо всех инцидентах, зарегистрированных в Программе, а также важная информация о событиях, связанных с конечными точками, на которых установлены агенты;

4) **Инциденты** – на странице отображается информация с описанием инцидентов, зарегистрированных в Программе;

5) **Инцидент** – на странице отображается информация о выбранном инциденте и набор инструментов для редактирования, изменения статуса инцидента и создания комментариев к нему;

6) **Процесс** – на странице отображается информация о процессе и его дереве, где аналитик может проследить цепочку событий, приведших к возникновению инцидента.

На **Главной странице** аналитику доступен просмотр общей информации по контролируемой инфраструктуре:

– количество и состав агентов (активные, находящиеся в изоляции и на верификации);

– общее количество инцидентов и количество открытых инцидентов;

– количество событий за последние 15 минут и за один день;

– количество пакетов с событиями, передаваемыми на сервер, в очереди;

– тайминги проверки артефактов TI, отдельно сетевые артефакты и файлы (при наведении курсора на значок 

аналитику будет показано время, прошедшее с момента регистрации последнего сетевого(файлового) события, которое было обработано/обогащено/аннотировано алгоритмом TI);

– количество открытых инцидентов;

– последние обнаруженные процессы и модули;

– текущее значение количества событий, приходящих с агентской сети в секунду, вторая цифра показывает среднее количество событий в секунду на одном агенте;

– среднее за неделю количество событий, приходящих с агентской сети в секунду;

– динамика инцидентов;

– распределение инцидентов по критичности;

– динамика ключевых событий (события с критичностью **Средняя** и события с блокирующим действием);

– критичность ключевых событий;

– топ 10 правил в инцидентах;

– топ 10 техник MITRE ATT&CK в инцидентах;

– инциденты в уязвимостях.

Для просмотра всех инцидентов, зарегистрированных в Программе, необходимо выполнить переход на страницу **Оповещения** или страницу **Инциденты**.

Аналитик работает с автоматически определяемыми Программой инцидентами, которые возникают при обнаружении аномальной активности на конечных точках с агентами. Аналитик просматривает события, входящие в эти инциденты и определяет, действительно ли они являются угрозой для защищаемой инфраструктуры, и на основе этого вердикта может предпринять те или иные действия:

1) Изолировать зараженного агента;

2) Удалить вредоносное ПО на конечной точке с помощью функционала отправки команд агенту;

3) Завершить вредоносный процесс на странице **Процесс**;

4) Отреагировать на вредоносную ативность с помощью команд терминала;

5) Загрузить подозрительный файл в хранилище Программы;

6) Выяснить масштабы компрометации на странице **Артефакты TI**;

7) Закрыть инцидент после устранения последствий атаки или воздействия вредоносного ПО;

8) Закрыть инцидент, если факт вредоносного воздействия или аномальной активности не подтвердился;

9) Внести в наборы исключений файл или программу, если произошло ложноположительное срабатывание, и т.д.

Если рассматривать работу аналитика с точки зрения проактивного поиска угроз, то наибольшую ценность для такого рода деятельности представляет страница **Активность**. Подробная информация о проактивном поиске на странице **Активность** содержится в подразделе 11.26.

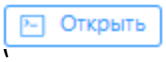
В верхней части окна Программы с помощью значка  можно переключиться на темную тему. В этой же области, рядом со значками переключения между темной и светлой темой, при наличии проблем на сервере появится значок  , который сигнализирует о необходимости обращения аналитика к сервисному инженеру, осуществляющему настройку состояния подсистемы мониторинга сервера (это могут быть такие

решения, как Gatus или Zabbix), если такие решения настроены для сервера EDR. Если такой настройки нет, то необходимо обратиться к разработчикам Программы для дополнительной консультации.

11.2 Онлайн-терминал

Онлайн-терминал – это инструмент для управления операционной системой, на которой установлен агент, позволяющий выполнять команды в режиме онлайн-сессии, то есть онлайн-терминал предоставляет возможность управлять удаленной конечной точкой и выполнять действия реагирования на конечной точке в режиме реального времени. Онлайн-терминал работает как интерпретатор командной строки.

На данный момент не предусмотрено отображение прогресса исполнения команд, а также нет возможности прервать исполнение.

Кнопка онлайн-терминала  находится на горизонтальной панели управления рядом с кнопками быстрого перехода к открытым разделам () и сворачивания боковой панели (), которая позволяет устанавливать с агентом сессию live-терминала и отправлять команды без задержек. Также вызов онлайн терминала производится нажатием кнопки **Открыть** (

) в области **Управление** на странице **Агент**.

Чтобы соединиться со средой выполнения команд, необходимо нажать кнопку **Открыть сессию**. После этого выбор агента осуществляется в окне **Открытие терминальной сессии** в списке агентов. В список попадают активные на данный момент агенты. Параллельно можно открывать несколько сессий. Для добавления дополнительной сессии в окне онлайн-терминала необходимо нажать кнопку (

).

С помощью онлайн-терминала аналитик может:

– выполнять диагностические и реагирующие команды на удалённой машине;

– управлять процессами, файлами, ключами реестра, сетевыми соединениями и сетевой изоляцией;

– загружать файлы с агента в централизованное Хранилище и обратно;

– снимать дампы памяти процессов и инициировать сканирование файловой системы;

– отправлять пользователю уведомления и управлять иконкой агента в системном трее;

– вести журнал введённых команд и повторно использовать их без ручного перенабора.

В списке выбора агента отображается только 20 случайных активных агентов. Для поиска нужного агента необходимо уточнить его имя или добавить агента по группе. Фильтр выбора агента по группе находится

справа от строки выбора агента (). После выбора агента создается активная сессия и состояние подключения меняется на **Подключено,** а связь с агентом отображается как **Установлена**.

Каждая открытая сессия — это самостоятельное защищённое соединение с одним агентом. Аналитик может одновременно работать с несколькими агентами, переключаясь между вкладками сессий внутри одного окна онлайн-терминала.

Чтобы завершить сессию, необходимо нажать кнопку **Закрыть сессию** (). После этого сессия закроется. Нажатие кнопки **Свернуть окно терминала** () рядом с кнопкой полноэкранного режима закрывает окно онлайн-терминала без закрытия сессии.

После закрытия сессии вся её внутренняя история выполнения команд (вывод агента) удаляется.

Примечание

Сессия может прерваться, если онлайн-терминал бездействует в течение восьми часов (при этом во время бездействия должна сохраняться связь между агентом и сервером).

В онлайн-терминале можно выполнять нативные команды RT Protect EDR. Список этих команд отображается на панели справа в окне онлайн-терминала (кнопка **Команды**).

Примечание

Для получения справки по встроенной команде, необходимо вызвать команду с одним из параметров: **/h**, **/help**, **-h**, **--help**, **/?**. Для всех остальных команд необходимо использовать параметр **/?**.

В случае, если происходит ошибка при открытии или в процессе работы сессии, необходимо нажать кнопку **Переоткрыть сессию** ().

Для отправки команды онлайн-терминала используется клавиша **Enter**. Сочетание клавиш **CTRL+Enter** позволяет перейти на новую строку при написании команды. Сочетание клавиш **CTRL+стрелка вверх/вниз**

позволяет передвигаться по истории команд, кроме того, историю команд можно просмотреть на панели справа. Клавиша **Tab** позволяет выполнить автозавершение команды (из списка команд).

В окне онлайн-терминала отображается история введенных команд (кнопка ). При нажатии кнопки открывается история команд, которую при необходимости можно очистить с помощью кнопки **Очистить историю команд**.

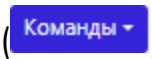


Примечание

Функция онлайн-терминала доступна только пользователям с включённым правом «Доступ к терминалу реагирования».

По умолчанию онлайн-терминал отображается в виде боковой панели. Чтобы развернуть его на всю площадь окна браузера, необходимо нажать иконку полноэкранного режима в заголовке панели (). Повторное нажатие возвращает панель в исходный размер. Полноэкранный режим удобен при работе с большими объёмами вывода или при одновременном анализе нескольких сессий.

11.2.1. Нативные команды (агенты Windows и Linux)

Для удобства аналитиков основные нативные команды, используемые для управления хостами с установленными агентами, заданы в списке в правой части окна (

). Команды содержат краткое описание ().

Список нативных команд:

– admin_msg (не поддерживается на данный момент в Linux);

– block (не поддерживается на данный момент в Linux);

– drop (не поддерживается на данный момент в Linux);

– fsscan;

– get;

– get-log (не поддерживается на данный момент в Linux);

– help;

– memdump;

– memscan (не поддерживается на данный момент в Linux);

– net_contain;

– put;

– remed (не поддерживается на данный момент в Linux);

– reset-errors (не поддерживается на данный момент в Linux);

– startas (не поддерживается на данный момент в Linux);

– stop;

– tray (не поддерживается на данный момент в Linux);

Команда **admin_msg** – отправляет сообщение на компьютер с агентом. Команда выполняется согласно синтаксису admin_msg <Сообщение> [-b64] [-i=<Тип значка>] [-t=<Заголовок>], где:

<Сообщение> – текст сообщения;

<Тип значка> – тип значка сообщения (0 – нет значка, 1 – информация, 2 – предупреждение, 3 – ошибка, по умолчанию используется тип значка информация);

<Заголовок> – заголовок сообщения (по умолчанию содержит название Программы);

-b64 – указывается, если сообщение закодировано в формате base64.

Примеры написания команды:

admin_msg "Сетевой доступ будет заблокирован на время проведения расследования" – отправка сообщения, заданного в текстовом виде;

admin_msg 0JzQvdC+0LPQvtGB0YLRgNC+0YfQvdC+0LUK0YHQvtC+0LHRidC10L3QuNC1 -b64 – отправка UTF-сообщения, заданного в формате base-64 (удобно ипользовать, если сообщение содержит переносы строк и другие служебные символы);

admin_msg "Компьютер будет заблокирован через 1 минуту" -i=2 -t="Предупреждение" – отправка сообщения с заголовком и предупреждающим типом значка.

Команда **block** – добавляет, удаляет и отображает список блокировок, установленных на агенте.

Команда выполняется согласно синтаксису:

block

<set

<<cmdl <Комбинация командных строк> [-b64]> |

<file <Хеш файла | Имя файла> [-h]> |

<net <IP | Хост>[:Порт]>>

[-ttl <Время жизни>] [-force] [-approve]> |

<list [cmdl | file | net] [-csv]> |

<del

<cmdl <Комбинация командных строк> [-b64]> |

<file <Хеш файла | Имя файла> [-h]> |

<net <IP | Хост>[:Порт]>> |

<id <ID блокировки>

<*>>

Где:

1) Действия:

– set – добавляет новую/обновляет существующую блокировку;

– list – отображение списка блокировок;

– del – удаление блокировки.

2) Типы блокировок:

– cmdl – блокировка запуска по командной строке;

– file – блокировка доступа к файлу;

– net – блокировка доступа к сетевому эндпоинту.

3) Флаги (Комбинация командных строк - комбинация из командной строки процесса, его родителя и прародителя, разделенные пробелами).

– b64 – указывается, если командные строка закодирована в формате base64;

– h – указывается, если указан хеш файла;

– id – указывается, если удаление блокировки осуществляется по ID;

– ttl – время жизни блокировки в секундах (по умолчанию: 3600 сек);

– force – опция "Приоритет над исключениями";

– approve – опция "Блокировка действует и в контексте критических системных процессов";

– csv - Указывается, если отображение списка блокировок необходимо выполнить в формате csv

– * Указывается для команды "del", если требуется удалить все блокировки

Примеры написания команды **block**:

– block set cmdl * * -install -ttl 1 – добавляет блокировку запуска по командной строке (командная строка прародителя="*", родителя="*", процесса="-install") с временем жизни 1 минута;

– block set file test.exe -force –- добавляет блокировку доступа к файлу "test.exe" с опцией "Приоритет над исключениями":

– block set file e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 -h -force –approve – добавляет блокировку доступа к файлу по хешу и опциями "Приоритет над исключениями" и "Блокировка действует и в контексте КСС";

– block set net test.ru – добавляет блокировку доступа к доменному имени "test.ru";

– block set net 192.168.0.1 – добавляет блокировку доступа к IP-адресу "192.168.0.1";

– block list – отображает список всех блокировок;

– block list cmdl – отображает список блокировок запуска по командной строке;

– block del id 1 – удаляет блокировку с ID=1;

– block del file test.exe - удаляет блокировку доступа к файлу "test.exe";

– block del * – удаляет все блокировки;

– block clear – удаляет все блокировки;

– block clear file – удаляет все блокировки доступа к файлу.

Команда **drop** – принудительно завершает сетевое соединение.

Команда выполняется согласно синтаксису drop [-id|-ep] <fluuid или flow или endpoint> [-w admin|ti], где

– -id – fluuid или flow сетевого соединения;

– -ep – endpoint, все сетевые соединения с которым необходимо завершить (в формате hostname:[port]);

– -w – кто завершил сетевое соединение: admin – администратор, ti – TI платформа (по умолчанию: admin).

Примеры написания команды **drop**:

drop -ep www.malware.net – завершает все сетевые соединения с www.malware.net;

drop -ep www.malware.net:4444 – завершает все сетевые соединения с www.malware.net по порту 4444;

drop -ep 192.168.10.10:5555 – завершает все сетевые соединения с 192.168.10.10 по порту 5555;

drop -id c24bba95-9d6b-01da-2d12-000000000000 – завершает сетевое соединение с уникальным идентификатором (поле fluuid в событии) c24bba95-9d6b-01da-2d12-000000000000;

drop -id 2096738 – завершает сетевое соединение с идентификатором (поле flow в событии) 2096738.

Команда **fsscan** выполняется согласно синтаксису fsscan <директория проверки> и требует наличия на агенте правил сканирования по YARA-правилам для файла, по которым и будет производиться сканирование. В случае запуска команды без указания директории, будет осуществлено сканирование файловой системы, начиная с корневого каталога.

Команда **get** – загружает файл в файловое хранилище EDR.

Команда выполняется согласно синтаксису get [-f] <Полный путь до файла> [-t <ti или cloud>] [-r] [-xl] [-y], где:

-f –путь до файла;

-t – тип хранилища для загрузки файла (ti – ti-платформа, cloud – хранилище EDR, по умолчанию берется тип хранилища cloud);

-r – удаление файла после успешной загрузки (по умолчанию: файл не удаляется);

-xl – разрешить загрузку файла больше 32 МБ (по умолчанию: ограничение на макс. размер загружаемого файла 32 МБ)

-y – перезаписать файл в хранилище.

Пример написания команды:

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" (загрузка файла в хранилище EDR);

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" -t cloud (загрузка файла в хранилище EDR);

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" -t ti (загрузка файла на ti-платформу).

Команда **get-log** – загружает логи агента в файловое хранилище, команда выполняется согласно синтаксису get-log <Наименование лога>, где наименование лога агента принимает следующие значения:

driver – лог драйвера;

usb – лог usb-драйвера;

service – лог службы.



Совет

Логи драйвера на хосте можно также собрать в папке C:\Windows\VrpntMetadata, логи USB-драйвера в папке C:\Windows\VrpusbcMetadata, а логи службы в папке C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR.

Команда **help** – позволяет получать справочную информацию о списке основных команд онлайн терминала и их кратком описании. Чтобы узнать справочную информацию о конкретной команде, используется параметр **/?**, например, dir /?.

Команда **memdump** – сохраняет снимок памяти указанного процесса в файл. Файл сохраняется в директорию dumps (в ProgramData\<директория агента>). Команда выполняется согласно синтаксису: memdump {[-id] <UUID процесса> | <PID>}.

Пример написания команды:

memdump 2260

memdump -id 2260

memdump {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

memdump -id {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

В результате выполнения команды в директории **C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\dumps** будет создан файл с дампом процесса.

Команда **memscan** – сканирует память указанного процесса на наличие вредоносного кода. Команда выполняется согласно синтаксису: memscan {[-id] <UUID процесса> | <PID>}, где:

pid – это идентификатор процесса (вместо PID процесса можно указать его уникальный идентификатор в RT Protect EDR, то есть UUID).

Пример написания команды:

memscan 1080

memscan -id 1080

memscan {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

memscan -id {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

Команда **net_contain** – управляет сетевой изоляцией агента. Команда выполняется согласно синтаксису net_contain [0|off|false|1|on|true], где значение 0, off и false означают, что изоляция агента будет выключена, а 1, on и true, что изоляция будет включена. **Net_contain** без аргументов показывает текущее состояние изоляции агента.

Примеры написания команды:

net_contain 0 – изоляция сети выключена;

net_contain 1 – изоляция сети включена;

net_contain false – изоляция сети выключена;

Команда **put** – загружает файл с сервера EDR на машину с установленным агентом. Команда выполняется согласно синтаксису put [-u] <Ссылка для загрузки> [-w <Расположение файла на агенте>] [-y] [-n <Новое имя файла>], где:

-u – это ссылка для загрузки (ссылку можно получить во вкладке **Загрузка файлов в разделе** Хранилище);



Примечание

Ссылка может быть постоянной или временной (временная ссылка действительна в течение 24 часов).

-w – расположение файла на агенте (директория, в которую загружается файл; если директория не существует, то она создается, по умолчанию **C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\downloads**), для агента Linux директория по умолчанию (**opt\avd\downloads**);

-y – перезапись существующего файла (по умолчанию перезаписи нет);

-n – новое имя файла (по умолчанию имя берется из ссылки для загрузки).

Примеры написания команды:

1) Команда загрузки файла на машину с агентом по пути C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\download\first_aid_kit.exe:

put https://<адрес_сервера>/api/storage/user/object/<UUID-объекта>/first_aid_kit.exe;

2) Команда загрузки файла на машину с агентом по пути C:\Tools\file_ver_1.exe и переименование файла:

put https://<адрес_сервера>/api/storage/user/object/<UUID-объекта>/first_aid_kit.exe -w C:\Tools -n file_ver_1.exe.

Команда **remed** – ремедиация файловых и реестровых операций (возвращение состояния файловой и реестровой системы к исходному состоянию, до воздействия программ-шифровальщиков).



Важно

Следует обратить внимание, что ремедиация не работает для файловой системы FAT 32

Команда выполняется согласно синтаксису:

remed <Действие: clean или restore> [Параметры] Действие clean – очистить хранилище, restore – ремедиация файлов/реестра.

Параметры действия restore:

– hid – ID группы процессов <-range <Начало/Конец>><-files и/или -registry>;

Например: 2026-02-11T10:00:00/2026-02-11T18:00:00 или

2026-02-20T14:08:29.699050200Z/2026-02-20T25:08:10.699050200Z

– files – ремедиация файлов (по умолчанию: выключен);

– registry – ремедиация ключей\значений реестра (по умолчанию: выключен).

1) Параметры действия clean:

Максимальный возраст файлов.

Допустимые суффиксы:

– d (дни);

– h (часы),

– m (минуты, по умолчанию используется значение из профиля Антишифра);

– all (удалить все файлы).

Примеры выполнения команд:

1) Ремедиация файлов группы процессов HID={FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} за временной диапазон от 2026-02-11T10:00:00 до 2026-02-11T18:00:00 (локальное время агента):

```
remed restore -hid {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -range 2026-02-11T10:00:00/2026-02-11T18:00:00 -files
```

2) Ремедиация файлов и реестра группы процессов HID={FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} за временной диапазон от 2026-02-20T14:08:29.699050200Z до 2026-02-20T25:08:10.699050200Z (UTC время):

```
remed restore -hid {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -range 2026-02-20T14:08:29.699050200Z/2026-02-20T25:08:10.699050200Z -files -registry
```

3) Удаляет зарезервированные файлы старше 10 часов:

```
remed clean 10h
```

4) Удаляет все зарезервированные файлы:

```
remed clean all
```

Команда **reset-errors** – сбрасывает счетчики прикладных и системных ошибок на агенте, команда выполняется согласно синтаксису reset-errors [all | app | sys], где:

all – сброс всех счетчиков ошибок (выполняется по умолчанию);

app – сброс счетчика прикладных ошибок;

sys – сброс счетчика системных ошибок.

Примеры выполнения команд:

Сброс счетчиков системных и прикладных ошибок:

```
reset-errors
```

Сброс счетчика прикладных ошибок:

```
reset-errors app
```

Сброс счетчика системных ошибок:

```
reset-errors sys
```

Команда **shutdown** – позволяет управлять питанием.

Пример использования команды:

shutdown /r – полная перезагрузка компьютера после завершения работы.

Команда **startas** – запускает процесс под определенным пользователем. Команда выполняется согласно синтаксису startas [-cmd] <Командная строка> [-u <Имя пользователя>] [-ws {normal | hidden | minimized | maximized}], где:

-cmd – это командная строка для запуска;

-u – имя пользователя с активной сессией (по умолчанию используется активная сессия пользователя);

-ws – стиль окна запускаемого процесса: normal (по умолчанию), hidden, minimized, maximized.

Пример написания команды:

startas calc.

Команда **stop** – завершает процесс. Команда выполняется согласно синтаксису sstop <[-id] UUID-процесса> | <-pid ID-процесса> | <-hid HID-процесса> [-hive [0]] [-c <Статус завершения процесса>] [-w admin|ti] [-t <Тип сообщения>], где:

-id – это UUID процесса;

-pid – ID процесса;

-hid – идентификатор группы процесса;

-hive – признак завершения группы процессов (0 – не завершать группы процессов)

-c – статус завершения процесса (по умолчанию 0);

-w – кто завершил процесс: admin – администратор, ti – ti-платформа (по умолчанию admin) Если установлено значение ti, то завершается процесс и другие процессы его группы, для отмены завершения группы процессов необходимо передать параметру -hive значение 0;

-t – тип сообщения, определяет уровень уведомления о завершении процесса: info, warning, error (по умолчанию: если параметр -w установлен как admin, то -t принимает значение info, если параметр -w установлен как ti, то -t принимает значение error).

Примеры написания команды:

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} – завершает процесс с UUID={FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4};

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti – завершает процесс с PID=31415;

stop -pid 31415 –hive – завершает процесс PID=31415 и другие процессы его группы;

stop -hid 137e583f-134b-01db-c200-000000000000 – завершает группу процессов HID=137e583f-134b-01db-c200-000000000000.

Формат команды для кнопки **Завершить процесс**: stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}

Формат команды для завершения процесса по требованию TI-платформы: stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti

Команда **tray** – управляет значком и уведомлениями в трее. Команда выполняется согласно синтаксису tray [<Уровень>], где:

[<Уровень>] 0 – нет значка в трее, уведомления не выводятся;

[<Уровень>] 1 – есть значок, уведомления не выводятся;

[<Уровень>] 2 – есть значок, показывать только критические уведомления;

[<Уровень>] 3 – есть значок, показывать все уведомления.

Пример написания команды:

tray (выводит информацию о текущем состоянии значка трея);

tray 2 (переводит значок трея в режим показа только критических уведомлений).

11.2.2. Описание других команд, работающих на агенте Windows (популярные команды интерпретатора и нативные команды)

Команда **copy** – копирует один или несколько файлов из одного места в другое. Команда выполняется согласно синтаксису copy [опции] [источник] [назначение].

Примеры написания команды copy:

copy file.txt C:\backup\ – копирует file.txt в папку C:\backup;

copy /Y data.log backup.log – копирует с заменой без подтверждения.

Команда **dir** – выводит список файлов и подкаталогов в текущей или указанной директории. Команда выполняется согласно синтаксису dir [диск:][путь][имя_файла] [опции].

Примеры написания команды dir:

dir /A:D – вывод только папок в текущем каталоге;

dir *.txt – поиск файлов по маске .txt.

Команда **enable** – включает управление защитой агента, установленного с параметром /no_driver.

Пример: enable.



Совет

Локально перезапуск службы можно осуществить с помощью команды Setup /noUI /update, запущенной из каталога, в котором находится установочный файл текущего агента.

Команда **inventory** – обновляет информацию об установленном ПО, обновлениях и драйверах агентов.

Команда **ipconfig** – служит для отображения сетевых настроек TCP/IP и управления ими. Примеры использования команды:

ipconfig /all – подробная конфигурация всех адаптеров;

ipconfig /flushdns – очистка DNS-кеша.

Команда **mkdir** – позволяет создавать новые папки. Пример написания команды:

mkdir папка1 папка2 папка3 – создает 3 папки с указанными именами в текущей директории.

Команда **move** – используется для перемещения файлов и папок. Команда выполняется согласно синтаксису move [источник] [назначение].

Пример написания команды:

move C:\Files\old.txt C:\Backup\new.txt – файл old.txt переместится в папку C:\Backup и переименуется в new.txt.

Команда **netlimit** – ограничивает максимальную скорость отправки событий. Команда выполняется согласно синтаксису: netlimit [<Макс. скорость>], где:

<Макс. скорость> – Максимальная скорость отправки (Кбит\с) (значение 0: без ограничений).

Пример написания команды:

1) Вывод текущего ограничения максимальной скорости отправки:

netlimit

2) Установка ограничения максимальной скорости отправки 64 Кбит\с (минимально рекомендованная скорость передачи для утилиты curl, используемой в Программе для передачи данных):

netlimit 64

3) Снятие ограничения на максимальную скорость:

netlimit 0

Команда **netstat** – позволяет анализировать сетевые подключения, статистику интерфейсов и состояние портов. Команда выполняется согласно синтаксису netstat [опции]. Пример выполнения команды:

netstat -ano – показывает все активные подключения и PID процессов.

Команда **reg** – встроенная утилита в Windows для работы с реестром (Registry) из командной строки. Она позволяет:

1) Добавлять, изменять и удалять ключи и параметры реестра.

2) Экспортировать и импортировать ветки реестра.

3) Сравнивать разделы реестра.

4) Загружать и выгружать кусты (hives) реестра (например, для редактирования реестра другого пользователя или системы). Команда выполняется согласно синтаксису reg [операция] [параметры].

Пример выполнения команды:

reg query HKLM\Software\Microsoft\Windows\CurrentVersion – выведет все параметры в этом ключе.

Команда **restore** (команда относится к устаревшему функционалу, так как функции резервирования больше не используются в RT Protect EDR, поддерживается первыми и вторыми версиями агента, команда оставлена для совместимости с этими версиями) – восстанавливает зарезервированные файлы. Команда выполняется согласно синтаксису restore [-id] <UUID-процесса> [-c], где:

-id – это UUID процесса;

-c – аргумент для удаления созданных файлов.

Пример написания команды:

restore -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}.

Команда **tasklist** – выводит список всех запущенных процессов (программ и служб) в командной строке, предоставляет информацию об именах процессов, их PID (идентификаторах), потреблении памяти и других параметрах. Команда выполняется согласно синтаксису tasklist [параметры]. Пример написания команды:

tasklist /M ntdll.dll – показать процессы, использующие определённый DLL-файл.

Команда **trace** управляет трассировкой агента. Команда выполняется согласно синтаксису trace <-start или -stop> <-svc или -drv> [маска логируемых подсистем (по умолчанию трассируются все подсистемы: 0xFFFFFFFF)][уровень логирования (по умолчанию: 0xFF)][-s], где:

-start – запускает трассировку;

-stop – останавливает трассировку;

-svc – управление трассировкой службы;

-drv – управление трассировкой драйвера;

-usb – управление трассировкой USB-драйвера;

– [маска логируемых подсистем] – маска трассируемых подсистем службы или драйвера (используется в команде -start);

– [уровень логирования] – 0x5 (Verbose), 0x4 (Informational), 0x3 (Warning), 0x2 (Error), 0x1 (Critical), (используется в команде -start) (по умолчанию уровень логирования определяется как **Verbose**);

– -s – аргумент, позволяющий не удалять файл трассировки после остановки (по умолчанию файл будет удален после удачной отправки на сервер), (используется в команде -stop).

Маски логируемых подсистем и наименования этих подсистем приведены в таблице 57.

Таблица 41 – Маски логируемых подсистем

Подсистемы	Маски
Маски логируемых подсистем для службы агента	
TRACE_SERVICE_ENGINE	0x00000001
TRACE_EVENTS	0x00000002
TRACE_METADATA_ENGINE	0x00000004
TRACE_AGENT_UPDATE	0x00000008
TRACE_FILE_SCANNER	0x00000010
TRACE_NETWORK_CONTAINMENT	0x00000020
TRACE_SESSION_MONITOR	0x00000040
TRACE_ETW_CONSUMER	0x00000080
TRACE_ETW_DOTNET_LOAD_IMAGE_MONITOR	0x00000100
TRACE_ETW_RPC_MONITOR	0x00000200
TRACE_ETW_KERBEROS_ATTACK_MONITOR	0x00000400
TRACE_ETW_SYSTEMTIME_CHANGED_MONITOR	0x00000800
TRACE_ETW_WMI_ACTIVITY_MONITOR	0x00001000
TRACE_ETW_MONITORS	0x00002000
TRACE_TERMINAL	0x00004000

Подсистемы	Маски
TRACE_WMI_MONITOR	0x00008000
TRACE_SYSTRAY	0x00010000
TRACE_MS_GROUP_POLICY	0x00020000
TRACE_YARA	0x00040000
TRACE_ML	0x00080000
Маски логируемых подсистем для драйвера агента	
TRACE_REGISTRY_MONITOR	0x00000001
TRACE_REGISTRY_MATCHER	0x00000002
TRACE_REGISTRY_CONFIG_PARSER	0x00000004
TRACE_RESERVED1	0x00000008
TRACE_FS_MONITOR	0x00000010
TRACE_FS_MONITOR_SIGN	0x00000020
TRACE_FS_MONITOR_RULES	0x00000040
TRACE_FS_MONITOR_HASHES	0x00000080
TRACE_FS_MONITOR_SCAN	0x00000100
TRACE_FS_MONITOR_DEF_SCAN	0x00000200
TRACE_RESERVED2	0x00000400
TRACE_RESERVED3	0x00000800
TRACE_ARW	0x00001000
TRACE_ARW_BLOCK_OPERATION	0x00002000
TRACE_ARW_RESERVED1	0x00004000
TRACE_ARW_RESERVED2	0x00008000
TRACE_PATH_CLASSIFY	0x00010000
Маски логируемых подсистем для USB-драйвера	
TRACE_BASE	0x00000001
TRACE_PNP	0x00000002
TRACE_AGENT_INTERACTION	0x00000004

Примеры написания команды:

1) Трассировка всех подсистем службы с уровнем логирования Verbose (если не указывается конкретный уровень логирования, то применяется уровень логирования по умолчанию):

```
trace -start –svc
```

2) Трассировка подсистем службы: TRACE_SESSION_MONITOR и TRACE_WMI_MONITOR, с уровнем логирования Warning:

```
trace -start -svc 0x8040 0x3
```

3) Остановка трассировки службы:

trace -stop -svc

4) Трассировка всех подсистем драйвера с уровнем логирования Verbose:

trace -start -drv

5) Трассировка подсистем драйвера TRACE_REGISTRY_MONITOR, TRACE_REGISTRY_MATCHER, TRACE_REGISTRY_CONFIG_PARSER с уровнем логирования Error:

trace -start -drv 0x7 0x2

6) Остановка трассировки драйвера:

trace -stop -drv

7) Трассировка всех подсистем USB-драйвера с уровнем логирования Verbose:

trace start usb

8) Остановка трассировки USB-драйвера:

trace -stop -usb

Команда **type** – выводит содержимое текстового файла в командной строке. Команда выполняется согласно синтаксису type [путь_к_файлу]. Пример использования команды:

type D:\file.txt – выводит содержимое файла file.txt.

Команды для управления трассировкой WPP агента Windows:

1) Трассировка основного драйвера:

Запуск трассировки – logman.exe start agent_drv -rt -ets -p {F550C865-C532-4133-8EFE-E55DFC0D94A2} 0xFFFFFFFF 0xFF -o C:\Temp\AgentDrvTrace.etl;

Остановка трассировки – logman.exe stop agent_drv –ets;

2) Трассировка USB-драйвера:

Запуск трассировки – logman.exe start agent_usb -rt -ets -p {FC723033-2348-4E3E-89B8-1BCCCF57B7C2} 0xFFFFFFFF 0xFF -o C:\Temp\AgentUsbTrace.etl;

Остановка трассировки – logman.exe stop agent_usb –ets;

3) Трассировка службы:

Запуск трассировки – logman.exe start agent_svc -rt -ets -p {F0E2F7DA-9B90-4761-A7D4-E58F9DA05DF3} 0xFFFFFFFF 0xFF -o C:\Temp\AgentSvcTrace.etl;

Остановка трассировки – logman.exe stop agent_svc –ets.

Команда **ramdump** сохраняет дамп физической памяти в файл. Команда выполняется согласно синтаксису ramdump list | all | <начало диапазона>:<длина диапазона> [-f, --file FILE][-y, --yes] [-i, --ignore-errors].

Действия:

list – Вывод на экран списка доступных диапазонов физической памяти;

all – сохранение дампов всех доступных диапазонов физической памяти в файлы;

<начало диапазона> – шестнадцатеричное число, должно быть кратно размеру страницы памяти (0x1000);

<длина диапазона> – шестнадцатеричное число, должно быть кратно размеру страницы памяти (0x1000).

-f, --file FILE – путь\имя файла дампа (если не задано, то файл будет автоматически создан в каталоге \"ProgramData\<каталог агента>\Dumps\").

-y, --yes – перезапись файла дампа, если он существует (по умолчанию перезаписи нет);

-i, --ignore-errors – игнорирование ошибок в процессе чтения памяти (по умолчанию не игнорируются).

Примеры команд:

Вывод списка доступных диапазонов физической памяти – ramdump list;

Сохранение дампов всех доступных диапазонов физической памяти в файлы – ramdump all;

Сохранение дампов всех доступных диапазонов физической памяти в файл \"my.bin\" в каталоге в каталоге \"C:\\dumpout\\\" с перезаписью предыдущего – ramdump -a -f \"C:\\dumpout\\my.bin\" -y;

Сохранение заданного диапазона физической памяти в файл в каталог \"ProgramData\<каталог агента>\Dumps\" с игнорированием ошибок чтения памяти – ramdump 0x30000:0x1000 --ignore-errors.

11.2.3. Команды Linux

Онлайн-терминал для агентов Linux поддерживает команды командной оболочки bash, а также проприетарные команды EDR (put, get, memdump и т.д.) Полный список нативных команд, доступных для Linux-агента, можно вызвать, набрав в онлайн-терминале команду **help** в открытой сессии Linux-агента. Чтобы открыть описание конкретной команды, необходимо ввести имя команды с аргументом **–help.**

get – загрузить файл на сервер;

put – загрузить файл на агент;

stop – остановить процесс;

inventory – обновить информацию об установленном ПО;

cmode – установить режим защиты: KMOD или eBPF;



Примечание

В режиме eBPF команда **net_contain** работает для операционных систем, у которых версия ядра Linux ниже 5.8.

memdump – собрать дамп памяти процесса;

fsscan – выполнить сканирование директории с помощью YARA;

net_contain – управление сетевой изоляцией агента (работает только в режиме ядра).

Команды **get**, **put**, **stop**, **inventory**, **memdump** и **net_contain** идентичны командам, выполняемым на агентах Windows.



Совет

Чтобы получить в Хранилище EDR лог агента Linux необходимо указать в команде **get** путь **/var/log/avd.log**

Команда **fsscan** выполняется согласно синтаксису fsscan <директория проверки> и требует наличия на агенте правил сканирования по YARA-правилам для файла, по которым и будет производиться сканирование. В случае запуска команды без указания директории, будет осуществлено сканирование файловой системы, начиная с корневого каталога. Результат сканирования сохраняется в директории **/opt/avd/reports**.

Пример команды:

`fsscan /opt`

Команда `cmode <0|1>`

0 – KMOD (режим модуля ядра).

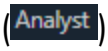
1 – BPF (режим eBPF).



Примечание

Команда **memdump** сохраняет дамп процесса в директорию, которая создается после исполнения команды (**/opt/avd/dumps**)

11.3 Операции с профилем пользователя

Чтобы открыть меню операций с профилем пользователя, необходимо кликнуть на имя пользователя (

) в верхней части страницы. Откроется меню, состоящее из двух пунктов:

1) **Профиль** (откроется страница, на которой аналитик может изменить данные своей учетной записи);

2) **Выход** (выход из учетной записи пользователя).

На странице **Профиль пользователя** аналитик может отредактировать данные своей учетной записи, а также просмотреть информацию по открытым сессиям и при необходимости выйти из всех открытых сессий на всех устройствах, с которых был осуществлен вход в Программу.

В некоторых случаях аналитику может быть удобно получать уведомления об инцидентах на свою электронную почту, для этого ему необходимо зайти на страницу **Профиль пользователя** и установить флажок **Получать уведомления о новых инцидентах на почту**, после чего нажать кнопку **Сохранить**. Кроме того, аналитик может настроить двухфакторную аутентификацию при входе в учетную запись. Чтобы это сделать, ему необходимо:

1) Установить в профиле флажок **Использовать двухфакторную аутентификацию**.

2) Нажать кнопку **Сохранить**.

После применения двухфакторной аутентификации аналитику во время входа в учетную запись будет необходимо ввести числовой код, который приходит на почту, указанную в профиле. Числовой код актуален в течение двух минут после отправления на почту.

В профиле аналитик может также поменять следующие данные:

1) Имя;

2) Фамилия;

3) Email.

Аналитик может при наличии соответствующих прав в любой момент изменить пароль на странице своего профиля, для этого необходимо нажать кнопку **Сменить пароль** и в открывшемся окне ввести текущий и новый пароль с учетом требований, указанных в нижней части окна (рис. 12). Для завершения операции необходимо нажать кнопку **Сохранить**.

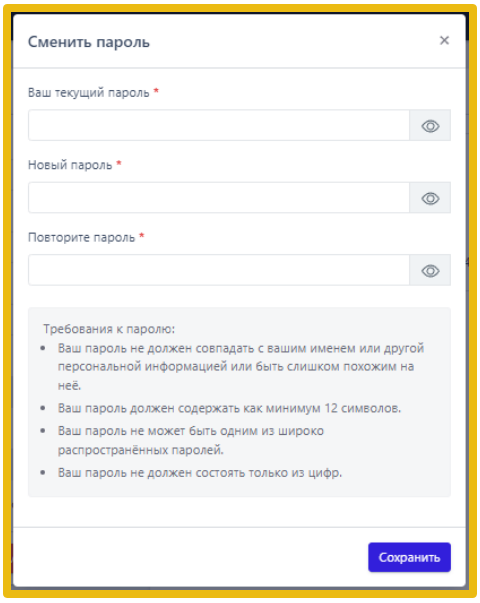


Рисунок 12 – Окно «Сменить пароль»

Чтобы выйти из текущего профиля, аналитику необходимо нажать кнопку пункта меню **Выход**, после чего откроется окно входа на сервер управления Программы (рис. 13).

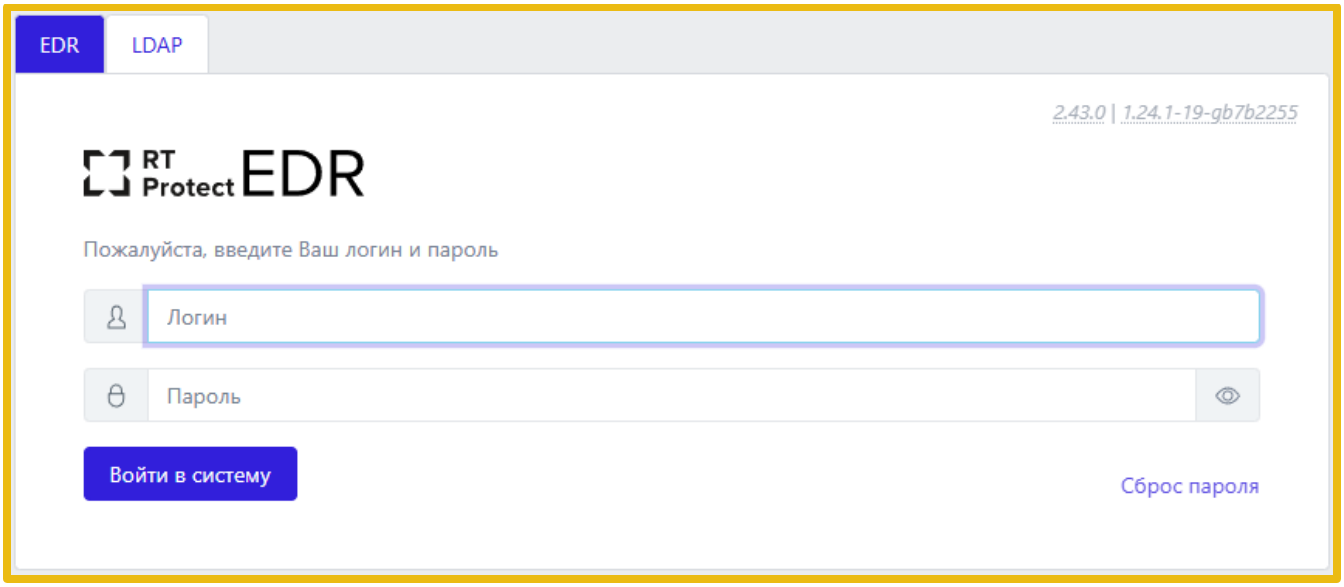


Рисунок 13 – Окно входа в Программу

Аналитик может войти как обычным пользователем, созданным на странице **Пользователи** на сервере управления EDR, так и пользователем LDAP (созданным с помощью LDAP-сервера).

В некоторых случаях аналитику, входящему в систему как обычный пользователь, может потребоваться восстановить пароль в связи с тем, что он может его забыть (операция требует соответствующих прав). Для этого в окне входа в программу находится кнопка **Сброс пароля**, которая позволяет по логину отправить на почту запрос, содержащий ссылку на сброс пароля.

На электронную почту, указанную в профиле пользователя, будет направлено письмо, содержащее ссылку, при нажатии которой в браузере откроется окно. В этом окне аналитик может ввести новый пароль (рис. 14).



Рисунок 14 – Окно восстановления пароля

Пароль должен соответствовать требованиям к паролю, утвержденным парольной политикой Программы:

1) Не должен совпадать с именем пользователя или с другой персональной информацией или быть слишком похожей на нее;

2) Должен содержать как минимум 12 символов;

3) Не должен быть одним из широко распространенных паролей;

4) Не должен состоять только из цифр.

11.4 Расследование инцидентов со страницы «Оповещения»

В Программе предусмотрена система уведомлений о возникновении инцидентов в защищаемой инфраструктуре. Оповещения об инциденте возникают в режиме реального времени при регистрации инцидентов на сервере.

При появлении событий, несущих угрозу, в правой части окна модуля администрирования, открытого в браузере, появляются сообщения о возникновении инцидента (рис. 15).

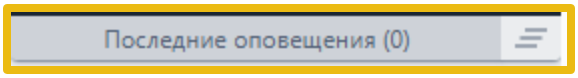


Рисунок 15 – Уведомление о возникновении инцидента

На странице **Оповещения** показывается информация о событиях, происходящих в защищаемой инфраструктуре (в том числе инциденты), в порядке регистрации их на сервере.

На странице аналитик имеет возможность фильтровать информацию об оповещениях, используя различные параметры фильтрации. Приведены следующие фильтры:

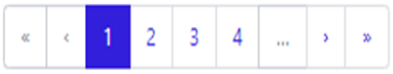
1) **Показывать по** (10, 20, 50, 100) – количество строк отображается согласно выбранному элементу;

2) **Критичность** (**Не задана**, **Информация**, **Низкая**, **Высокая**, **Средняя**, **Критичная**) – оповещения отображаются согласно выбранному критерию фильтрации;

3) **Статус оповещения** (**Не задан**, **Прочитанные**, **Непрочитанные**) – оповещения отображаются согласно выбранному критерию фильтрации;

4) **Тип оповещения** (**Все типы**, **Инцидент**, **Потеря связи с агентом**, **Изменился состав ПО**) – оповещения отображаются согласно выбранному критерию фильтрации.

Элементы навигации и информационные элементы, представленные в окне:



Выбрано: 0 из 8631

Найдено: 8631, показано: с 1 по 10

Прочитать все

–навигация по страницам (переход на первую страницу, переход на предыдущую страницу и т.д.)

– количество выбранных элементов

–общее количество найденных оповещений, количество показанных на странице

–кнопка подтверждения (прочитать все выбранные оповещения)



– кнопка подтверждения (прочитать выбранные оповещения)



– кнопка выбора строки с оповещением

– кнопка навигации в окне фильтрации

– отметить как прочитанные

Аналитик может просмотреть дополнительную информацию по событию (производится кликом по кнопке › . В зависимости от типа оповещения поля таблицы содержат разную информацию (рис. 16).

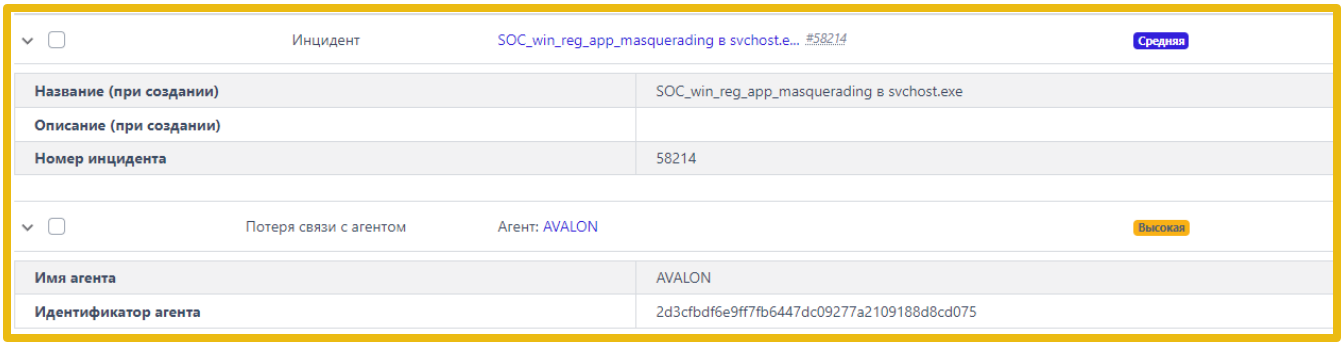


Рисунок 16 – Дополнительная информация о событии

Значение имени, присвоенного инциденту в таблице с информацией о событии, выполняет роль ссылки на страницу **Инцидент**. Для получения подробной информации и редактирования параметров инцидента аналитик может перейти на страницу **Инцидент**, нажав имя-ссылку в поле **Название (при создании)**.

Далее интерес для аналитика может представлять страница **Процесс**. Страница открывается при нажатии в области **Обнаружения** ссылки в виде имени процесса, связанного с событием. Событие-обнаружение может быть частью инцидента или единственным событием выбранного инцидента.

На странице **Процесс** аналитику доступна информация о процессах, предшествовавших возникновению инцидента, а также информация о процессах, ставших его следствием. Информация об этих процессах представлена в виде дерева.

11.5 Работа с деревом процессов

При расследовании инцидента важно понять, каким образом была инициирована вредоносная активность, какой процесс ее запустил и каким образом (через запуск дочернего процесса, загрузку вредоносного модуля или иначе).

Процесс в операционной системе — это экземпляр исполняемой программы, который включает в себя:

1) Код программы (инструкции);
2) Данные (переменные, буферы и т. д.);
3) Состояние выполнения (регистры процессора, счётчик команд, стек);
4) Ресурсы (память, файловые дескрипторы, устройства ввода-вывода).

Дерево процессов – это графическое отображение запуска программ на компьютере с установленным агентом. Дерево процессов состоит из родительских и дочерних процессов. С помощью клика левой кнопкой мыши по исполняемому модулю процесса открывается страница с информацией о процессе и его дочерние процессы (при их наличии).

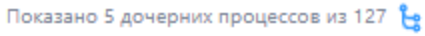
Для детального рассмотрения дерева процессов и изменения его расположения, необходимо использовать кнопки (**Изменить ориентацию дерева**) и (**Изменить размер области дерева**).

После нажатия кнопок и окно отображения дерева процессов увеличится в масштабе и дерево процессов поменяет пространственную ориентацию.

Примечание

В системе RT Protect EDR при построении дерева процессов используется информация о фактическом родителе (инициаторе). В большинстве случаев инициатор и родитель процесса – это один и тот же процесс. При подмене родительского процесса информация о нем включается в событие старта дочернего процесса.

Если у родительского процесса количество дочерних процессов превышает удобное для просмотра количество процессов, то в правом верхнем углу области отображения появится кнопка для загрузки оставшихся процессов в область отображения.

Рядом с кнопкой загрузки дополнительных дочерних процессов показано количество отображаемых дочерних процессов и общее количество дочерних процессов для выбранного родительского процесса ().

Примечание

Значки, визуализирующие процессы, могут различаться по цвету в зависимости от свойств или состояния процесса (– обычный процесс, – главный процесс группы (родитель узла), – процесс заблокирован).

Глубина поиска ограничивается фильтром **Время регистрации события старта процесса** – им удобно пользоваться, чтобы исключить из отображения нерелевантные узлы (процессы, которые существовали ранее, но уже завершились). Снизу от области отображения дерева процессов находится область с подробной информацией о выделенном в данный момент родительском или дочернем процессе.

Вкладки, которые включают большое количество элементов, могут подгружать информацию в течение некоторого времени, в этот момент рядом с именем вкладки отобразится мигающий значок (к примеру,).

После завершения загрузки информации рядом с названием вкладки отобразится количество элементов, на которые так или иначе повлиял процесс, выбранный ранее (к примеру, Реестр (154)).

В таблице отображаются следующие вкладки:

1) Информация;
2) Файлы;
3) Сеть;
4) Реестр;
5) IPC;
6) DLL/SO;
7) Автозапуск;
8) Событие старта;

9) Правила/MITRE.

В нижней части страницы **Процесс** находятся кнопки операций и ссылки:

_ Все события процесса ;

_ Ключевые события процесса ;

_ Распространенность ;

_ Реагирование .

Все события процесса – при нажатии ссылки Все события процесса происходит переход к странице **Активность**, на которой будут представлены все дочерние процессы выбранного родительского процесса.

Ключевые события процесса – перед тем, как перейти по ссылке, необходимо нажать кнопку **Загрузить данные** ( ), после чего при нажатии ссылки происходит переход на страницу **Активность**, на которой отображаются важные события, связанные с процессом. При этом отображаемые события должны подчиняться логике DSL-запроса, указанного в строке **Запрос на языке DSL** (рис. 17).



Примечание

Ключевыми являются события, критичность которых равна или превышает критичность **Низкая,** или события, для которых назначено блокирующее действие.

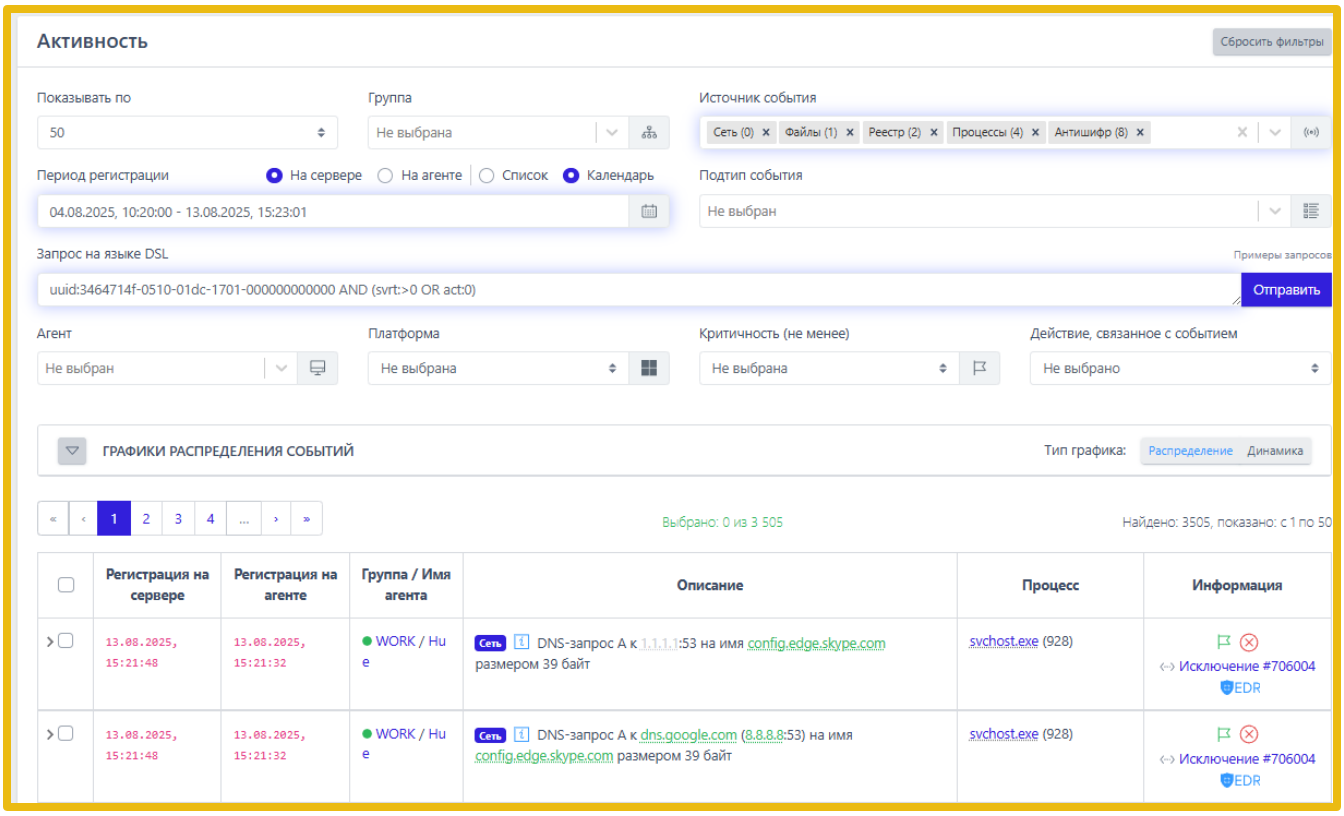


Рисунок 17 – Ключевые события процесса

Распространенность – перед тем, как перейти по ссылке, необходимо нажать кнопку **Загрузить данные** ( ), после чего при нажатии ссылки происходит переход на страницу **Активность**. На странице можно увидеть всех агентов, на которых обнаружен файл с соответствующим хешем.

Реагирование – кнопка позволяет выполнить операции реагирования в рамках выбранного процесса или группы процессов. Кнопка активна, если активен агент, на котором процесс был запущен.

Группа процессов в операционных системах — это совокупность связанных процессов, которые выполняются вместе и управляются как единое целое. Работая группой, каждый из участвующих в ней процессов может выполнять свою особую роль, например, один процесс читает файлы и передаёт данные второму, второй создаёт шифрованные копии, а ещё несколько процессов удаляют исходные файлы. В контексте ИБ и защиты от вредоносной активности объединение процессов в группы позволяет рассматривать всё происходящее в этих в процессах как одно целое, тем самым, не дав вредоносной активности разбиться на отдельные независимые шаги.

Главный процесс группы – это процесс, родитель которого принадлежит другой группе процессов. Главный процесс группы порождает дочерние процессы, однако не все из них входят в общую с ним группу: те, что не входят, становятся главными процессами своих собственных групп и т.д. Таким образом, формируется иерархия групп процессов.

На странице **Процесс** для пользователя доступны следующие операции реагирования:

1) Завершить процесс;
2) Завершить группу процессов;
3) Сделать дамп памяти процесса;
4) Сканировать память процесса;
5) Ремедиация;
6) Блокировка запуска процесса по командной строке;
7) Блокировка доступа к файлу;
8) Удалить файл/каталог;
9) Отправить файл на анализ в TI.

Завершить процесс – операция реагирования, которая завершает выбранный процесс. Для этого автоматически подставляется его **uuid** или **pid**.

Завершить группу процессов – операция реагирования, которая завершает группу процессов. Для этого в окне реагирования автоматически подставляется **hid** (идентификатор группы процессов).

Сделать дамп памяти процесса – операция реагирования, позволяющая сделать дамп памяти процесса. Для этого в окне реагирования автоматически подставляется **uuid** или **pid** процесса.

Сканировать память процесса – операция реагирования, позволяющая сканировать память процесса с помощью YARA-правил (память). В окне реагирования автоматически подставляется **uuid** или **pid** процесса.

Ремедиация – операция реагирования, выполняющая откат действий, запущенных определенным процессом. В окне реагирования автоматически подставляется идентификатор группы процессов (**hid**).

Блокировка запуска процесса по командной строке – операция реагирования, позволяющая блокировать запуск процесса по его командным строкам (родителя, прародителя и самого процесса).

Блокировка доступа к файлу – операция реагирования для полной блокировки доступа к файлу. Блокировка действует по имени или по хешу.

Удалить файл или каталог – операция реагирования, позволяющая удалять заданный файл/каталог.

Отправить файл на анализ в TI – операция реагирования для отправки файла на анализ в инстанс TI-платформы, на которой настроена интеграция с песочницей.

Вкладка «Информация»

В таблице раздела отображается общая информация о процессе. Для этого пользователю показаны следующие поля:

1) Исполняемый модуль;
2) Командная строка;
3) Время старта/завершения;
4) Имя пользователя (SID);
5) SHA-256;
6) Цифровая подпись;
7) Флаги исполняемого модуля;
8) Поведенческие признаки;

Исполняемый модуль – в поле отображается имя модуля исполняемого файла, который инициировал запуск процесса. Рядом с именем находится значок реагирования (), который позволяет загрузить модуль в файловое хранилище для проведения дополнительного анализа.

Командная строка – в поле отображается значение командной строки, которая запустила рассматриваемый процесс.

Время старта/завершения – в поле отображается год, месяц, число и время до секунды, в которое был выполнен старт и завершение рассматриваемого процесса на агенте.

Имя пользователя (SID) – в поле отображается имя пользователя и идентификатор безопасности пользователя, от имени которого был запущен рассматриваемый процесс.

SHA-256 – в поле отображается хеш-сумма исполняемого файла, запустившего процесс. При нажатии ЛКМ на значение хеш-суммы пользователю показывается всплывающее окно с кратким отчетом TI-платформы об исполняемом файле. Рядом с хеш-суммой отображаются две кнопки. Первая кнопка позволяет скопировать

хеш в буфер обмена ( ). Вторая позволяет перейти на страницу **Артефакты TI** для выбранной хеш-суммы ( ).

Цифровая подпись – в поле отображается значение сертификата Code Signing для исполняемого файла рассматриваемого процесса.

Флаги исполняемого модуля – в поле показаны флаги, с которыми исполняется программа, кнопка Показать все... открывает дополнительную область с флагами исполняемого модуля процесса.

Поведенческие признаки – в поле показаны поведенческие признаки программы, кнопка Показать все... открывает дополнительную область с поведенческими признаками процесса.

Вкладка «Файлы»

В таблице вкладки **Файлы** отображается информация о файлах, с которыми связан рассматриваемый процесс (рис. 18).

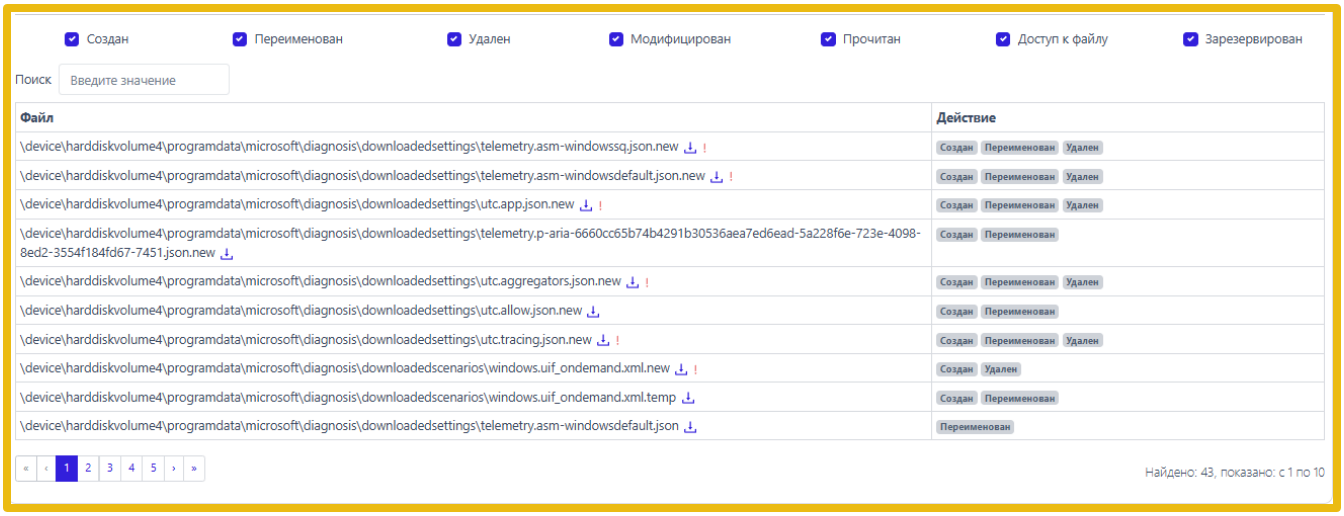


Рисунок 18 – Информация о файлах процесса

Для фильтрации файлов предусмотрена система флажков. Файл, соответствующий выбранному параметру, при снятии флажка не будет отображаться в таблице. Рядом с абсолютным именем файла отображается кнопка загрузки файла ( ) в файловое хранилище для проведения дополнительного анализа с помощью TI-платформы или программы просмотра файлов.

Если среди действий с файлом из списка было удаление, то он помечается значком ! . При наведении курсора мыши на значок пользователю выводится предупреждающее сообщение (рис. 19).

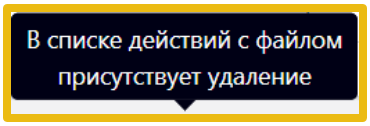


Рисунок 19 – Сообщение о присутствии в списке удаления файла

Для поиска по списку файлов используется фильтр **Поиск**.

Вкладка «Сеть»

Во вкладке **Сеть** отображается информация о сетевых подключениях процесса:

1) Входящие подключения;
2) Исходящие подключения;
3) DNS-запросы;
4) SSL Hello.

Информация о сетевых подключениях представлена в табличном виде.

Таблицы включают в себя следующие поля:

1) IP-адрес;
2) Имя хоста, соответствующее удаленному IP-адресу;
3) Удаленный порт;
4) Локальный порт;
5) Протокол;
6) Тип DNS-запроса;
7) Количество запросов.

IP-адрес – показывает сетевой адрес соответствующего сетевого подключения. При нажатии ЛКМ на значение адреса всплывает окно с кратким отчетом об объекте, полученным от TI-платформы (если это глобальный адрес).

Имя хоста, соответствующее удаленному IP-адресу – в поле отображается доменное имя конечной точки, с которой осуществлялось сетевое соединение, доменное имя также автоматически проверяется TI-платформой (если это не внутренний домен). При нажатии ЛКМ на значение имени аналитик может просмотреть отчет.

Локальный порт – в поле отображается номер порта, по которому осуществлялось сетевое соединение со стороны локального хоста.

Удаленный порт – в поле отображается номер порта, по которому осуществлялось сетевое соединение со стороны удаленного хоста.

Протокол – в поле отображается сетевой протокол, по которому осуществлялось сетевое соединение.

Тип DNS-запроса – показывает типы записей о соответствии имени и служебной информации в системе доменных имён, например, A, AAAA, CNAME, MX и т.д.

Количество запросов – показывает количество запросов SSL HELLO к удаленному хосту.

Вкладка «Реестр»

Во вкладке **Реестр** отображается информация о ключах реестра, с которыми производил действия выбранный процесс.

Информация о ключах реестра представлена в таблице, в которой присутствуют следующие столбцы:

1) **Ключ реестра** – в поле прописывается путь ключа реестра, с которым выбранный процесс производил те или иные действия;

2) **Значение** – в поле отображается значение, которое было внесено выбранным процессом в ключ реестра;

3) **Действие** – в поле отображается действие, которое совершил выбранный процесс с ключом реестра: это может быть внесение данных в значение ключа, удаление ключа, создание нового ключа и т.д.

Вкладка «Взаимодействие процессов»

Во вкладке **Взаимодействие процессов** отображается информация о процессах, взаимодействовавших или взаимодействующих с выбранным процессом.

Информация разбита на две информационные области **Доступ к процессу** и **Доступ к нити процесса** (рис. 20).



Доступ к процессу (6)

Имя исполняемого образа	Запрошенные права	Предоставленные права	Кол-во событий
C:\Windows\System32\smss.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	4
C:\Windows\System32\autochk.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\csrss.exe	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	2
C:\Windows\System32\wininit.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\winlogon.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\svchost.exe	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	1

Доступ к нити процесса (4)

Имя исполняемого образа	Запрошенные права	Предоставленные права	Кол-во событий
C:\Windows\System32\smss.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	2
C:\Windows\System32\autochk.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1
C:\Windows\System32\wininit.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1
C:\Windows\System32\winlogon.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1

Рисунок 20 – Информация на вкладке «Процессы»

Информация представлена в таблице, которая содержит следующие поля:

– Имя исполняемого образа;

– Запрошенные права;

– Предоставленные права;

– Кол-во событий.

В области **Доступ к процессу** показана информация о том, к каким процессам в системе выбранный процесс осуществлял доступ, и какие права при предоставлении доступа были запрошены и предоставлены этому процессу.

В области **Доступ к нити процесса** показана информация о том, к каким нитям выбранный процесс осуществлял доступ, и какие права при предоставлении доступа были запрошены и предоставлены.

Вкладка «Загруженные DLL/SO»

Во вкладке **Загруженные DLL/SO** отображается информация о нативных и .Net-библиотеках DLL, используемых выбранным процессом.

> **Важно**
>
> Если в профиле безопасности агента установлена опция **Исключать события загрузки известных модулей**, то в списке DLL этих модулей не будет. Подробный список известных DLL-библиотек содержится в пункте 11.28.2.

Информация о библиотеках, которые были загружены рассматриваемым процессом, представлена в таблице со следующими полями:

1) **Нативные** или **.NET** (содержит абсолютный путь нативной или .NET-библиотеки);
2) Размер файла;
3) Подпись;
4) **Размещение** (содержит базовый адрес DLL в файловой таблице);
5) Хеш (SHA-256).

В поле с хеш-суммой аналитик может скопировать значение хеша в буфер обмена с помощью кнопки , а также перейти по ссылке () на страницу **Артефакты TI**, чтобы изучить подробную информацию о выбранной библиотеке (когда и где обнаружена, распространенность в инфраструктуре и т.д.).

Рядом с названием библиотеки находится кнопка раскрытия дополнительной информации о событии, связанном с библиотекой ( ). При нажатии ЛКМ на кнопку открывается карточка событий, связанная с рассматриваемыми процессом и библиотекой.

Для процесса **%SYSTEM%** будет представлен список загруженных в процесс модулей ядра, дополнительная информация о которых также становится доступной при нажатии кнопки .

Вкладка «Точки автозапуска»

Во вкладке **Точки автозапуска** отображается информация о точках автозапуска, созданных рассматриваемым процессом в реестре (рис. 21).



Реестр (21)

Ключ реестра	Значение	Тип данных
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	DependOnService	REG_MULTI_SZ
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	ImagePath	REG_EXPAND_SZ
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	ErrorControl	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	Type	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ObjectName	REG_SZ
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	DisplayName	REG_SZ
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ImagePath	REG_EXPAND_SZ
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ErrorControl	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	Start	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	Type	REG_DWORD
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc		
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc		

Рисунок 21 – Точки автозапуска

Примечание

Под точками автозапуска подразумеваются процессы, автоматически запускаемые на агентах при возникновении тех или иных условий, например, запуск программы при загрузке операционной системы.

Рядом с названием точки автозапуска в таблице находится кнопка раскрытия дополнительной информации, связанной с этой точкой ›. При нажатии ЛКМ на кнопку › открывается карточка событий, связанная с ключами реестра, с помощью которых процессом создавались точки автозапуска.

Вкладка «Распространенность»

Во вкладке **Распространенность** отображается информация о распространении артефакта (под артефактами в EDR подразумеваются хеши, IP-адреса и домены, проверяемые TI-платформой) в агентской сети.

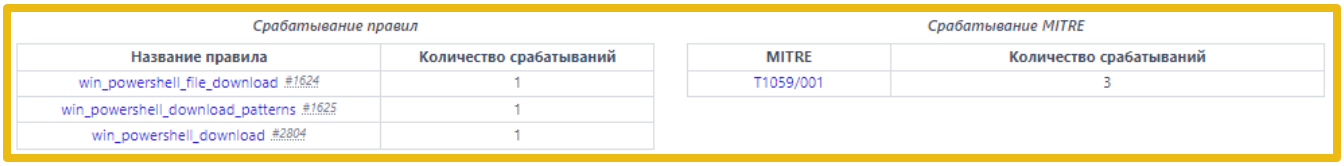
При этом аналитику показывается, когда артефакт был впервые зарегистрирован, на каком агенте это произошло и путь до исполняемого файла. Цифры в названии вкладки показывают, на каком количестве агентов присутствует артефакт.

Вкладка «Событие старта»

Во вкладке **Событие старта** показана карточка события для старта процесса.

Вкладка «Правила/MITRE»

Во вкладке **Правила/MITRE** содержится информация о срабатываниях действующих в EDR правил, а также техник MITRE для выбранного процесса (рис. 22).



Срабатывание правил

Название правила	Количество срабатываний
win_powershell_file_download #1624	1
win_powershell_download_patterns #1625	1
win_powershell_download #2804	1

Срабатывание MITRE

MITRE	Количество срабатываний
T1059/001	3

Рисунок 22 – Правила/MITRE

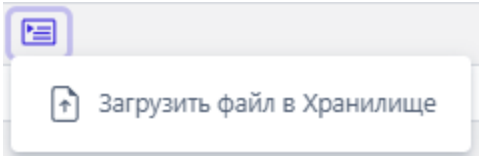
11.6 Загрузка и проверка файлов в хранилище

На странице **Активность** аналитик может открыть карточку события и просмотреть дополнительную информацию об этом событии.

Чтобы просмотреть карточку события-обнаружения необходимо нажать на кнопку ›.

Карточка событий содержит различные сведения в зависимости от типа и подтипа событий. Часть полей, отображаемых в карточке, являются общими для всех типов и подтипов событий.

В поле **Полное имя исполняемого файла процесса** содержится путь до исполняемого файла. Аналитик может выгрузить файл с конечной точки и загрузить в файловое хранилище сервера EDR для проверки с помощью TI-платформы или программы просмотра файлов.

Для загрузки выбранного файла в файловое хранилище модуля администрирования необходимо нажать кнопку 

.

Кнопка активна не только для **app** (**Полное имя исполняемого файла процесса**), но и для **who** (**Полное имя исполняемого модуля-инициатора операции**) и **name** (**Полное имя файла**). Для удобства кнопка реагирования (загрузки файла) продублирована в правой верхней части карточки события ().

Для дальнейшего анализа файла следует перейти в раздел **Хранилище** и с помощью представленных на странице фильтров найти нужный файл. В целом, файлы, сохраненные недавно, попадают в верхнюю часть таблицы во вкладке **Файлы с агентов**.

В Хранилище возможно выполнить следующие действия:

– проверить с помощью базы данных TI-платформы (кнопки TI и);

– просмотреть файл с помощью программы просмотра файлов (кнопка);

– удалить файл из хранилища (кнопка);

– получить ссылку на скачивание файла ( ), которую можно использовать для отправки файла из хранилища на агент, используя команду put;

– загрузить файл на TI-платформу ( ), если файл был уже загружен ранее, значок загрузки будет изменен ( );

– скачать файл на хост, с которого осуществлен доступ к серверу управления ( );

– загрузить файл с хоста, с которого осуществлен доступ к серверу управления, в Хранилище;

– разрешить перманентное скачивание файла с сервера на агент и скопировать ссылку (ссылка становится постоянной) на этот файл ( );

– создать задачу загрузки архива (если файл, сохраненный в Хранилище большой или нужно скачать несколько больших файлов, то удобно воспользоваться функцией загрузки архива, который будет сохранен во вкладке Задачи по загрузке архивов);

– скачать архив на хост ( ), с которого осуществлен доступ к серверу управления;

При нажатии кнопки TI (безопасный файл) в столбце **Результаты проверки** появляется окно с результатами анализа файла TI-платформой. Кнопка со значком TI обозначает вредоносный файл. Кнопка со значком TI обозначает подозрительный файл. Кнопка со значком TI обозначает проверку файла на TI-платформе в текущий момент времени. В случае загрузки файла, информация по которому отсутствует на TI-платформе, кнопка отчета файла отображается со значком TI. Нажатие кнопки открывает окно с кратким отчетом по артефакту, чтобы посмотреть полный отчет, необходимо нажать кнопку **Перейти к отчету**, после чего открывается страница подробного отчета TI-платформы о проверке загруженного файла (рис. 23).

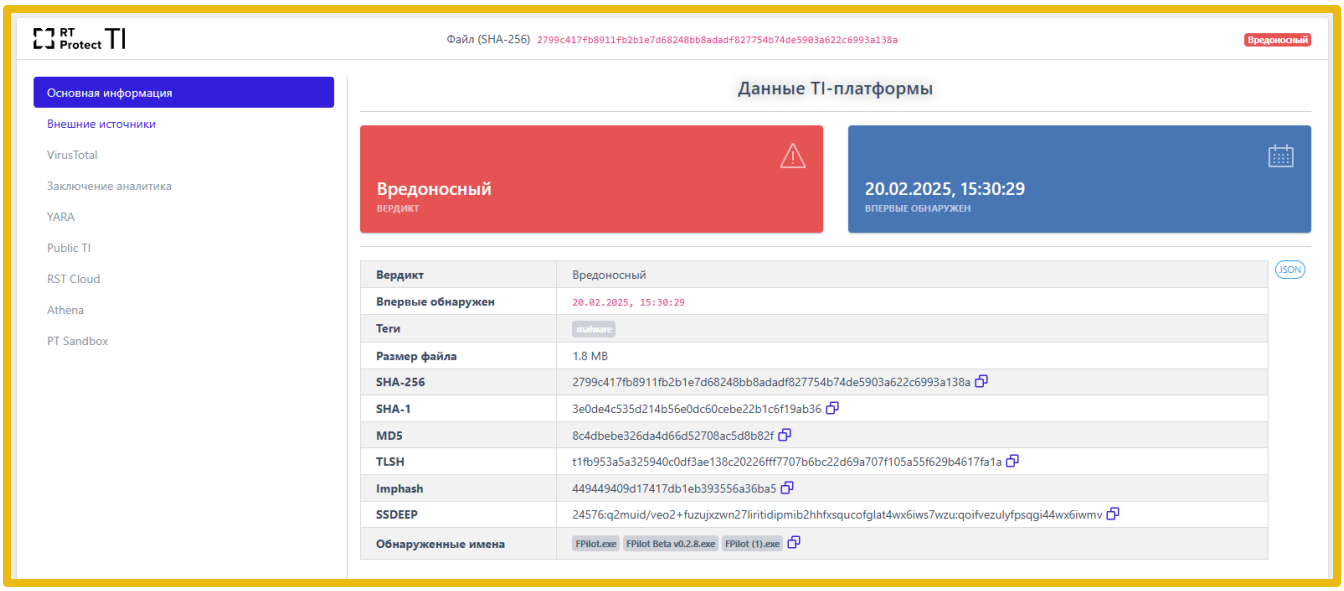


Рисунок 23 – Окно отчета проверенного файла

Отчет TI-платформы также можно посмотреть в формате JSON, нажав кнопку JSON .

В зависимости от артефакта страница отчета может содержать разную информацию, но всегда будет содержать вкладку **Основная информация,** где отображается вердикт TI-платформы по выбранному артефакту. На странице отчета могут быть показаны следующие вкладки:

1) Внешние источники;

2) **VirusTotal** (вкладка делится на две части: DETECTION с вердиктами вендоров и DETAILS с подробной информацией об артефакте);

3) Заключение аналитика;

4) YARA;

5) **Public TI** и другие (в зависимости от модулей, подключенных к TI-платформе).

После изучения файла аналитик может принять решение о дальнейших действиях: закрыть инцидент и внести файл в исключения, если произошло ложноположительное срабатывание, изолировать агента, на котором файл был обнаружен, воспользоваться терминалом или задействовать операции реагирования для возврата системы в состояние до вредоносного воздействия, продолжить расследование с помощью фильтрации событий на странице **Активность** и т.д.

11.7 Расследование с «Главной страницы» или страницы «Инциденты»

На главной странице аналитик может просмотреть сводную информацию обо всей инфраструктуре, подключенной к модулю управления:

– количество защищаемых агентов;

– количество событий в защищаемой инфраструктуре за последние 15 минут;

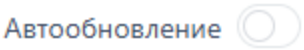
– общее количество инцидентов;

– значение EPS (Event per Second), которое показывает количество приходящих от агентов событий в секунду (показывается текущее суммарное значение со всех активных агентов и среднее значение EPS в пересчете на одного активного агента);

Примечание

Для периодов **Час**/**День**/**Неделя** EPS – это суммарное число событий за период, делённое на 60, то есть относительный индикатор нагрузки, а не мгновенный EPS. Сам же график при любом периоде показывает корректную динамику — количество событий по периодам времени.

Таким образом, график EPS представляет собой монитор объёма телеметрии EDR во времени (всего и в пересчёте на активного агента), с выбором периода и обновлением. Чтобы включить автообновление на Главной странице необходимо использовать ползунок



– информация об инцидентах (динамика и распределение по критичности);

– информация о ключевых событиях (динамика и распределение по критичности);

Примечание

Под ключевыми событиями подразумеваются события с критичностью **Средняя** или выше и события, для которых установлено действие **Блокировать.**

– информация об уязвимостях и возникших инцидентах, связанных с этими уязвимостями.

В разделе **Главная страница** аналитик также может просмотреть, сколько пакетов с событиями находится в очереди для отправки на сервер, это может помочь выявить проблемы на сервере (например, очередь может образоваться, если жесткий диск сервера частично вышел из строя). Наличие большой очереди может свидетельствовать о проблемах в работе сервера или о большом потоке событий.

Для проверки тайминга отставания проверок артефактов TI используется иконка TI в правом верхнем углу страницы. Отставание означает, что события с артефактами находятся в базе elasticsearch без вердиктов. Алгоритм не успевает их аннотировать и события без вердиктов копятся.

Для детального изучения инцидента необходимо перейти на страницу с инцидентами (рис. 24). Аналитик может сразу перейти на страницу **Инциденты** в разделе **События** на панели управления модуля администрирования.

Совет

Первое, что желательно сделать аналитику при обнаружении инцидента, если инцидент не является ложноположительным срабатыванием – это настроить изоляцию агента.

Если произошло ложноположительное срабатывание, то аналитику необходимо создать исключающее правило, проще всего это сделать с помощью мастера исключений.



Рисунок 24 – Окно страницы «Инциденты»

В верхней части страницы отображается график, показывающий количество зарегистрированных инцидентов в течение выбранного периода (по умолчанию за все время).

Открывается с помощью кнопки **Показать графики** ( ) в строке **Динамика инцидентов**. График можно поменять с линейного на столбчатый тип.

В поле кнопки выбора инцидентов содержится кнопка раскрытия дополнительной информации о событиях, включенных в инцидент ( ). При нажатии ЛКМ на значок снизу от строки инцидента открывается дополнительная информационная область, в которой пользователь может просмотреть важные данные об инциденте (рис. 25).

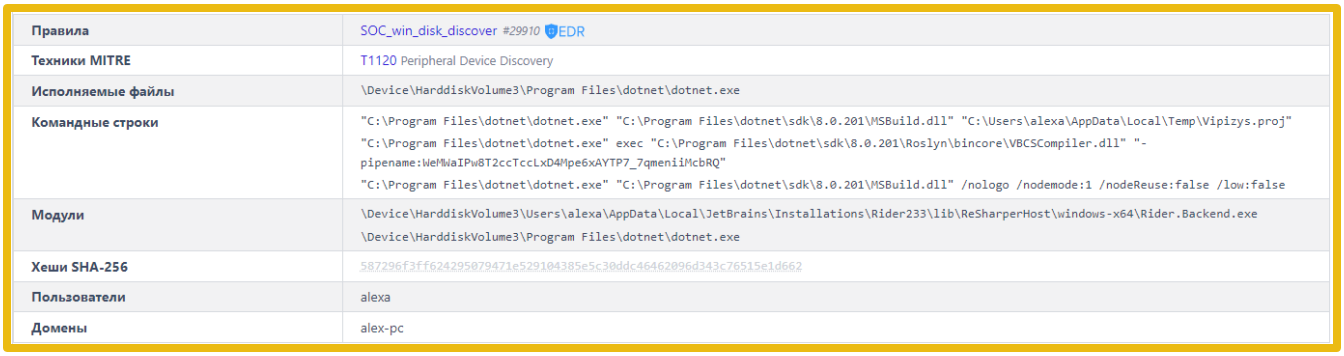


Рисунок 25 – Дополнительная информация об инциденте

В поле **Критичность** основной таблицы с инцидентами показывается информация о степени критичности инцидента. Инцидент автоматически формируется при выявлении события, критичность которого составляет **Средняя** или выше. Вручную можно формировать инциденты на основе событий с любой критичностью.

В поле **Название** таблицы **Инциденты** находится имя, присвоенное инциденту и его номер. Инциденты, которые пользователи создают вручную, помечаются значком . Значок отображается рядом с названием. При нажатии ЛКМ на имени инцидента происходит переход на страницу **Инцидент**.

Для изменения названия инцидента в поле **Название** справа от имени инцидента содержится кнопка **Редактировать** ( ). Кнопка будет отображаться только для инцидента, у которого назначен ответственный за его решение пользователь. При нажатии кнопки открывается окно **Редактирование инцидента** (рис. 26).

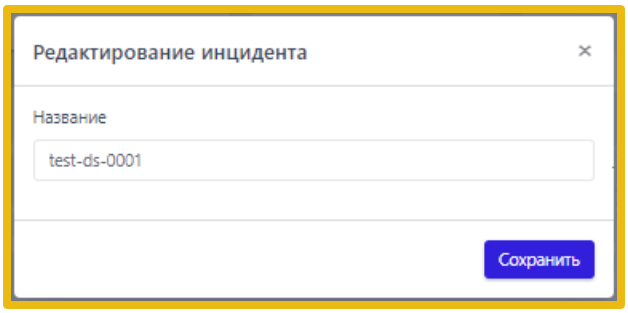


Рисунок 26 – Редактирование инцидента

Для изменения имени инцидента необходимо ввести произвольное имя в строке **Название**, после чего нажать кнопку **Сохранить** для завершения операции. После завершения операции в нижней части страницы отобразится всплывающее окно с сообщением.

В поле **Время регистрации** отображается информация о времени регистрации инцидента.

В поле **Время действия** отображается информация о времени, в течение которого происходил инцидент. Это время рассчитывается, как разница между временем, когда началось первое событие инцидента, и временем, когда закончилось последнее событие инцидента.

В поле **Агенты** отображается информация о группе, в которую входит агент, для которого создан инцидент и имя агента. При нажатии на имени группы или названии агента происходит переход к страницам **Группа** и **Агент**.

В поле **Кол-во событий** отображается информация о количестве событий, входящих в инцидент.

В поле **Ответственный** находится кнопка **Изменить** ( ), с помощью которой можно изменить пользователя, ответственного за решение инцидента. Кнопка отображается только для назначенных инцидентов. При нажатии кнопки **Изменить** открывается окно **Выбор ответственного по инциденту** (рис. 27).

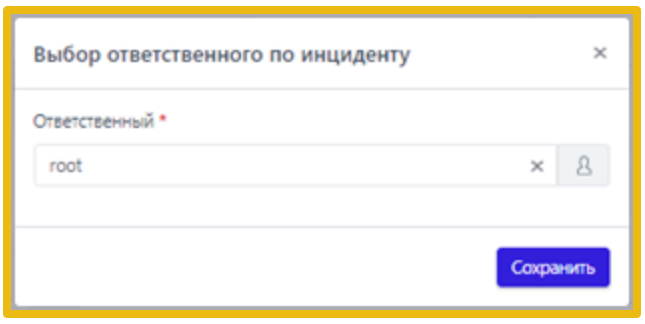


Рисунок 27 – Выбор пользователя, ответственного за решение инцидента

В случае, если ответственный за инцидент уже был назначен, то для выбора нового пользователя, ответственного за инцидент, необходимо в строке **Ответственный** удалить текущего пользователя, нажав в ней кнопку × . Далее выбрать пользователя из списка, нажав ЛКМ на пустую строку поля **Ответственный**, или ввести в ней с клавиатуры имя нового пользователя, ответственного за инцидент.

Для завершения процедуры назначения ответственного пользователя следует нажать кнопку Сохранить, после чего в нижней части страницы отобразится всплывающее окно с сообщением.

В поле **Статус** отображается информация о текущем статусе инцидента. В зависимости от текущего статуса инцидента в поле будут отображаться различные кнопки, с помощью которых можно изменить некоторые параметры инцидента:

1) Закрыть инцидент – (активна при статусе **Назначен** или **Новый**);

2) Назначить или открыть инцидент повторно – (активна при статусе **Новый** и **Закрыт**);

Для закрытия инцидента необходимо нажать кнопку **Закрыть инцидент** ( ) и в открывшемся окне **Закрытие инцидента** нажать кнопку **Сохранить**. Закрыть инцидент можно даже в случае, если для него не назначен ответственный.

После выполнения операции в нижней части страницы появится всплывающее окно с сообщением.

По умолчанию в окне **Закрытие инцидента** в поле **Комментарий** стоит запись **[Закрытие инцидента]**, ее можно изменить на произвольный комментарий или сохранить статус инцидента без комментария. Информация, указанная пользователем в комментарии, отобразится на странице **Инцидент**.

Для того, чтобы назначить ответственного пользователя по новому инциденту, необходимо нажать кнопку **Назначить инцидент** ( ) и в открывшемся окне **Назначение инцидентов** в поле **Ответственный** выбрать пользователя, ответственного за решение инцидента, после чего нажать кнопку **Сохранить**.

После завершения операции по назначению ответственного за решение инцидента в нижней части страницы появится окно с сообщением.

Кроме назначения ответственного в окне **Назначение инцидента** пользователь может ввести произвольный комментарий в поле **Комментарий**, сохранить статус инцидента без комментария или оставить комментарий по умолчанию. Желательно, чтобы комментарий был информативным и отражал суть текущей стадии работы с инцидентом. Информация, указанная пользователем в поле **Комментарий**, отобразится на странице **Инцидент**.

Чтобы открыть инцидент, необходимо нажать кнопку **Назначить инцидент (открыть повторно)** (), после чего в открывшемся окне **Назначение инцидентов** нажать кнопку **Сохранить**, изменив или сохранив текущего пользователя в качестве ответственного за решение инцидента. При повторном назначении можно, как и при любой другой смене статуса, добавить комментарий, который отобразится на странице **Инцидент**.

Для фильтрации инцидентов по тем или иным признакам на странице **Инциденты** содержатся следующие фильтры:

1) Показывать по;
2) Группа;
3) Агент;
4) Критичность;
5) Ответственный;
6) Создатель;
7) Период регистрации (список или календарь)
8) Статус;
9) Правило (поиск по правилам, на основе которых создаются обнаружения);
10) MITRE (поиск по TTP);
11) Полное имя исполняемого модуля процесса;
12) Запрос на языке DSL.

Принцип работы с фильтрами не отличается от работы с фильтрами в разделе **Активность**.

В полях фильтров **Правило**, **MITRE**, **Полное имя исполняемого модуля процесса** поддерживается автоподставление символов wildcard (*) для фильтров по агрегированным полям.

Для фильтрации в поле фильтра **Правило**, следует писать название правила без расшифровки.

Пример:

MaliciousDomain в chrome.exe – правило с расшифровкой (MaliciousDomain – правило, по которому будут фильтроваться инциденты).

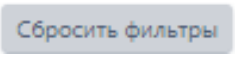
Фильтр **Период регистрации** в сравнении с фильтром **Период регистрации (на сервере)** на странице **Активность** содержит одно дополнительное значение **Всё время**, при выборе которого показываются все когда-либо зарегистрированные в Программе инциденты.

В поле фильтра **Статус** возможно выбрать следующие варианты статуса инцидента из всплывающего списка:

1) Новый;

2) Назначен;

3) Закрыт.

В поле фильтра **Ответственный** задаётся фильтрация инцидентов по пользователю, ответственному за решение инцидента. Сброс значений фильтров осуществляется с помощью кнопки 

.

Для сортировки инцидентов в полях таблицы с инцидентами **Критичность**, **Название**, **Время регистрации** и **Статус** используются кнопки смешанной сортировки , сортировки по возрастанию и сортировки по убыванию  .

Чтобы закрыть инциденты, необходимо выбрать один или несколько инцидентов с помощью кнопки выбора, отметив их флажками, далее нажать кнопку **Закрыть выбранные**, после чего в окне **Закрытие инцидентов** ввести произвольный комментарий и нажать кнопку **Отправить**. При назначении желательно оставить комментарий, который поможет ответственному за решение инцидента сотруднику приступить к выполнению своей задачи. Закрывать инциденты можно даже тогда, когда для них не назначены ответственные.

Для удаления инцидентов необходимо отметить флажками кнопки выбора соответствующих инцидентов и нажать кнопку **Удалить выбранные** в нижней части страницы **Инциденты**. Далее необходимо нажать в открывшемся окне кнопку **Начать удаление**, после чего подтвердить операцию.

Начнется удаление инцидента. После завершения операции необходимо нажать кнопку **Закрыть**. Вместе с инцидентами удаляются события, входящие в этот инцидент.

Процесс удаления инцидента возможно прервать. Для прерывания инцидента требуется нажать по иконке **Прервать удаление**. Удаление инцидента прервется на том инциденте, которому еще не отправлена команда на удаление, и в списке удаляемых инцидент не помечен  .

11.7.1. Анализ инцидента

Для начала анализа инцидента необходимо в столбце **Название** страницы **Инциденты** нажать левой кнопкой мыши по названию интересующего инцидента для перехода на страницу **Инцидент**.

В окне страницы **Инцидент** следует просмотреть общую информацию об инциденте и его событиях. Кратко ознакомиться с информацией о событии или событиях, составляющих инцидент, можно, нажав кнопку › в строчке напротив интересующего события (рис. 28). Обнаружения, представленные в инциденте можно сортировать в соответствии с фильтром **Критичность (не менее)**: при выборе определенного значения критичности в списке отобразятся события с критичностью, равной выбранной, и выше.

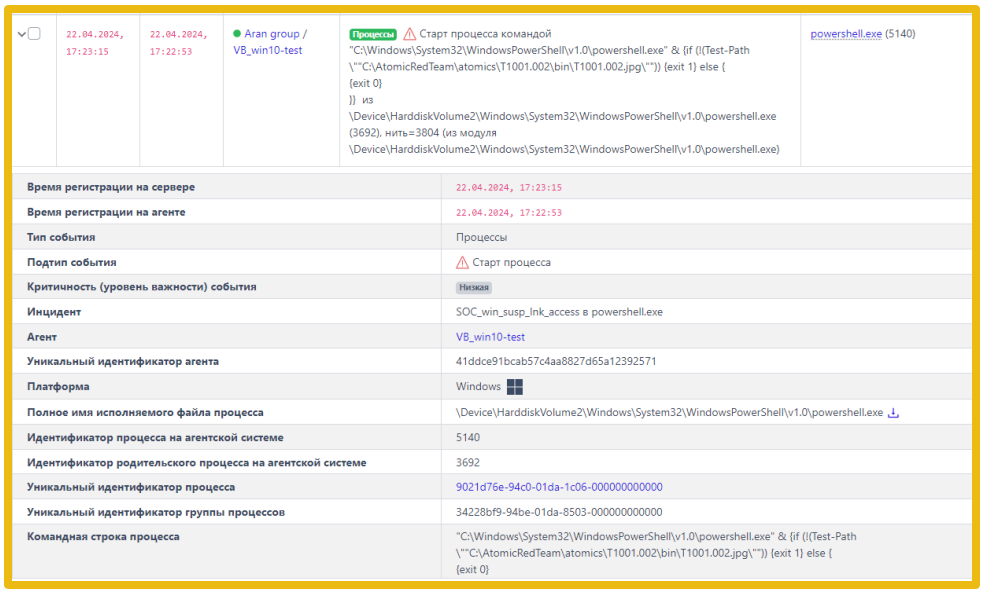


Рисунок 28 – Вызов всплывающего окна с информацией о событии

Дополнительная информация о выбранном событии содержится на странице в виде карточки события. Информация в окне о событии имеет различное содержание в зависимости от типа и подтипа события.

Карточку события можно просмотреть в формате JSON, чтобы при необходимости составить правило для индикации атак. Сведения о метаданных, обнаруживаемых Программой и предоставляемых аналитику в карточках событий содержатся в разделе 9.

Справа от таблицы с данными находится кнопка JSON. Любой элемент или блок элементов в формате JSON можно скопировать, нажав кнопку . Для возврата к результатам отчета в формате HTML необходимо нажать ЛКМ на значок HTML.

Жизненный цикл каждого инцидента подразумевает прохождение трех стадий:

– новый инцидент;

– назначенный в работу;

– закрытый инцидент.



Совет

Если инцидент не представляет больше ценности для дальнейшей работы, его можно удалить. Для этого используется кнопка **Удалить инцидент** в области **Информация об инциденте**. При этом вместе с инцидентом удаляются и события, которые входят в этот инцидент.

В зависимости от статуса инцидента у страницы **Инцидент** функциональность может различаться. Для нового и закрытого инцидента недоступна функция редактирования инцидента. Чтобы отредактировать инцидент, необходимо назначить пользователя, ответственного за его решение. Страница **Инцидент** разделена на следующие области:

1) Инцидент;

2) Комментарии;

3) Дополнительная информация;

4) Обнаружения.

В области **Инцидент** пользователь может назначить инцидент на того или иного аналитика для дальнейшей работы или выполнить другие действия:

– редактировать инцидент;

– закрыть инцидент;

– открыть инцидент повторно;

– удалить инцидент;

– сохранить отчет об инциденте в файл формата pdf на компьютер, с которого осуществлен доступ в модуль администрирования (кнопка PDF).

В области **Инцидент** отображаются следующие данные:

– название инцидента;

– критичность инцидента;

– ответственный за решение инцидента;

– статус инцидента;

– агент, на котором произошли события инцидента;

– время регистрации инцидента;

– время действия инцидента;

– описание.

Редактировать можно следующие параметры:

– название;

– ответственный;

– критичность;

– описание.



Примечание

Операции редактирования имени инцидента, критичности, описания, а также исключение событий из инцидента становятся доступными после назначения ответственного за инцидент.

После завершения редактирования необходимо нажать кнопку **Сохранить изменения**.

В области **Комментарии** пользователь может указать произвольный комментарий. Также комментарии указываются автоматически при переводе инцидента из одного статуса в другой, например, при назначении или закрытии инцидента.



Примечание

Поле **Комментарий**, как и поле **Описание**, не должно превышать 1000 символов (байтов).

Для добавления нового комментария следует нажать кнопку **Создать комментарий**, после чего открывается окно **Создать комментарий** (рис. 29).

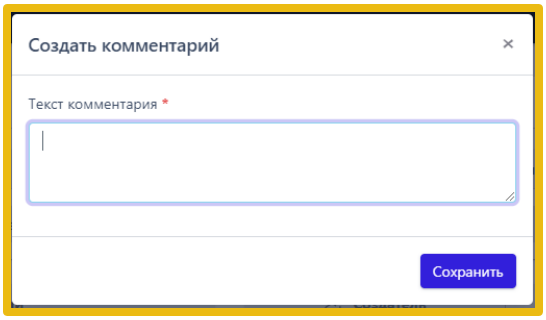


Рисунок 29 – Окно ввода комментария

Для добавления комментария к инциденту необходимо ввести в окне **Новый комментарий** текст комментария и нажать кнопку **Отправить**, после чего комментарий пользователя будет добавлен на страницу инцидента.

Для отмены ввода комментария следует в окне **Новый комментарий** нажать кнопку **Отмена** или **Закрыть окно** ( ).

В области **Дополнительная информация** представлена информация по инциденту с уточнением параметров, характеризующих инцидент, таких как наименование правила, на основе которого сформирован инцидент, имена исполняемых файлов и командные строки, участвующие в инциденте, затронутые инцидентом пользователи и домены, удаленные сетевые точки и локальные конечные точки, хеши, техники MITRE и т.д.

В области **Обнаружения** в табличном виде представлена информация о событиях, которые были включены в инцидент при его регистрации. Переход по страницам в таблице в случае, если события в инциденте не умещаются на одной странице, осуществляется с помощью пагинатора.

В верхней части области **Обнаружения** отображается информация об общем количестве событий в инциденте и фильтр **Показывать по** (можно задавать следующие значения: 10, 20, 50, 100).

В таблице с обнаружениями информация распределена по следующим полям:

1) Регистрация на сервере;

2) Регистрация на агенте;

3) Группа/Имя агента;

4) Описание;

5) Процесс;

6) Информация.

Регистрация на сервере – содержит информацию о годе, месяце, дне и точном времени регистрации обнаружения на сервере по стандарту UTC.

Регистрация на агенте – содержит информацию о годе, месяце, дне и точном времени регистрации обнаружения на агенте, то есть по текущему времени, которое установлено на машине с агентом.

Группа/Имя агента – в поле отображаются группа, в которой находится агент, и название агента, имена группы и агента служат гиперссылкой для перехода к соответствующим страницам.

Описание – содержит краткое описание события, которое системой определено как обнаружение или телеметрия, событие-обнаружение помечается значком  .

Процесс – содержит имя процесса, действия которого привели к обнаружению Программой, имя процесса отображается в виде ссылки для перехода к странице **Процессы**.

В поле **Информация** показаны следующие данные по обнаружению:

– Критичность/Действие;

– MITRE;

– Правило.

Критичность/Действие – показывает уровень угрозы, которая исходит от обнаруженного события для защищаемой ИТ-инфраструктуры (для автоматических обнаружений это средний, высокий и критичный уровень), а также в поле отображается действие, предпринятое в связи с обнаружением события. Программой предусмотрены три действия: блокировать, детектировать и продолжение наблюдения. В последнем случае поле останется пустым.

MITRE – в поле отображается идентификатор техники атаки MITRE ATT&CK, который соответствует событию, добавленному в инцидент (идентификатор назначается опционально).

Правило – в поле отображается наименование правила, в соответствии с которым событие было добавлено в инцидент.

В поле **Информация** также находится кнопка **Ложное срабатывание** (). Нажав на кнопку, пользователь может создать исключение для файла, исключение для программы или сетевое исключение с помощью мастера исключений.

Общий вид окна при создании исключения с помощью мастера исключений для файла представлен на рисунке 30.

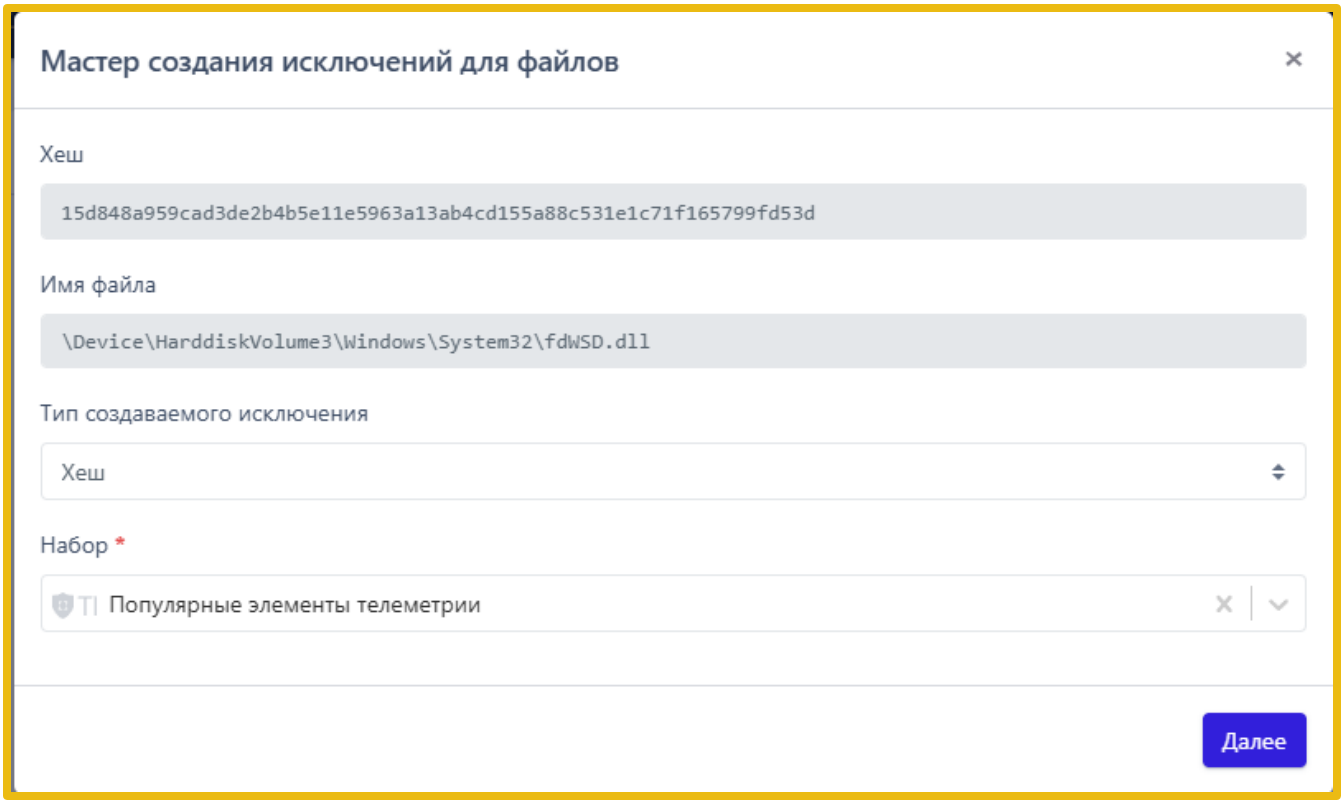


Рисунок 30 – Окно мастера создания исключений

В данном окне поля **Хеш**, **Имя файла** устанавливаются автоматически из выбранного обнаружения, требуется определить только тип создаваемого исключения: исключение по хеш-сумме или исключение по имени файла. Также можно указать набор, в который следует добавить исключение.

Для дальнейшего создания исключения требуется нажать кнопку **Далее**, после чего произойдет переход к окну добавления исключения (рис. 31).

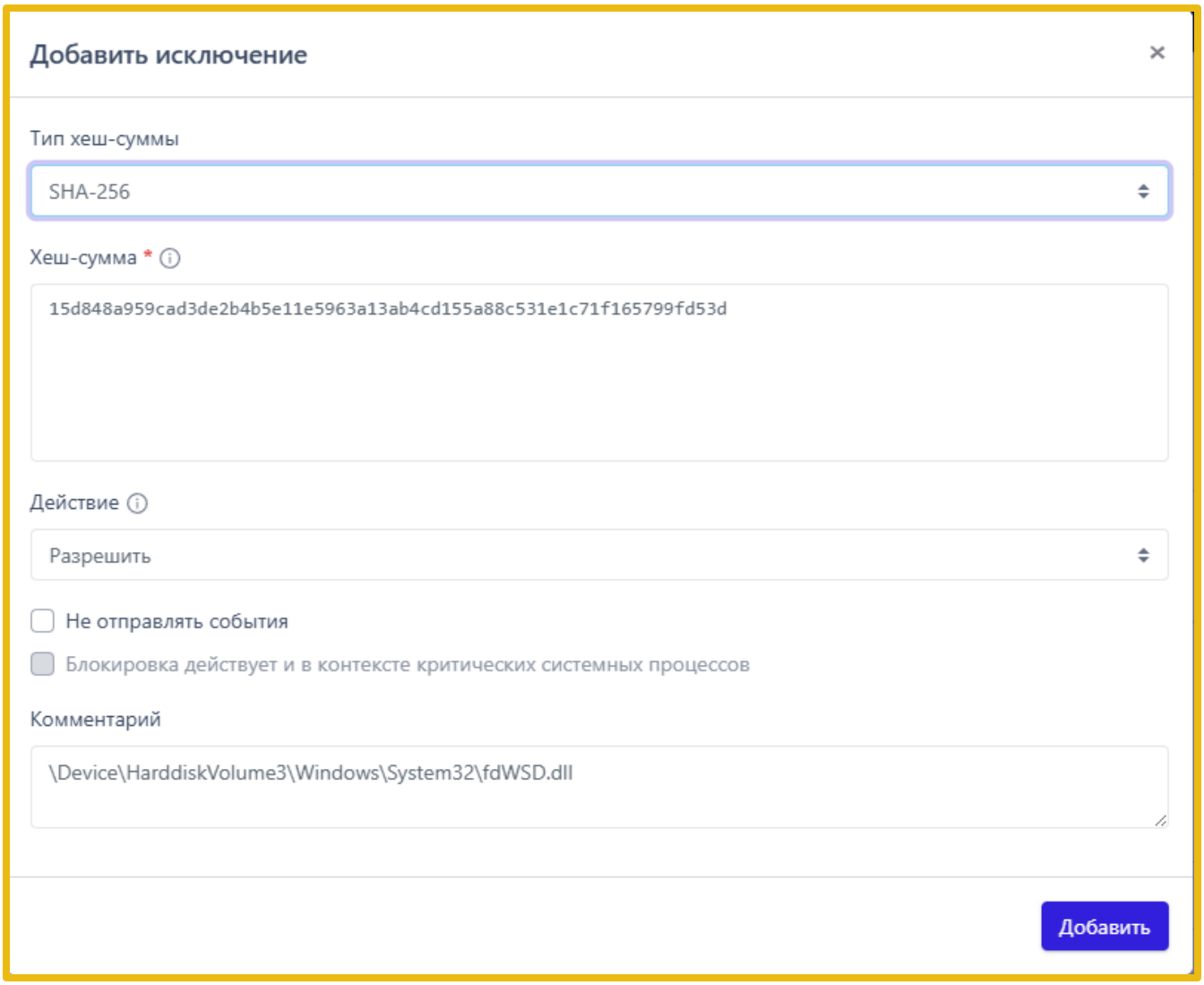


Рисунок 31 – Окно добавления исключения

Хеш-сумма заполняется автоматически из предыдущего окна. Чтобы завершить добавление исключения, требуется только определить действие (**Разрешить/Блокировать**) и установить флаги, если требуется, **Не отправлять события** и **Блокировка действует и в контексте критических системных процессов**. Флаг **Не отправлять события** позволяет не отправлять в **Активность** события срабатывания исключения.

Флаг **Блокировка действует и в контексте критических системных процессов** следует применять осторожно, срабатывания исключений могут привести к установке ОС в состояние «синего экрана». После установки флагов необходимо нажать кнопку **Добавить**. Исключения для программ и сетевые исключения создаются по аналогичной схеме.

После просмотра информации об инциденте аналитик может сохранить отчет о нем в файл формата pdf на компьютер, с которого осуществлен доступ в модуль администрирования. Для этого предусмотрена кнопка PDF в области **Информация об инциденте**.



Совет

Кроме фильтрации событий и просмотра дополнительной информации в расследовании инцидентов аналитику могут помочь данные киберразведки (Threat Intelligence), которые предоставляются TI-платформой.

Для просмотра дополнительных данных об артефактах, выявленных в инциденте, можно просмотреть отчет TI-платформы. Платформа сопоставляет и анализирует данные компьютерных угроз из нескольких источников в режиме реального времени для поддержки защитных действий Программы. На данный момент платформой проверяются следующие артефакты:

1) Хеш файла;
2) Глобальный IP-адрес;
3) Глобальное имя домена.

Проверка выполняется в нескольких источниках, в зависимости от типа артефакта набор источников может отличаться:

1) Внешние источники;
2) VirusTotal;
3) Заключение аналитика;
4) YARA;
5) IOC;
6) Whois;
7) Public TI.

TI-платформа может предоставлять другие аналитические данные:

– индикаторы атак;
– заключения аналитика;

– индикаторы компрометации;

– YARA-правила;

– журналы.

Страницы отчета TI-платформы открываются на вкладке **Основная информация**, которая содержит сводные данные из всех доступных для выбранного артефакта источников (см. рис. 23).

В верхней части страницы отчета отображается наименование и значение артефакта и вердикт TI-платформы. На левой панели отчета отображаются вкладки с наименованиями источников данных, от которых были получены сведения для вынесенного вердикта. На правой панели отчета отображается информация о выбранном артефакте.

Информация представлена в табличном виде. Поля таблицы могут содержать следующие данные:

1) Вердикт (безопасный/вредоносный/подозрительный/неизвестный/в процессе анализа);
2) Время обнаружения;
3) Размер файла;
4) Хеш, рассчитанный по алгоритму SHA-256;
5) Хеш, рассчитанный по алгоритму SHA-1;
6) Хеш, рассчитанный по алгоритму MD5;
7) Хеш, рассчитанный по алгоритму TLSH;
8) Хеш, рассчитанный по алгоритму Imphash;
9) Хеш, рассчитанный по алгоритму SSDEEP;
10) Обнаруженные имена.

Для значений хеш-сумм и обнаруженных имен доступна функция копирования в буфер обмена. Чтобы скопировать нужные значения в буфер обмена, необходимо нажать кнопку **Скопировать в буфер обмена** в строке с выбранным значением хеш-суммы или обнаруженными именами.

Справа от таблицы с данными находится кнопка JSON. Любой элемент или блок элементов в формате JSON можно скопировать, нажав кнопку . Для возврата к результатам отчета в формате HTML необходимо нажать ЛКМ на значок HTML.

11.7.2. PDF-отчет об инцидентах

PDF-отчет об инцидентах можно сохранить на странице **Инциденты,** нажав кнопку **Скачать отчет в PDF** (). Отчет содержит информацию об инцидентах, сортируемых в соответствии с настроенными на странице фильтрами. Данные в отчетах представлены в следующем списке:

1) Настройки активных фильтров (показывает, какие фильтры были установлены на странице **Инциденты** в момент сохранения отчета);

2) Статистика по результатам:

– сколько инцидентов найдено;

– топ-10 исполняемых файлов;

3) Топ-10 правил в инцидентах;

4) Топ-10 техник MITRE в инцидентах;

5) Распределение инцидентов по критичности.

11.7.3. PDF-отчет об инциденте

PDF-отчет об инциденте аналитик может сохранить на странице **Инцидент**, нажав кнопку **Скачать отчет в PDF** (). Отчет содержит наиболее релевантную информацию об инциденте:

1) Общие сведения:

– название;

– время регистрации;

– время действия;

– группа/имя агента;

– критичность;

– статус;

– создатель (автоматически или вручную);

– ответственный;

– число событий в инциденте;

2) Дополнительная информация:

– название правила или правил, на основе которых создан инцидент;

– техники MITRE (если техника определена);

– абсолютные пути исполняемых файлов;

– операционная система компьютера, на котором произошел инцидент;

– командные строки;

– модули;

– хеши (в зависимости от указанных в профиле безопасности настроек файлового монитора);

– пользователи;

– домены;

– файлы.

11.8 Принципы работы TI-платформы в RT Protect EDR

Принцип работы с артефактами в RT Protect EDR в интеграции с RT Protect TI выглядит следующим образом:

1) При обнаружении очередного артефакта агентом (попытка запуска процесса, установления сетевого соединения и т.д.) производится его анализ по наборам индикаторов компрометации на самом агенте;

2) Если артефакт присутствует в наборе, соответствующее действие блокируется в синхронном режиме (например, не допускается запуск процесса);

3) В ином случае информация об артефакте вместе с событием отправляется на сервер EDR;

4) Далее в рамках интеграции осуществляется обращение к TI-платформе для получения вердикта по артефакту, в случае получения заключения «Вредоносный», агенту направляется команда, например, на завершение процесса.

В любом из описанных случаев в EDR генерируется инцидент.

Наборы индикаторов компрометации для агентов могут формироваться как вручную на сервере EDR, так и получаться с TI-плаформы, на которой, в свою очередь, формироваться динамически (галочка "теневой набор" в соответствующем разделе аналитики EDR в веб-интерфейсе TI-платформы). Это позволяет хранить на агентах ограниченный, но актуальный набор индикаторов компрометации для синхронного реагирования на угрозы.

Также важно, что интеграции (например, VirusTotal) запускаются только при анализе соответствующих событий в веб-интерфейсе TI-платформы (переход на страницу отчета об артефакте). Таким образом, это позволяет использовать ограниченные квоты только для исследуемых артефактов, а для анализа всех артефактов на потоке использовать базу данных, формируемую на основе подключенных фидов.

В рамках интеграции TI-платформы с решениями класса Sandbox (песочница) возможна отправка потенциально вредоносных файлов с агента в TI-платформу и далее в песочницу (также данный функционал доступен из веб-интерфейса TI-платформы). Это осуществляется путём использования команды **get** в консоли агента с параметром "-t ti" (подробнее о команде **get** см. в пункте 11.2.1).

На проверку TI-платформой не отправляются файлы со следующими характеристиками:

– для программы отключен анализ файловой активности через механизм исключений для программ;

– событие с файлом сгенерировано на этапе, предшествующем первичной синхронизации аналитики;

– имя файла соответствует шаблону через регулярные выражения;

– файл подписан доверенной электронной подписью;

– исполняемый файл или исполняемый файл процесса находится в исключениях для файлов со статусом **Разрешено** или является «известным» безопасным файлом по своему содержимому, список «известных» файлов со временем меняется).

Список доверенных электронных подписей:

1) Microsoft Corporation;
2) Microsoft Windows;
3) Microsoft Dynamic Code Publisher;
4) Windows Phone;
5) .NET;
6) Google Inc;
7) Google LLC;
8) AO Kaspersky Lab;
9) Kaspersky Lab JSC;
10) Kaspersky Lab;
11) YANDEX LLC;

12) VMware, Inc.;
13) Mozilla Corporation;
14) PGP Corporation;
15) Oracle America, Inc.;
16) Opera Norway AS;
17) Dropbox, Inc;
18) Viber Media S.à r.l.;
19) Adobe Inc.;
20) Microsoft Windows Publisher;
21) Oracle Corporation;
22) Opera Software AS;
23) Avast Software s.r.o.;
24) Searchinform ООО;
25) Skype Software Sarl;
26) JetBrains s.r.o.;
27) ESET, spol. s r.o.;
28) Intel Corporation;
29) Sophos Ltd;
30) Adobe Systems, Incorporated;
31) Ghisler Software GmbH;
32) Bitdefender SRL;
33) Realtek Semiconductor Corp.;
34) Docker Inc;
35) Trend Micro, Inc.;
36) Autodesk, Inc.;
37) Vivaldi Technologies AS;
38) Adobe Systems Incorporated;
39) Realtek Semiconductor Corp;

40) ООО Searchinform;

41) Hewlett-Packard Company;

42) Samsung Electronics CO., LTD.;

43) Apple Inc.;

44) Acronis International GmbH;

45) HP Inc.;

46) ABBYY Production LLC;

47) BITDEFENDER LLC;

48) GitHub, Inc.;

49) McAfee, Inc.;

50) Paragon Software GmbH;

51) Qualcomm Atheros, Inc.;

52) Telegram Messenger LLP;

53) Oculus VR, LLC;

54) Sony Corporation;

55) Sophos Limited;

56) Symantec Corporation;

57) Acronis, Inc;

58) Malwarebytes Corporation;

59) Sentinel Labs, Inc.;

60) АО IB REFORM;

61) JSC RT IB;

62) LLC Bezopasnaya Informatsionnaya Zona;

63) Doctor Web Ltd.;

64) "VMware, Inc.";

65) Microsoft Windows Hardware Compatibility Publisher;

66) KIBC TECHNOLOGY;

67) LLC "Stakhanovets".

Список может меняться со временем.

Кроме указанных выше файлов на проверку сервера TI не отправляются ip-адреса и домены, связанные со следующими событиями:

– для программы отключен анализ исходящего и входящего трафика через механизм **Исключения для программ**;

– для программы отключен анализ DNS-сообщений через механизм **Исключения для программ**;

– взаимодействие с удаленным хостом разрешено через механизм **Сетевые подключения**;

– запрашиваемое доменное имя находится в сетевых исключениях со статусом **Разрешено**;

– событие с ip-адресом или доменом сгенерировано на этапе, предшествующем первичной синхронизации аналитики.

Если коротко представить алгоритм работы TI с вредоносными артефактами, то можно сказать, что если TI-платформа выносит вердикт о том, что в системе обнаружены вредоносный домен, IP-адрес или хеш исполняемого файла, автоматически выполняются следующие операции:

1) В Программе регистрируется инцидент;
2) Процесс вредоносного файла автоматически завершается;
3) Обращение к вредоносному домену или IP-адресу автоматически блокируется.



Примечание

На TI-платформе проверяются глобальные адреса и домены, проверка локальных адресов и доменов не предусмотрена.

При обнаружении подозрительного артефакта выполняется только детектирование события, при этом создается инцидент.

В некоторых случаях вердикт TI-платформы, присвоенный артефакту при первоначальном к нему обращении, может отличаться от назначенного впоследствии. В этой ситуации события с такими артефактами в разделе **Активность** помечаются значком  .

Важной функцией TI-платформы является централизованное хранение и распространение до отдельных серверов EDR аналитических наборов и наборов с исключениями. К аналитическим относятся

индикаторы атак, индикаторы компрометации, YARA-правила и журналы, к наборам с исключениями относятся исключения для программ, исключения для файлов, сетевые исключения и исключения индикаторов атак.

Для применения на агентах наборы с правилами должны быть назначены в соответствующих конфигурациях. Эта операция выполняется на страницах **Агенты** (для назначения на большое количество агентов или агентов, сгруппированных по определенным признакам) или **Агент**. После назначения и применения наборов правила, содержащиеся в них, будут работать на выбранных агентах.

Изменения наборов и сохранение новой конфигурации на TI-платформе для таких наборов приведет к автоматическому сохранению и применению новой конфигурации на агентах (такой набор имеет пометку **Успешно синхронизирован**) (рис. 32).

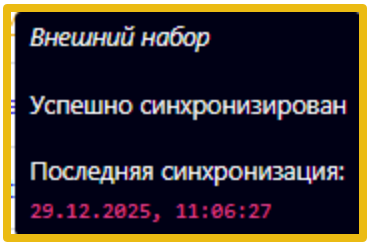


Рисунок 32 – Успешная синхронизация TI-набора

Аналитики EDR не могут изменять TI-наборы, но при этом могут просматривать содержимое наборов, а также копировать и перемещать данные из наборов.

11.9 Проверка распространенности артефактов TI в агентской сети

Артефакты TI – это инструмент для систематизации артефактов, анализируемых TI-платформой. Артефакты TI осуществляют фиксацию первичного события, в котором артефакт был задействован, и помогают выяснить распространенность артефактов в агентской сети.

Артефакт — это наблюдаемый признак (индикатор), извлекаемый из событий агента: контрольная сумма файла, сетевой адрес или доменное имя. По мере поступления событий с агентов EDR накапливает такие индикаторы и обращается к платформе TI для получения по ним вердикта.

Раздел **Артефакты TI** сводит эти данные в единый реестр и позволяет:

– просматривать все артефакты, обнаруженные в инфраструктуре, в разрезе их типа;

– видеть актуальный вердикт TI по каждому артефакту (безопасный, вредоносный, подозрительный и т. д.);

– оценивать распространённость артефакта — на скольких агентах он встречается;

– быстро переходить от артефакта к связанным событиям, агентам, правилам IOC и конфигурациям;

– инициировать проверку (обогащение) артефакта на платформе TI и изучать подробный отчёт по нему.

Раздел используется при разборе инцидентов и проактивном поиске угроз (threat hunting). Информация, представленная на странице **Артефакты TI**, помогает понять, является ли встреченный в инфраструктуре файл, IP-адрес или домен известной угрозой, и насколько широко он распространён в защищаемой инфраструктуре.

События и дополнительная информация, связанная с каждым уникальным артефактом, хранятся без ограничения по времени хранения.



Важно

Раздел **Артефакты TI** требует интеграции с TI-платформой (платформа должна быть подключена и доступна по сети).

Если артефакт не проверялся алгоритмами TI (находится в белом списке), то не показывается на странице **Артефакты TI**. Такими артефактами являются хеши, добавленные в исключения для файлов, ip-адреса и домены, добавленные в сетевые исключения, хеши файлов, подписанных доверенной подписью, локальные IP-адреса и т.д.

Пользователь может искать нужный артефакт с помощью фильтров:

1) Показывать по (10, 20, 50, 100, 500 строк в таблице);
2) Платформа (Windows или Linux);
3) SHA-256;
4) Период регистрации на сервере;
5) Запрос на языке DSL;
6) Вердикт артефакта;

7) Путь;

8) Подпись.

Для поиска нужного IP-адреса используются следующие фильтры:

1) Показывать по (10, 20, 50, 100, 500 строк в таблице);

2) Платформа;

3) IP-адрес;

4) Период регистрации;

5) Запрос на языке DSL;

6) Вердикт артефакта.

Для фильтрации по доменам используются следующие фильтры:

1) Показывать по (10, 20, 50, 100, 500 строк в таблице);

2) Платформа;

3) Домен;

4) Период регистрации;

5) Запрос на языке DSL;

6) Вердикт артефакта.

Централизованный поиск артефактов по всему модулю администрирования осуществляется в полях **SHA-256**, **IP-адрес**, **Домен**. Поиск осуществляется отдельно по индикаторам компрометации, событиям на странице **Активность**, наборам сетевых исключений для доменов и IP-адресов и наборам файловых исключений для хешей. В случае обнаружения артефакта в том или ином разделе станет активной соответствующая иконка или иконки () для SHA-256 и () для доменов и IP-адресов.

Вердикт TI-платформы открывается, если пользователь нажмет поле с хеш-суммой, IP-адресом или доменом. Первоначально открывается краткий отчет. Полный отчет доступен, если нажать кнопку **Перейти к отчету**.

Вердикт артефакта отражает оценку платформы TI. Он отображается в данных артефакта и используется в фильтре **Вердикт артефакта**. Возможные значения представлены в таблице 42.

Таблица 42 – Вердикты TI-платформы

Вердикт	Значение
Неизвестный	Платформа не имеет данных для однозначной оценки артефакта.
Безопасный	Артефакт признан легитимным и неопасным.
Вредоносный	Артефакт относится к вредоносной активности.
Подозрительный	Есть признаки потенциальной угрозы; требуется дополнительный анализ.
Выполняется анализ	Артефакт находится в процессе проверки на платформе.
Недействительный	Артефакт некорректен или не может быть проверен.

Дополнительно встречаются специальные состояния:

1) **Белый список –** артефакт внесён в доверенный список и не считается угрозой;

2) **Не найден –** по артефакту отсутствует запись на платформе TI, то есть нет результата проверки.

Белый список – это особое состояние артефакта, означающее, что артефакт намеренно не проверялся TI-платформой, потому что связанное с ним событие было признано доверенным. В этом случае события отфильтровываются еще до обращения к TI.

Белый список решает три задачи:

1) Снижение шума — доверенные события не порождают «Обнаружения и не создают инциденты;

2) Снижение нагрузки — заведомо легитимные хэши/домены/адреса не отправляются на сервер аналитики и в фиды TI;

3) Ускорение обработки — отфильтрованному событию сразу присваивается соответствующий класс, чтобы оно не запрашивалось повторно из базы Elasticsearch при следующих итерациях ретро-проверки.

Как событие/артефакт попадает в белый список?

1) Для файловых и процессных артефактов (хэши SHA-256):

– у файла установлен признак «белого» файла (поле события fwhite), либо у процесса в rf0 стоит флаг WhiteListed;

– цифровая подпись файла (sgnr) входит в список доверенных издателей;

– нативный системный процесс (флаг Native в rf0).

– доверенный загружаемый модуль/драйвер (флаг ImageWhiteListed в `ldf`).

– путь/имя соответствует системным шаблонам .NET NativeImages.

– установлен флаг подавления файловых проверок (exclf/whof) в исключениях для программ;

– событие произошло до первичного обновления аналитики;

– файл попадает в настроенные исключения для файлов.

2) Для сетевых артефактов (IP и домены):

– локальные/нероутируемые или недопустимые для проверки адреса и домены;

– установлены флаги подавления проверок исходящего, входящего трафика и DNS-запросов в исключениях для программ;

– узел или запрашиваемый домен в белом списке/исключениях;

– событие произошло до первичного обновления аналитики.

Пользователь может просмотреть дополнительную информацию о первичном событии, в котором фигурирует выбранный артефакт, нажав кнопку › в строке с событием. После нажатия кнопки откроется карточка события, как на странице **Активность**.

11.9.1. Ретроспективная проверка артефактов TI

Ретроспективная проверка (ретро-проверка) — это механизм, который периодически перепроверяет ранее зафиксированные в системе артефакты по актуальным вердиктам платформы TI. Если объект, который в момент наблюдения считался неизвестным или безопасным, позднее получает вердикт «подозрительный» или «вредоносный», система автоматически создаёт обнаружение по уже произошедшему событию. То, что вчера было безопасным, сегодня может оказаться угрозой. Ретро-проверка находит именно такие случаи.

Базы данных TI пополняются непрерывно. Между моментом, когда файл скачался или установилось сетевое соединение, и моментом, когда индикатор попал в TI как вредоносный, может пройти заметное время. Без ретро-проверки такое событие так и осталось бы «чистым» в истории. Ретро-проверка:

– выявляет угрозы, которые ещё не были известны в момент возникновения;

– не требует ручного перепросмотра истории аналитиком, так как всё происходит автоматически;

– при срабатывании может сразу запустить реагирование – закрыть соединение или завершить процесс.

Как работает ретропроверка

Периодический опрос TI. Системная служба ретро-проверки через заданные интервалы (по умолчанию раз в 60 минут) запрашивает у платформы TI список артефактов, у которых изменился вердикт с момента прошлой проверки.

Первый запуск. При самом первом запуске берётся история за предшествующий период (по умолчанию 30 дней назад). Далее проверяются только изменения с момента последней успешной проверки, поэтому работа идёт без повторов.

Сопоставление с событиями. Для каждого изменившегося артефакта система находит в хранилище ранее зафиксированные события, где этот артефакт встречался.

Принятие решения. Если новый вердикт «хуже» прежнего, по событию формируется обнаружение; вердикт артефакта в истории обновляется в любом случае.

Само по себе изменение вердикта не всегда приводит к обнаружению. Оно создаётся только при ухудшении вердикта, то есть при переходе:

– из любого «нормального» состояния (неизвестный, безопасный и т. п.) в «подозрительный» или «вредоносный»;

– из «подозрительного» во «вредоносный».

Обнаружение не создаётся, если вердикт не изменился или повторяется (защита от дублей), вердикт изменился «в лучшую сторону», событие входит в белый список. Классы вердиктов TI приведены в таблице

Таблица 43 – Классы вердиктов TI

Класс вердикта	Значение
Неизвестный	Объект пока не классифицирован
Безопасный	Угроз не выявлено
В процессе анализа	Объект исследуется
Подозрительный	Признаки потенциальной угрозы – может породить обнаружение
Вредоносный	Подтверждённая угроза – может породить обнаружение
Недействительный	Вердикт аннулирован

При создании ретроспективного обнаружения система:

– повышает важность события («высокая» для подозрительного вердикта, «критическая» для вредоносного);

– проставляет имя сработавшего правила, отражающее тип и вердикт артефакта (например, MaliciousFile, SuspiciousIp, MaliciousDomain);

– привязывает событие к технике MITRE ATT&CK T1204 «User Execution», подтехника T1204.002 (Malicious File) для файлов и T1204.001 (Malicious Link) для сетевых артефактов;

– запускает автоматическое реагирование – агенту направляется действие (завершить процесс или закрыть сетевое соединение), а в **Планировщике задач** ставится связанная задача.

Новое обнаружение появляется в общем потоке событий и доступно для разбора аналитиком наравне с обнаружениями реального времени. Основные параметры ретро-проверки приводятся в таблице 44.

Таблица 44 – Параметры ретро-проверки

Параметр	Назначение	По умолчанию
Период ретро-проверки	Как часто опрашивается TI на предмет изменения вердиктов	60 минут
Окно ретроспективы	Глубина истории при самом первом запуске	30 дней
Соединение с TI-платформой	Активное соединение с TI-платформой, через которую запрашиваются вердикты	требуется
Аналитика по процессам и файлам	Включает проверку файловых артефактов (SHA-256)	включено
Аналитика сетевой активности	Включает проверку IP-адресов и доменов	включено
Лимит артефактов в запросе	Количество артефактов при выгрузке изменений из TI	300

11.10 Конфигурирование аналитических правил

Для конфигурирования правил обнаружения аналитику необходимо перейти в разделы панели управления, объединенные термином **Аналитика**. Конфигурирование правил доступно аналитикам при наличии соответствующих прав (доступ к аналитике, управление наборами и конфигурациями и изменение аналитики и профилей).

Аналитика содержит следующие разделы:

1) Индикаторы атак (ИА);

2) Индикаторы компрометации (ИК);

3) YARA-правила (файлы);

4) YARA-правила (память);

5) Журналы.

Разделы содержат наборы правил для обнаружения вредоносной активности в автоматическом режиме. В программе сохранены аналитические наборы, которые позволяют детектировать известные и неизвестные угрозы. Сервер EDR также получает аналитические наборы от TI-платформы (TI-данные).

В добавление к предустановленной экспертизе (встроенным правилам на агенте, подробнее см. в разделе 11.10.5) или экспертизе, получаемой от сервера с TI-информацией, аналитик может создавать и редактировать собственные наборы правил, чтобы эффективнее обнаруживать вредоносную или аномальную активность в рамках определенной, хорошо ему известной инфраструктуры.

В программе предусмотрено создание множественных наборов, то есть аналитик может назначить агенту произвольное количество аналитических наборов. То же самое касается и наборов с исключениями.

Примечание

Наборы аналитических правил и исключений, получаемые Программой от TI-платформы (внешние наборы), помечаются значком TI , если наборы синхронизируются, и значком TI , если синхронизации нет. Аналитик может удалять несинхронизируемые наборы. При этом синхронизируемые наборы удалять и изменять аналитик не может. Если синхронизация внешнего набора завершилась с ошибкой, то такой набор помечается значком TI .

К инструментам анализа событий относятся:

1) Индикаторы атак (ИА);

2) Индикаторы компрометации (ИК);

3) YARA-правила (для файлов и памяти процесса);

4) Журналы.

Важно

Имена для индикаторов атак и индикаторов компрометации не должны превышать 200 символов (байтов).

Перечисленные компоненты передаются агенту в виде отдельных конфигурационных файлов и работают в режиме реального времени, при этом индикаторы компрометации и YARA-правила отвечают за статический анализ исполняемых файлов, а индикаторы атак за динамический анализ, то есть анализ во время выполнения программ.

Важно

Количественный показатель загружаемых на агенте EDR аналитических правил не предусматривается, вместо этого есть ограничения на максимальный объем файла с правилами, который не должен превышать 32 мегабайта. Для примера, если мы применяем файл с доменными именами (индикаторы компрометации), то 32 мегабайта вместят в себя около пятисот тысяч доменов.

Для YARA-правил действует ограничение в 1 гигабайт.

Аналитика подразумевает назначение двух типов действий:

1) Блокировать;
2) Детектировать.

Важно

В случае с журналами при обнаружении будет выполняться только детектирующее действие. Для YARA-правил по умолчанию выполняется блокирующее действие, но можно установить детектирующее действие в секции **meta** в поле **action**, указав действие **detect**.

По умолчанию файловая аналитика (подсчет хешей, матчинг индикаторов, сработки YARA-правил) выполняется только для исполняемых файлов и только при их запуске или загрузке, если исполняемый файл

– это динамически загружаемая библиотека. Опция профиля безопасности агента **Расширения файлов с потенциально активным содержимым** позволяет дополнительно указать расширения файлов (помимо исполняемых), для которых также требуется включить файловый анализ, который будет производиться в режиме реального времени при доступе к этим файлам.

Важно

Активная блокировка на срабатывания ИА, ИК и YARA-правил выполняется через модуль ядра, в режиме eBPF все блокировки переопределяются на детектирование.

В некоторых случаях при блокировании файлов может возникнуть коллизия, когда файл будет фактически заблокирован, но при этом открываться на машине с агентом. Происходит это вследствие того, что некоторые процессы могут кешировать файлы, предоставляя к этим файлам доступ после создания блокирующей аналитики, когда операция **чтение файла** становится недоступна.

В качестве примера приведем такой случай. Во время открытия произвольного pdf-файла программа-просмотрщик Windows glcnd.exe выполняет его чтение, после чего файл кешируется этим же процессом.

Далее аналитик создает индикатор компрометации, блокирующий доступ к упоминаемому выше файлу. Вследствие того, что файл закеширован процессом glcnd.exe, он открывается, так как фактически чтения файла в таком случае не выполняется, при этом в списке инцидентов у нас появится инцидент о срабатывании индикатора компрометации. После завершения процесса glcnd.exe рассматриваемая коллизия исчезнет.

При работе с аналитическими наборами и передаче изменений в них агенту необходимо помнить, что для применения на агенте измененных конфигураций правил требуется время, поэтому следует убедиться для корректной работы правил, что конфигурация применена на агенте (рис. 33).

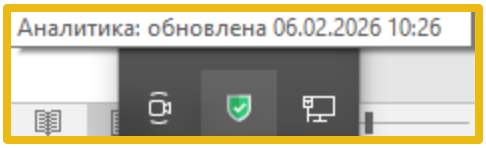


Рисунок 33 – Сообщение об обновлении аналитики в трее агента

Обычно операция отправки конфигурации на агент занимает не более пяти секунд.

11.10.1. Индикаторы атак

Индикаторы атак в общем смысле – это правила, позволяющие идентифицировать характерные потенциально опасные с точки зрения ИБ поведенческие паттерны программ, работающих на компьютерах защищаемого контура. В отличие от индикаторов компрометации, которые являются артефактами уже свершившейся кибератаки на ИС, индикаторы атак характеризуют определенную стадию прогрессирующей в данный конкретный момент кибератаки. Это принципиальное отличие позволяет детектировать и реагировать на кибератаку (в том числе автоматически) непосредственно в момент ее развития, в том числе на самом раннем этапе.

Для иллюстрации сказанного можно провести аналогию с банком и грабителем. Индикаторы компрометации в таком случае – это улики, оставленные грабителем после совершения им преступления. А индикаторы атак – это характерные признаки грабителя, который охрана банка распознает через систему видеонаблюдения, когда грабитель только приближается к банку или входит в него.

В EDR-решениях индикаторы атак реализуются за счет алгоритмов, выявляющих в потоке событий от программ, работающих на защищаемых компьютерах, определенные события или их цепочки, и выделяющих их в форму обнаружений (detections) или предупреждений (alerts), назначая им уровень угрозы, реакцию и др. атрибуты, характеризующие потенциальную атаку. Например, «процесс word.exe порождает дочерний процесс powershell.exe», или «процесс svchost.exe устанавливает сетевое соединение с хостом malwarehost.com» и т.п. Для каждого из приведенных примеров можно назначить уровень угрозы, а также предписать схему реагирования, например, запретить указанное действие. Также можно связать с правилом идентификаторы техники и тактики из широко известного классификатора угроз MITRE ATT&CK. Можно добавить тэги и/или связать правило с той или иной APT-группировкой.

Процесс поиска в потоке событий определенной последовательности событий, удовлетворяющих некоторому условию, называется корреляцией событий или матчингом над потоком событий. Этот процесс может происходить в режиме реального времени (на стороне агента EDR, в рамках его потока событий) или в оффлайн-режиме на стороне сервера EDR. Первый вариант позволяет выполнить противодействие (если требуется) в режиме реального времени, не давая атаке шанса развиться, однако ограничен рамками событий

только одного агента. Второй вариант не позволяет выполнить противодействие в режиме реального времени, т.к. требуется какое-то время, чтобы события, возникающие на агенте, были доставлены до сервера и обработаны им, перед тем как сервер сможет выполнить корреляцию. При этом возможно произвести корреляцию среди нескольких агентов и источников событий (как, например, в SIEM-системах). Автоматизированное реагирование в таком случае заключается в отправке команды по нейтрализации атаки от сервера к агенту. Весь процесс при этом, как правило, стремится выполниться за некоторое нормативное (но не гарантированное) сравнительно короткое время, чтобы прогресс атаки с момента ее обнаружения был минимальным.



Важно

В режиме eBPF (Linux) индикаторы атак работают только на детектирование, то есть для индикаторов атак автоматически определяется тип действия **Детектировать**, даже если в правилах было установлено блокирующее действие.

Определение индикаторов атак в RT Protect EDR

ИА в системе RT Protect EDR представляют собой правила корреляции событий **на стороне агента в режиме реального времени**. При описании семантики ИА ниже будут использоваться термины модели данных событий RT Protect EDR (см. пункт **Состав и типы полей событий**

Полный перечень доступных полей событий

ИА имеют следующие атрибуты (поля):

1. **Имя**. Кратко описывает суть выявляемой индикатором активности или угрозы (например, SuspiciousOfficeChildProcess и т.п.). Имя является уникальным и используется для идентификации ИА в разных ситуациях. Если ИА соответствует известному sigma-правилу, то «хорошим тоном» будет использование имени этого sigma-правила в качестве имени индикатора (например, proc_creation_win_powershell_download_patterns).



Примечание

При срабатывании индикатора его имя будет указано в поле **rul** сгенерированного события-обнаружения и может использоваться при написании программного исключения для борьбы с ложноположительными срабатываниями ИА в ситуации, когда непосредственно уточнить логику (условие срабатывания) индикатора не представляется возможным.

2. **Тип**. Тип ИА однозначно идентифицирует тип события, возникновение которого на агенте всякий раз будет являться поводом к матчингу индикатора. Например, если ИА имеет тип «Старт процесса», то каждый раз при запуске процесса агент будет анализировать это событие на предмет соответствия одному или нескольким ИА этого типа, назначенных ему. При срабатывании ИА в поток событий наряду с исходным событием будет вставлено соответствующее ему событие-обнаружение, в поле **Правило** (rul) которого будет указано имя индикатора, а в полях **Критичность** (svrt), **Действие** (act) и **MITRE** (mitre) будут перенесены значения соответствующих полей индикатора (см. ниже). Полный перечень доступных типов ИА в системе RT Protect EDR представлен в пункте

3. Типы индикаторов атак

4. **Условие**. Условие является логическим выражением в терминах схемы событий RT Protect EDR и определяет условие срабатывания ИА при возникновении на агенте события заданного типа. Синтаксис и семантика условных выражений описывается в пункте

5. Синтаксис и семантика условных выражений индикаторов атак.

6. **Критичность**. Критичность определяет соответствующий атрибут события-обнаружения, возникающего при срабатывании ИА.

7. **Действие**. Действие определяет автоматизированную реакцию на возникшее событие в случае срабатывания для него ИА. В качестве действия предусматривается возможность блокирования соответствующей исходной активности, приведшей к срабатыванию индикатора. Альтернативой является генерация события-обнаружения без реагирования (т.е. только детектирование).

8. **Режим**. Режим работы ИА определяет механику генерации события-обнаружения при срабатывании индикатора. Предусматриваются следующие режимы:

– обычный;

– без генерации события-обнаружения;

– с однократной генерацией события-обнаружения (в этом режиме для каждого процесса (приложения), в контексте которого сработал ИА, событие-обнаружение генерируется только один раз).

Для всех режимов реакция, если она предписана, выполняется всякий раз при срабатывании ИА.

9. **Классификатор MITRE ATT&CK**. Ссылка на классификатор угроз MITRE ATT&CK позволяет связать ИА с известной вредоносной техникой и тактикой, что впоследствии при срабатывании ИА из-за выявленной атаки на ИС позволяет аналитику наглядно видеть задействованные атакующими техники/тактики и получить по ним сводную справочную информацию из классификатора.

10. **Описание**. Краткое описание активности, выявляемой ИА.

11. **Комментарий**. Развернутое описание активности, выявляемой ИА.

Если для некоторого исходного события срабатывает больше одного ИА, то результирующее действие (реакция) в отношении данного события определяется как «блокировать», если хотя бы один из сработавших ИА предписывает соответствующую реакцию.



Важно

В режиме работы агента «только детектирование» для всех ИА, назначенных ему, игнорируется предписываемое ИА блокирующее действие (см. пункт 11.28.2).

Типы индикаторов атак

В Программе представлено 27 типов ИА, а именно:

1) Установка исходящего сетевого соединения (CONNECT);
2) Прием входящего сетевого соединения (ACCEPT);
3) Инициирование защищенного SSL-соединения (сообщение SSL HELLO);
4) Открытие локального порта на прием входящих соединений (LISTEN);
5) Получение ответа сервиса DNS (DNS RESPONSE);
6) Создание нового файла (CREATE NEW);
7) Переименование файла (RENAME);
8) Удаление файла (DELETE);

9) Прямой доступ к диску (тому) на чтение (DISK READ);

10) Прямой доступ к диску (тому) на запись (DISK WRITE);

11) Создание именованного канала (CREATE NAMED PIPE);

12) Подключение к именованному каналу (CONNECT NAMED PIPE);

13) Доступ к файлу (ACCESS);

14) Создание альтернативного потока для файла (CREATE STREAM HASH)

15) Создание ключа реестра (CREATE KEY);

16) Удаление ключа реестра (DELETE KEY);

17) Изменение значения реестра (SET VALUE);

18) Удаление значения реестра (DELETE VALUE);

19) Переименование ключа реестра (RENAME KEY);

20) Загрузка драйвера (LOAD DRIVER);

21) Создание процесса (CREATE PROCESS);

22) Завершение процесса (STOP PROCESS);

23) Загрузка образа (LOAD IMAGE);



Важно

Индикатор, блокирующий загрузку образа, распространяется на работу всей системы, поэтому желательно однозначно идентифицировать блокируемые библиотеки при создании индикаторов.

24) Доступ к стороннему процессу (OPEN PROCESS);

25) Создание нити (потока) в стороннем процессе (CREATE REMOTE THREAD);

26) Доступ к нити стороннего процесса (OPEN THREAD);

27) Загрузка образа в сторонний процесс (LOAD REMOTE IMAGE);

Важно

Для некоторых индикаторов атак можно задавать только детектирующее действие, это относится к таким типам индикаторов, как **Завершение процесса** и **Открытие локального порта на прием (LISTEN)**.

Синтаксис и семантика условных выражений индикаторов атак

В системе RT Protect EDR условные выражения индикаторов атак являются логическими (т.е. результат выражения – это «истина» или «ложь») и имеют Си-подобный синтаксис.

Лексическая грамматика

Выражения состоят из последовательности токенов, каждый из которых может быть идентификатором (identifier), ключевым словом (keyword), константой (constant), строкой (string-literal) или символом пунктуации (punctuator), согласно грамматике ниже:

1) token:

– identifier;

– keyword;

– punctuator;

– constant;

– string-literal.

Каждая из перечисленных синтаксических категорий будет рассмотрена подробно ниже.

Идентификатор – это буквенно-цифровая последовательность, начинающаяся с буквы. Идентификаторы семантически могут обозначать ключевые слова или поля схемы данных событий, задействованные в выражениии. Идентификаторы могут включать символы A-Z,a-z,_,0-9, согласно грамматике ниже:

1) identifier:

– nondigit;

– identifier nondigit;

– identifier digit;

2) nondigit: один из

– _ a b c d e f g h i j k l m;

– n o p q r s t u v w x y z;

– A B C D E F G H I J K L M;

– N O P Q R S T U V W X Y Z;

3) digit: один из

– 0 1 2 3 4 5 6 7 8 9.

Ключевые слова – это идентификаторы, которые зарезервированы для нужд языка написания условных выражений ИА, согласно грамматике ниже:

1) keyword: один из

– true false matches rematches lookup contains icontains iequals startswith;

– istartswith endswith iendswith and not or

Символы пунктуации – это определенные последовательности, используемые для обозначения операторов, согласно грамматике ниже:

1) punctuator: один из

– ( ) .

– & * + - ~ !

– / % << >> < > <= >= ==

– != ^ | && ||

Константа – это непосредственно заданное числовое значение, согласно грамматике ниже:

1) integer-constant:

– decimal-constant;

– hexadecimal-constant;

2) decimal-constant:

– decimal-constant digit;

3) hexadecimal-constant:

– hexadecimal-prefix hexadecimal-digit;

– hexadecimal-constant hexadecimal-digit;

4) hexadecimal-prefix: один из

– 0x 0X;

hexadecimal-digit: один из

– 0 1 2 3 4 5 6 7 8 9;

– a b c d e f;

– A B C D E F.

Строка – это последовательность символов, заключенная в двойные кавычки, согласно грамматике ниже:

1) string-literal:

– "s-char-sequence";

2) s-char-sequence:

– s-char;

– s-char-sequence s-char;

3) s-char:

– любой элемент исходной кодировки, кроме двойной кавычки, обратной косой черты (\) и символа новой строки.

Символ \ внутри строки используется для обозначения escape-последовательности, согласно грамматике ниже:

1) escape-sequence:

– simple-escape-sequence;

– hexadecimal-escape-sequence;

2) simple-escape-sequence: один из

– \n \r \t \" \\

3) hexadecimal-escape-sequence:

– \x hexadecimal-digit;

– hexadecimal-escape-sequence hexadecimal-digit.

Типы операндов

Операндами условных выражений ИА в Программе являются значения полей событий, адресуемые в выражении по именам полей, согласно модели данных событий.



Важно

Для каждого типа ИА при написании его условного выражения доступны только поля соответствующего ему типа события, а также дополнительно поля общей части событий.

В условных выражениях ИА (как и в модели данных событий) операнды могут иметь следующие типы:

– bool (true/false);

– uint (целочисленный беззнаковый разрядностью 64 бита);

– string (строковый);

– exclusion_flags (одноименная структура битовых флагов);

– runtime_flags0 (одноименная структура битовых флагов);

– runtime_flags1 (одноименная структура битовых флагов);

– load_image_flags (одноименная структура битовых флагов);

– create_remote_thread_flags (одноименная структура битовых флагов);

– net_event_flags (одноименная структура битовых флагов);

– time (время, временной штамп);

– set (набор обнаружений).

Состав операторов

Набор операторов, доступных в условных выражениях ИА RT Protect EDR достаточно типичен и включает в себя логические, арифметические, строковые, битовые и специальные операторы, а также операторы сравнения.

Логические операторы

! (not) – логическое отрицание (логическое «НЕ»);

&& (and) – конъюнкция (логическое «И»);

|| (or) – дизъюнкция (логическое «ИЛИ»).

Операторы сравнения

== (bool, число, строка);

!= (bool, число, строка);

> (число);

< (число);

>= (число);

<= (число);

iequals (строка) – сравнение без учета регистра.

Строковые операторы

matches – соответствие строки паттерну с учетом регистра, определяемому регулярным выражением с использованием символов * и ?;

rematches – соответствие строки паттерну с учетом регистра, определяемому регулярным выражением в синтаксисе POSIX EXTENDED;

startswith – проверка префикса строки с учетом регистра;

istartswith – проверка префикса строки без учета регистра;

endswith – проверка суффикса строки с учетом регистра;

iendswith – проверка суффикса строки без учета регистра;

contains – проверка вхождения подстроки с учетом регистра;

icontains – проверка вхождения подстроки без учета регистра;

Арифметические операторы

+ (в т.ч. унарный) – сложение или унарный «минус»;

- (в т.ч. унарный) – вычитание или унарный «плюс»;

* – умножение;

/ – деление;

% – остаток от деления;

<< – логический сдвиг влево;

>> – логический сдвиг вправо.

Битовые операторы

^ – побитовое исключающее «ИЛИ»;

& – побитовое «И»;

| – побитовое «ИЛИ»;

~ – побитовое «НЕ».

Специальные операторы

. (оператор разыменования);

(– открывающая скобка;

) – закрывающая скобка.

Для доступа к отдельным флагам структур типа exclusion_flags, runtime_flags0, runtime_flags1, load_image_flags и create_remote_thread_flags предназначен оператор разыменования. Для получения целочисленного значения структуры с флагами используется конструкция .value.



Примечание

Оператор разыменования позволяет обращаться к отдельным полям значений временных типов, а именно: Year, Month, DayOfWeek, Day, Hour, Minute, Second, Milliseconds, например: time.Year == 2022 && time.Month == 12. Также можно использовать поля time_span_millis, time_span_sec, time_span_min, чтобы получить общее значение времени, выраженное в миллисекундах, секундах или минутах, соответственно.

Также оператор разыменования может использоваться применительно к строковым типам в следующих случаях:

– для перевода строки в нижний регистр (.lower) (пример: cmdl.lower matches "*something*");

– получения имени файла (.name) или пути (.path), если строка ссылается на полный путь с именем файла (пример: app.name iequals "myapp.exe" или app.path iendswith "\\windows\\system32\\");

– получения длины строки (.length) (пример: cmdl.length > 32).

Состав и типы полей событий

Полный перечень доступных полей событий

Нативные поля событий Программы для написания индикаторов атак описаны в таблице 45.

Таблица 45 – Поля для написания индикаторов атак

Наименование поля	Тип поля	Описание	Тип ИА
act	uint	Действие, предпринятое агентом до матчинга ИА	Любой
time	time	Время регистрации события	
pid	uint	Идентификатор процесса на агентской системе	
ppid	uint	Идентификатор родительского процесса на агентской системе	
app	string	Полное имя исполняемого файла процесса	
cmdl	string	Командная строка процесса	
argc	uint	Количество аргументов	
sess	uint	Номер сессии, в которой работает процесс на агентской системе	
rf0	runtime_flags0	Поведенческие признаки процесса (первая группа)	
rf1	runtime_flags1	Поведенческие признаки процесса (вторая группа)	
exclf	exclusion_flags	Флаги исполняемого файла процесса	
sid	string	SID пользователя, создавшего процесс	
app_sgnr	string	Издатель ЭП исполняемого файла процесса	
agent_build_number	uint	Номер сборки агента	
history	set	История сработавших индикаторов атак	
hive_history	set	История обнаружений группы процессов	
sys_history	set	История всех сработок в системе	
time_now	time	Текущее время	

Наименование поля	Тип поля	Описание	Тип ИА
time_nil	time	Нулевое (пустое время)	
proto	uint	Протокол	Любой сетевой
ipv6	bool	Признак работы по IPv6	
out	bool	Отправка (1) или прием (0)	
size	uint	Размер полезных данных (payload) сетевого пакета	
host	string	Имя хоста, соответствующее удаленному IP	
ssl_h	string	Имя хоста (server_name) из сообщения SSL Client Hello	Сеть: SSL HELLO Сеть: DNS-ответ
dnsq_h	string	Имя хоста из DNS-запроса	
dnsq_t	uint	Тип DNS-запроса	
dnsq_s	uint	Статус DNS-запроса	
dnsq_r	string	Результат DNS-запроса	
r_p	uint	Удаленный порт	Любой сетевой, кроме Сеть: Открытие локального порта на прием (LISTEN)
r_ip	string	Удаленный IP-адрес	
r_ip_v4_value	uint	Удаленный IPv4-адрес в форме числа	
l_p	uint	Локальный порт	Любой сетевой
l_ip	string	Локальный IP-адрес	
l_ip_v4_value	uint	Локальный IPv4-адрес в форме числа	
netf	net_event_flags	Сетевые флаги	
who	string	Полное имя исполняемого модуля–инициатора операции	Сеть; Процессы; Файлы; Реестр.
whof	exclusion_flags	Флаги исполняемого модуля–инициатора операции	
whotid	uint	Идентификатор нити–инициатора операции	
whoaddr	uint	Стартовый адрес нити–инициатора операции	
trace	string	Стек вызовов операции	
wdir	string	Рабочий каталог процесса	Процессы: Старт процесса
cmdlp	string	Командная строка родительского процесса	
cmdlg	string	Командная строка прародителя (grand parent)	
when	time	Время создания процесса	
cpath	string	Полное имя процесса-инициатора операции	
prot	uint	Уровень защиты процесса	
base	uint	Базовый адрес исполняемого образа в памяти	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа
isize	uint	Размер исполняемого образа в памяти	

Наименование поля	Тип поля	Описание	Тип ИА
			Процессы: Загрузка образа в сторонний процесс
crtime	time	Время создания файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу Файлы: Создание альтернативного потока для файла
chtime	time	Время последнего изменения файла	
fsize	uint	Размер файла	
ftype	uint	Тип файла	
attr	uint	Атрибуты файла	
sha1	string	SHA-1 файла	
md5	string	MD5 файла	
sha256	string	SHA-256 файла	
sgnr	string	Электронная подпись файла	
sgnr_s	uint	Статус электронной подписи файла	
pack	string	Тип упаковщика файла	
ofn	string	Оригинальное имя файла	
fcomp	string	Компания-издатель файла	
fver	string	Версия файла	
fdesc	string	Описание файла	
fprod	string	Продукт, к которому относится файл	
fwhite	bool	Признак нахождения файла в белом списке (по содержимому)	
path	string	Полное имя файла образа	Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс
imgf	exclusion_flags	Флаги образа	
ldf	load_image_flags	Флаги операции загрузки образа	
tpath	string	Полный путь и имя исполняемого файла целевого процесса	Процессы: Загрузка образа в сторонний процесс Процессы: Доступ к процессу Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе
tpid	uint	Идентификатор целевого процесса	
targf	exclusion_flags	Флаги образа целевого процесса	
trf0	runtime_flags0	Поведенческие признаки целевого процесса (первая группа)	
trf1	runtime_flags1	Поведенческие признаки целевого процесса (вторая группа)	
tid	uint	Идентификатор целевой нити	Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе

Наименование поля	Тип поля	Описание	Тип ИА
taddr	uint	Стартовый адрес целевой нити	Процессы: Создание нити в стороннем процессе
tf	create_remote_thread_flags	Флаги нити	
dsrd	uint	Запрашиваемые права доступа к процессу/нити	Процессы: Доступ к процессу Процессы: Доступ к нити процесса
grnt	uint	Предоставленные права доступа к процессу/нити	
asep	bool	Ключ/значение относится к категории автозапуска	Любой реестровый тип ИА
key	string	Путь ключа	
val_n	string	Имя значения реестра	Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа
val_t	uint	Тип значения реестра	Реестр: В значение ключа записаны данные
val_s	uint	Размер данных значения	
val_d	string	Данные значения	
new	string	Новое имя ключа	Реестр: Ключ переименован
name	string	Полное имя файла	Любой файловый
fnew	string	Новое имя файла	Файлы: Файл переименован
owrt	bool	Признак перезаписи файла	
delete	bool	Доступ на удаление	Файлы: Доступ к файлу
read	bool	Доступ на чтение	
modify	bool	Доступ на модификацию	
save	bool	Для файла была создана резервная копия	Файлы: Удален файл Файлы: Файл переименован
ads	bool	Операция совершается над альтернативным потоком данных файла	Файлы: Удален файл Файлы: Файл переименован Файлы: Создан новый файл Файлы: Доступ к файлу
arun	bool	Файл расположен в директории автозапуска	Файлы: Файл переименован Файлы: Создан новый файл

Аналитик может создавать инидикаторы атак, используя только представленные в таблице 45 поля, использование других полей из модели данных, которые обнаруживаются EDR и представлены в событиях

активности, не приведет к срабатыванию индикатора атаки. При этом при создании подобного индикатора Программа укажет на необходимость изменения условия, но даст возможность такой индикатор сохранить.



Примечание

Поле trace, которое доступно при написании условий ИА, имеет специфический формат – это последовательность строк, разделенных символом |, а каждая строка – это путь до исполняемого модуля или адрес в памяти (если модуль определить не удалось). Кроме того, путь в данном случае представляется в так называемом компактном виде. Пример: *1\kernel32.dll. Подробнее смотри в подпункте 9.1.

Атрибуты файлов (поле attr)

Атрибуты файла – это метаданные, которые ассоциированы с файлом и находятся в структурах файловой системы целевой ОС.

Windows-агент: допустимые значения комбинации атрибутов файла описаны в документации Windows – https://learn.microsoft.com/en-us/windows/win32/fileio/file-attribute-constants.

Тип файла (ftype)

Тип файла отражает внутреннюю классификацию файла со стороны агента.

Допустимы следующие значения:

0 – тип не определен;

1 – «обычный» файл;

2 – исполняемый файл;

3 – файл с активным содержимым;

4 – скрипт PowerShell.

Права доступа к процессам и нитям (поля dsrd и grnt)

Windows-агент: допустимые значения комбинации прав доступа к процессам описаны в документации Windows – https://learn.microsoft.com/ru-ru/windows/win32/procthread/process-security-and-access-rights.

Windows-агент: допустимые значения комбинации прав доступа к нитям описаны в документации Windows – https://learn.microsoft.com/ru-ru/windows/win32/procthread/thread-security-and-access-rights.

Статус ЭП файла (поле sgnr_s)

Поле sgnr_s может принимать одно из следующих значений:

0 – нет ЭП;

1 – есть ЭП;

2 – статус ЭП не определен.

Уровень защиты процесса (поле prot)

Уровень защиты процесса относится к подсистеме управления защищенными процессами Windows PPL (Protected Process Light).

Разделив значение prot на 16, можно получить один из уровней защиты, согласно документации Windows – https://learn.microsoft.com/ru-ru/windows/win32/api/processthreadsapi/ns-processthreadsapi-process_protection_level_information.

Первая группа runtime-флагов процесса (поле rf0 и др.)

Runtime-флаги представляют собой набор флагов процесса, которые отражают те или иные поведенческие особенности процесса и могут меняться (добавляться) с течением времени. Полный список можно просмотреть в таблице 46.

Таблица 46 – Описание первой группы runtime-флагов процесса

Имя флага	Числовая маска флага	Описание флага
ProcHiveRoot	0x1	Главный процесс группы
Wow64	0x2	32-х битный в 64-х битной системе
Native	0x4	Доверенный
Synthetic	0x8	Событие создания синтезировано
Managed	0x10	.NET
RunWithUAC	0x20	UAC
DroppedByParent	0x40	Родитель создал и запустил
LaterStage	0x80	Основные системные модули загружены

Имя флага	Числовая маска флага	Описание флага
IsInjected	0x100	API-вызовы контролируются
FromExplorer	0x200	В цепочке родителей есть EXPLORER
SuspiciousDirectory	0x400	Каталог запуска: RECYCLER, System Volume Information и т.п.
TempDirectory	0x2000	Каталог запуска: временный
SystemTempDirectory	0x4000	Каталог запуска: системный временный
NetworkDirectory	0x8000	Каталог запуска: сетевой путь
AutorunDirectory	0x20000	Каталог запуска: автозапуск
SystemDirectory	0x40000	Каталог запуска: системный
ProgramFilesDirectory	0x80000	Каталог запуска: Program Files
PreInitialUpdate	0x200000	Событие предшествовало первичному обновлению аналитики
NetMalwareSignature	0x400000	Срабатывание ИК в сетевом трафике: сигнатура
BlacklistedNetworkAccess	0x800000	Попытка обращения по сети к заблокированным IP-адресам/доменным именам
NetworkServer	0x1000000	Прослушивание сетевого порта, кроме loopback
NetworkAccess	0x2000000	Сетевой обмен (кроме loopback)
NetIOC	0x10000000	Срабатывание ИК в сетевом трафике: IP-адрес/доменное имя
Tampering	0x2000000000000	Применение техник подмены исполняемых образов
PostModified	0x4000000000000	Исполняемый файл модифицирован после проецирования
Deleted	0x8000000000000	Исполняемый файл удален
Renamed	0x10000000000000	Исполняемый файл переименован
FromServices	0x20000000000000	В цепочке родителей есть диспетчер служб
FromBrowser	0x40000000000000	В цепочке родителей есть браузер
FromOffice	0x80000000000000	В цепочке родителей есть офисная программа
Protected	0x100000000000000	Защищенный процесс/Windows Protected Process
Transacted	0x200000000000000	Транзакция на исполняемом файле
Trustlet	0x400000000000000	Изолированный процесс/Isolated User Mode Process
WhiteListed	0x800000000000000	Известный легальный
Trusted	0x1000000000000000	Подписан

Имя флага	Числовая маска флага	Описание флага
Untrusted	0x2000000000000000	Не подписан
Elevated	0x4000000000000000	Повышенные привилегии/Elevated

Вторая группа runtime-флагов процесса (поле rf1 и др.)

Runtime-флаги представляют собой набор флагов процесса, которые отражают те или иные поведенческие особенности процесса и могут меняться (добавляться) с течением времени (таблица 47).

Таблица 47 – Описание второй группы runtime-флагов процесса

Имя флага	Числовая маска флага	Описание флага
RegSecurityModify	0x1	Модификация security эл-тов реестра
RegStorePE	0x2	Запись потенциального исполняемого файла в реестр
InstallService	0x4	Регистрация службы в реестре
RegAsepModify	0x8	Модификация точек автозапуска реестра
MsHtaRun	0x10	Запуск утилиты mshta
Regsvr32Run	0x20	Запуск утилиты regsvr32
VerclsidRun	0x40	Запуск утилиты verclsid
SystemRestoreDisable	0x80	Выключение механизма восстановления системы
IcaclsRun	0x100	Запуск icacls
HhRun	0x200	Запуск просмотрщика chm-файлов
PsExecRun	0x1000	Запуск psexec
PowerShellRun	0x2000	Запуск powershell
CmdScriptRun	0x4000	Запуск cmd /c
TaskManage	0x8000	Запуск планировщика задач с параметрами /create или /change
MsiExecRun	0x10000	Запуск msiexec
Rundll32Run	0x20000	Запуск rundll32
ScriptRun	0x40000	Запуск скриптового интерпретатора
WhoAmIRun	0x80000	Выполнение команды whoami
ShellCodeExec	0x100000	Выполнение shell-кода
ContainsManagedCode	0x200000	Содержит .NET-код
MapRemoteView	0x400000	Проецирование образа в сторонний процесс
DoSpoofParentId	0x800000	Подмена родителя дочернему процессу
CreateRemoteThread	0x1000000	Создание нити в стороннем процессе
CmdLineTampering	0x2000000	Подмена командной строки
OpenThread	0x4000000	Открытие сторонней нити
OpenProcess	0x8000000	Открытие стороннего процесса
ControlPanelRun	0x10000000	Запуск панели управления Windows

Имя флага	Числовая маска флага	Описание флага
CMSTPRun	0x20000000	Запуск установщика профилей диспетчера подключений Windows
InstallUtilRun	0x40000000	Запуск установщика INF-файлов
OdbcconfRun	0x80000000	Запуск утилиты администрирования ODBC
RegAsmRun	0x100000000	Запуск утилиты регистрации .NET-сборок
MmcRun	0x400000000	Запуск консоли управления Windows
Unprotected	0x800000000	Не штатно уменьшен уровень защиты
ProtectionElevated	0x1000000000	Нештатно увеличен уровень защиты
HasRemoteView	0x2000000000	Содержит спроецированный извне образ
Tampered	0x4000000000	Подменен образ исполняемого файла
HasRemoteThread	0x8000000000	Содержит нить, созданную извне
ThreadOpen	0x10000000000	Открытие нити процесса извне
ProcessOpen	0x20000000000	Открытие процесса извне
SpoofParentId	0x200000000000	Подменен родительский процесс
RegisterTask	0x400000000000	Создание файлов в каталоге задач
SetAutorun	0x800000000000	Создание файлов в каталоге автозапуска
CreateMofFile	0x1000000000000	Создание *.mof-файлов в каталоге WMI
ReadSystemPEFile	0x2000000000000	Чтение системных исполняемых файлов, не связанное с их запуском
WriteExeFile	0x4000000000000	Запись в исполняемые файлы
NamedPipeClient	0x8000000000000	Клиент именованного канала
HasStreamComponent	0x10000000000000	В имени исполняемого файла присутствует компонент ntfs-потока
UnusualExeFileExtension	0x20000000000000	Имя исполняемого файла имеет нетипичное расширение
RandomFileName	0x40000000000000	Случайное имя файла
NamedPipeServer	0x80000000000000	Сервер именованного канала
CreateExeFile	0x100000000000000	Создание файлов с потенциально активным содержимым

Флаги исполняемых файлов (exclf и др.)

Флаги исполняемого файла – это признаки, сформированные по неизменным статическим данным файла или процесса, таким как его полное имя, оригинальное имя файла, информация об ЭП, комбинация командных строк. Определенные флаги доступны при написании исключений для программ, таким образом, они могут быть ассоциированы с теми или иными исполняемыми образами и будут учитываться агентом. Данные флаги не меняются с течением времени (при условии, что не меняются исключения для программ). Список флагов представлен в таблице 48.

Таблица 48 – Флаги исполняемых файлов

Имя флага	Числовая маска флага	Описание флага
DontSuppressEvents	0x1	Запрет принудительного подавления событий (*)
TaskScheduler	0x2	Планировщик задач tasksched
AllowCodeInjection	0x4	Разрешение внедрения кода в сторонние программы (*)
AllowWrite	0x8	Разрешение записи памяти сторонних программ (*)
Rundll32	0x10	DLL-хост rundll32
PowerShell	0x20	Интерпретатор powershell
Cmd	0x40	Командный интерпретатор cmd
MsiExec	0x80	Установщик программ msiexec
Explorer	0x100	Проводник explorer
CSS	0x200	Критический системный компонент
MsHta	0x400	Хост HTML-приложений mshta
Svchost	0x800	Хост служб svchost или его компонент
Lsass	0x1000	Системный компонент LSASS
AllowControlRead	0x2000	Разрешение чтения памяти сторонних программ и управления ими (*)
Prefetcher	0x4000	Служба префетчера Windows
ControlPanel	0x8000	Панель управления Windows
ScriptEngine	0x10000	Скриптовый движок
ImageWow64	0x20000	Компонент имеет 32-х битную и 64-х битную версию (*)
HostProcess	0x40000	Хост-процесс или его компонент
WhoAmI	0x80000	Утилита whoami
Csrss	0x100000	Системный компонент CSRSS
SkipInboundNetEvents	0x200000	Исключение из телеметрии входящих сетевых событий (*)
TCB	0x400000	Максимальное доверие
NTDLL	0x800000	Системная библиотека NTDLL
Vssadmin	0x1000000	Утилита управления резервным копированием vssadmin
Wmic	0x2000000	Утилита администрирования wmic
Wbadmin	0x4000000	Утилита администрирования wbadmin
BcdEdit	0x8000000	Утилита управления параметрами загрузки BCDEdit
DiskShadow	0x10000000	Утилита управления резервным копированием Diskshadow
Icacls	0x20000000	Утилита управления правами доступа к файлам iCACLS
PsExec	0x40000000	Утилита удаленного администрирования PsExec
VerifyTrust	0x80000000	Подтверждение по электронной подписи (*)
SkipAllEvents	0x100000000	Исключение всей телеметрии (*)

Имя флага	Числовая маска флага	Описание флага
Browser	0x200000000	Браузер
Office	0x400000000	Офисная программа
AllowDirectDiskWrite	0x800000000	Разрешение прямого доступа к диску для записи (*)
AllowDirectDiskRead	0x1000000000	Разрешение прямого доступа к диску для чтения (*)
CSSFriendly	0x2000000000	Право взаимодействия с критическими системными программами (*)
SkipOutboundNetEvents	0x4000000000	Исключение из телеметрии исходящих сетевых событий (*)
SkipFsEvents	0x8000000000	Исключение из телеметрии файловых событий (*)
SkipRegEvents	0x10000000000	Исключение из телеметрии событий реестра Windows (*)
AVEngine	0x20000000000	Антивирусный компонент (*)
SkipPmEvents	0x40000000000	Исключение из телеметрии событий поведения (*)
Verclsid	0x80000000000	Утилита Verclsid
Regsvr32	0x100000000000	Утилита Regsvr32
FsUtil	0x200000000000	Утилита FsUtil
SuppressDnsChecks	0x400000000000	Исключение анализа событий DNS (*)
TrustedDotNet	0x800000000000	.NET-компоненты, которым есть доверие
CMSTP	0x1000000000000	Установщик профилей менеджера подключений Windows
WmiPrvSE	0x2000000000000	Хост WMI
InstallUtil	0x4000000000000	Утилита установки INF-файлов
Odbcconf	0x8000000000000	Утилита конфигурации ODBC
DontInjectDll	0x10000000000000	Запрет внедрения DLL (*)
SuppressNetChecksIn	0x20000000000000	Исключение анализа входящей сетевой активности (*)
KnownDll	0x40000000000000	Известная DLL
DotNetNativeImage	0x80000000000000	Нативная версия .NET-сборки
KernelDll,	0x100000000000000	Системная библиотека KERNEL32 или KERNELBASE
SuppressFsChecks	0x200000000000000	Исключение анализа файловой активности (*)
RegAsm	0x400000000000000	Утилита регистрации .NET-сборки
SuppressNetChecksOut	0x800000000000000	Исключение анализа исходящей сетевой активности (*)
Mmc	0x1000000000000000	Консоль управления Windows
SuppressloaMatch	0x2000000000000000	Исключение матчинга индикаторов атак (*)
Hh	0x4000000000000000	Просмотрщик chm-файлов

Флаги операции загрузки исполняемого образа (поле ldf)

Флаги операции загрузки исполняемых образов – это комбинация признаков, касающихся конкретной операции загрузки исполняемого образа. Список флагов представлен в таблице 49.

Таблица 49 – Флаги операции загрузки исполняемого образа

Имя флага	Числовая маска флага	Описание флага
ImageScriptEng	0x1	Скриптовый движок
ImageRenamed	0x2	Переименованный образ
ImageManaged	0x4	Управляемый образ
ImageRandomName	0x8	Имя образа похоже на случайную последовательность знаков
ImageRemap	0x10	Образ загружается повторно
ImageInjected	0x20	Образ внедрен сторонним процессом
ImageTransacted	0x40	На файле образа действует транзакция ФС
ImageUnsigned	0x80	Образ не имеет встроенной ЭП
ImageSigned	0x100	Образ имеет встроенную ЭП
ImageSyntheticLoad	0x200	Синтетическое событие
ImageSigningPropsAvailable	0x400	Имеется информация об ЭП, полученная от системы
ImageWhiteListed	0x800	Доверенный образ
ImageDeleted	0x1000	Файл образа удален
ImagePostModified	0x2000	Файл образа модифицирован после проецирования

Флаги операции создания нити (поле tf)

Флаги операции создания нити – это комбинация признаков, касающаяся конкретной операции создания нити (таблица 50).

Таблица 50 – Флаг операции создания нити

Имя флага	Числовая маска флага	Описание флага
Float	0x1	Шеллкод

Флаги сетевого события (поле netf)

Флаги сетевого события – это комбинация признаков, относящихся к сетевым артефактам, имеющимся в событии (таблица 51).

Таблица 51 – Флаги сетевого события

Имя флага	Числовая маска флага	Описание флага
EndpointWhiteListed	0x1	Доверенный эндпоинт
RequestDomainNameWhiteListed	0x2	Доверенное запрашиваемое доменное имя

Тип значения реестра (поле val_t)

Тип значения реестра – это числовое значение, определяющее, как должны интерпретироваться данные в значении реестра согласно документации ОС Windows – https://learn.microsoft.com/ru-ru/windows/win32/sysinfo/registry-value-types.

Поля модели данных sysmon

Модель данных sysmon частично поддерживается в форме набора синонимов над мнемониками нативной модели RT Protect EDR. В событиях поля модели данных sysmon отсутствуют – они существуют только виртуально в условных выражениях ИА.

Полный перечень синонимов sysmon, а также их соответствие типам ИА и полям нативной модели данных событий, описано в таблице 52.

Таблица 52 – Поля модели данных Sysmon

Имя	Тип поля	Тип ИА	Нативное имя
UtcTime	time	любой	time
ProcessId, SourceProcessId	uint	любой	pid
ParentProcessId	uint	любой	ppid
Image, SourceImage	string	любой	app (с буквой диска)
TerminalSessionId	uint	любой	sess
User	string	любой	sid
CommandLine	string	любой	cmdl
CallTrace	string	OPEN PROCESS OPEN THREAD	trace
SourceThreadId	uint	любой	whotid
Protocol	uint	CONNECT ACCEPT LISTEN SSL HELLO DNS RESPONSE	proto
QueryName	string	DNS RESPONSE	dnsq_h
QueryStatus	uint	DNS RESPONSE	dnsq_s
QueryResults	string	DNS RESPONSE	dnsq_r
SourceIsIpv6, DestinationIsIpv6	bool	CONNECT ACCEPT	ipv6
SourceHostname	string	ACCEPT	*
DestinationHostName	string	CONNECT	*

Имя	Тип поля	Тип ИА	Нативное имя
SourceIp	string	CONNECT ACCEPT	*
SourcePort	uint	CONNECT ACCEPT	*
DestinationIp	string	CONNECT ACCEPT	*
DestinationPort	uint	CONNECT ACCEPT	*
Initiated	bool	CONNECT ACCEPT	*
ParentCommandLine	string	CREATE PROCESS	cmdlp
CurrentDirectory	string	CREATE PROCESS	wdir
ParentImage	string	CREATE PROCESS	cpath (с буквой диска)
FileVersion	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	fver
Description	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	fdecs
Company	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	fcomp
Product	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	fprod
OriginalFileName	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	ofn
Signature	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	sgnr
SignatureStatus	uint	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	*
Signed	bool	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	*

Имя	Тип поля	Тип ИА	Нативное имя
Hashes	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	*
ImageLoaded	string	LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE	path (с буквой диска)
TargetProcessId	uint	OPEN PROCESS OPEN THREAD CREATE REMOTE THREAD LOAD REMOTE IMAGE	tpid
TargetImage	string	OPEN PROCESS CREATE REMOTE THREAD LOAD REMOTE IMAGE	tpath (с буквой диска)
NewThreadId	uint	CREATE REMOTE THREAD OPEN THREAD	tid
StartAddress	uint	CREATE REMOTE THREAD	taddr
GrantedAccess	uint	OPEN PROCESS OPEN THREAD	grnt
TargetFilename, Device	string	CREATE NEW RENAME DELETE ACCESS	name (с буквой диска)
Archived	bool	DELETE RENAME	save
TargetObject	string	SET VALUE RENAME KEY DELETE KEY CREATE KEY	*
Details	string	SET VALUE	*
NewName	string	RENAME KEY	new

* поля являются виртуальными (соответствующие поля нативной модели данных событий отсутствуют).

Некоторые поля схемы sysmon являются виртуальными – соответствующие поля нативной схемы событий для них отсутствуют. Например, поле TargetObject в событиях реестра агента EDR для Windows.

Данное поле сочетает в себе и имя ключа и имя значения в реестре, в то время как в нативной схеме событий есть отдельное поле key (имя ключа) и отдельное поле val_n (имя значения). Другой пример – поле Details. Данное поле включает в себе определенным образом отформатированные тип и значение ключа реестра, например, «DWORD (0x00000002)».

Значения полей схемы sysmon, обозначающих имена файлов, в агенте EDR для Windows форматируются с использованием буквы диска, в то время как в нативной схеме событий используется формат имен диспетчера объектов Windows NT – Device\HarddiskVolume1\ и т.п.

Следует также отметить, что поле CallTrace схемы sysmon имеет иной формат по сравнению с полем trace нативной схемы событий и доступно не во всех категориях событий (в отличие от trace).

При написании условий индикаторов атак для RT Protect EDR с использованием в условии поля trace (стэк вызовов) нужно иметь в виду следующее. Формат поля trace – это последовательность строк (полных путем с именем модуля), где в качестве разделителя используется символ | (вертикальная черта). Для минимизации представления пути кодируются таким образом, что их известные префиксы заменяются специальными компактными последовательностями символов. Например, префикс \Device\HarddiskVolume1\Windows\system32\ заменяется на *1\, поэтому условие trace.lower matches «*\\windows\\system32\\spool\\drivers*» не сработает. Нужно стараться исключать известные префиксы при матчинге путей. К примеру, trace.lower matches «*\\spool\\drivers*» в данном случае отработает корректно.

Секвентальные индикаторы атак

Секвентальные ИА позволяют учесть в условии срабатывания одного индикатора факт срабатывания другого индикатора в определенном контексте. Это, в свою очередь, позволяет составлять сложные условия срабатывания, включающие в себя несколько разнотипных событий, происходящих с течением времени. Например, «установка сетевого соединения с предшествующим в диапазоне 5 секунд выполнением команды создания пользователя».

Для реализации секвентальных ИА предназначены виртуальные поля history, hive_history и sys_history, которые можно задействовать при написании условия секвентальных ИА. Данные поля являются виртуальными, поскольку физически отсутствуют в событиях и вычисляются агентом в момент вычисление условия ИА.

В history сохраняются обнаружения, зафиксированные в рамках процесса, в hive_history – в рамках группы процессов, в которую входит процесс, где возникло обнаружение, а в sys_history отмечаются обнаружения глобально для всей системы. Таким образом, если имеется следующая цепочка процессов: malware.exe, который запускает cmd.exe и pwsh.exe, который, в свою очередь, запускает net.exe, то

обнаружения отдельных процессов будут сохраняться в их истории history, также эти же обнаружения будут сохранены в общей истории hive_history всей группы процессов (malware.exe, cmd.exe, pwsh.exe, net.exe), и в глобальной истории sys_history срабатывания обнаружений всей системы, соответственно.

Обнаружения идентифицируются по имени. С каждым обнаружением связано время его последнего возникновения. При написании условия секвентального ИА для проверки наличия обнаружения в истории предназначен оператор contains, который возвращает булевский признак наличия искомого обнаружения в истории, а для получения времени последнего срабатывания обнаружения в истории используется оператор lookup, который возвращает время последнего срабатывания искомого обнаружения в истории или константу time_nil, если запрашиваемое обнаружение никогда не срабатывало. Полученное время из абсолютного формата в относительный можно перевести вычитанием его из текущего времени time_now. После чего можно обратиться к полям time_span_millis, time_span_sec или time_span_min полученной дельты времени, чтобы перевести ее в количество миллисекунд, секунд или минут, соответственно, и далее задействовать в условии ИА. Если искомого обнаружения в истории нет, то lookup вернет константу time_nil («пустое» время). Если ее вычесть из time_now, то в результате будет опять же time_now. Поэтому, если в условии, к примеру, написано (time_now - time_nil).time_span_sec <= 3, то это условие никогда не выполнится, поскольку текущее время в абсолютном выражении в секундах будет всегда больше 3 (или любых других логически обоснованных значений). Т.е. можно не заботиться о дополнительных проверках при написании lookup. На рисунке 34 представлен пример секвентального индикатора атак.

```
(host == "malware.com" or r_ip == "66.66.66.66") and
hive_history contains "dump_ntds" and
hive_history contains "run_net" and
(hive_history contains "run_pwsh_encoded_command" or hive_history contains "run_cmd_pipe_out") and
(time_now - sys_history lookup "some_WmiPrvSE_suspicious_activity").time_span_sec <= 5

```

Рисунок 34 – Секвентальный индикатор атак

Рекомендации по написанию индикаторов атак

Рекомендации при написании индикаторов атак следующие.

Если ИА соответствует известному sigma-правилу, то рекомендуется использование имени этого sigma-правила в качестве имени индикатора (например, proc_creation_win_powershell_download_patterns).

Для некоторых ИА допускается только детектирующее действие, это относится к таким типам индикаторов, как, например, **Завершение процесса** или «**Открытие локального порта на прием (LISTEN)** – где блокирующее действие неуместно или не реализовано технически.

Блокирующее действие индикатора типа **Загрузка образа** может иметь глобальный эффект для всех процессов системы, в которые загружается образ – такова техническая реализация блокировки. Поэтому желательно однозначно идентифицировать блокируемые библиотеки при создании индикаторов, а также предварительно тестировать правило в режиме детектирования.

Для всех типов ИА блокирующее действие, если оно происходит в контексте системного процесса или его компонента, может нарушить работу системы. Особенно, если блокировка произошла незапланированно, из-за того, что правило не протестировано должным образом на широком наборе машин. Для защиты от таких ситуаций введена опция «Блокировка действует и в контексте критических системных процессов». По умолчанию опция выключена и, если правило сработает в контексте критического системного процесса или его компонента, то блокирующее действие будет автоматически переопределено на **Детектирование**. Для ИА типа **Загрузка драйвера** данная опция должна быть выставлена вместе с блокирующим действием, иначе блокировка никогда не сработает, т.к. загрузка драйвера всегда происходит в системном процессе.

Для достижения максимального быстродействия при матчинге индикаторов атак в системе RT Protect EDR необходимо придерживаться следующих рекомендаций при написании условий их срабатывания.

Основное – это логическая структура условия. Матчер использует «ленивый» принцип вычисления, поэтому не будет продолжать вычисление выражения, если его результат уже предопределен. Исходя из этого, необходимо в начало сложных условий, сочетающих в себе многочисленные проверки, выносить простые предусловия. Например, правило (cmdl icontains «some_pattern1» or cmdl icontains «some_pattern2» or cmdl icontains «some_pattern3») and app iendswith «someware.exe» правильно с точки зрения производительности переписать так, чтобы вначале проверялось app, а затем все остальное.

При матчинге индикаторов атак наибольшее быстродействие имеют операторы, работающие с булевскими и числовыми значениями. Чуть медленнее операторы, работающие со строками в case-sensitive режиме. Еще более медленные те, что работают со строками в case-insensitive режиме. Еще более «тяжелыми» являются операции матчинга wildcard- и регулярных выражений – matches и rematches. При использовании

регулярных выражений, как правило, приходится дополнительно использовать спецификатор .lower, что еще немного снижает производительность из-за необходимости конвертации строки в нижний регистр.

К примеру, при прочих равных iendswith отработает быстрее, чем icontains, который в свою очередь опередит по производительности matches.lower.

Создание индикатора атак

В графическом интерфейсе RT Protect EDR правила индикации атак представлены в виде таблицы со сгруппированными наборами индикаторов.

Таблица наборов индикаторов имеет следующие столбцы (рис. 35):

1) Название набора;

2) **Количество записей** (правил в наборе);

3) **Привязано агентов** (количество агентов, которым назначен данный набор правил);

4) **Управление**, в поле содержатся следующие кнопки:

– кнопка редактирования названия набора ;

– кнопка удаления набора ;

– кнопка передачи агентам изменений набора ( ).

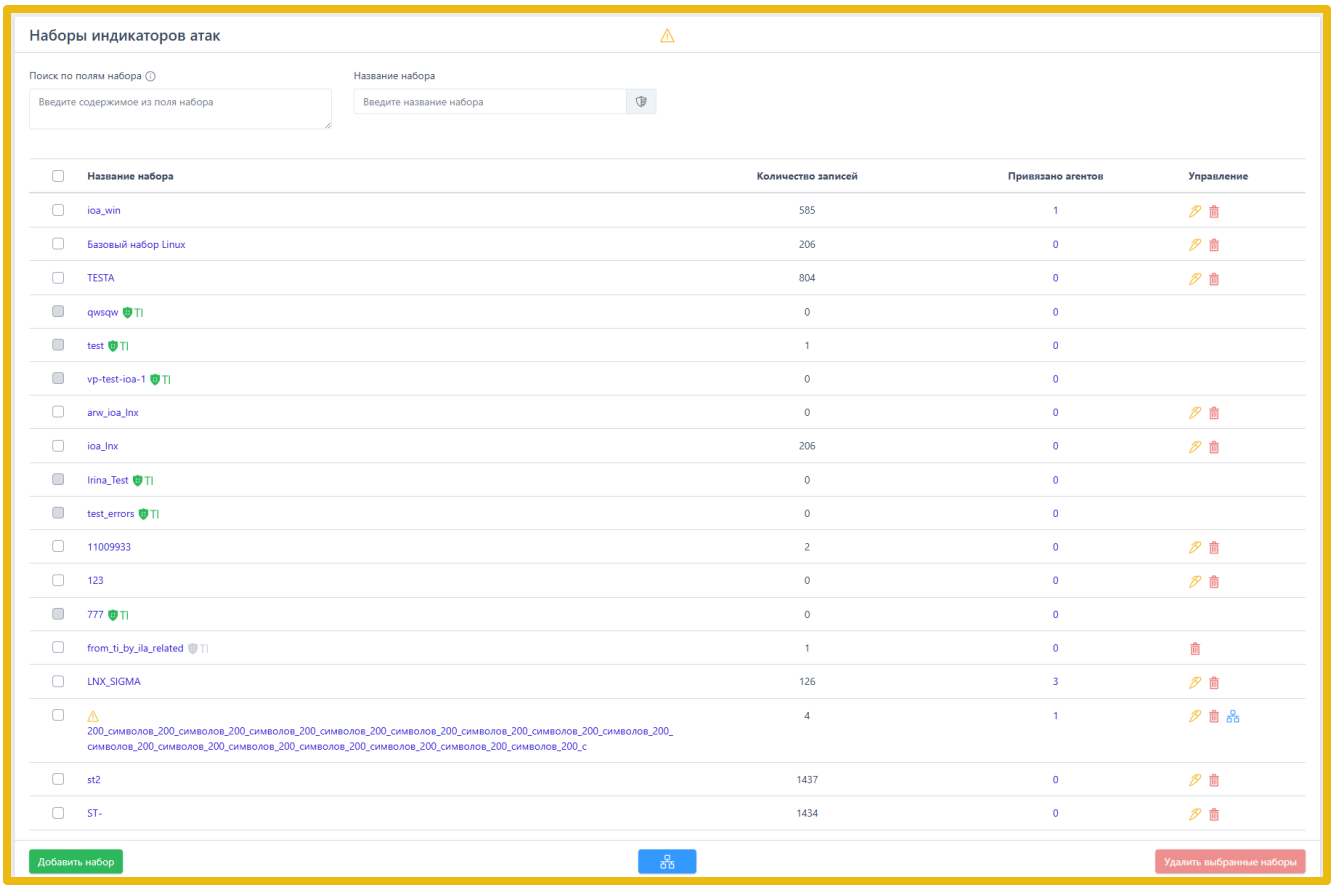


Рисунок 35 – Наборы индикаторов атак

Для поиска по наборам и их содержимому в EDR предусмотрен фильтр **Поиск по полям набора**, при написании запроса фильтр ищет соответствия во всех текстовых полях всех наборов, то есть выполняется сквозной поиск по всем наборам. Поиск по текстовым полям осуществляется без учета регистра.

На странице **Индикаторы атак** имеется возможность добавления/редактирования как самого набора, так и правил, входящих в набор, а также копирование индикатора из одного набора в другой. Правила в наборе представлены в виде таблицы со следующими столбцами (рис. 36):

1) Кнопка выбора (чекбокс);
2) Имя индикатора;
3) Тип индикатора (указывает на тип события);
4) Критичность/Действие, назначенные индикатору;
5) Идентификатор техники матрицы атак MITRE;
6) Дата создания/Автор индикатора;
7) Последнее изменение/Пользователь, внесший последнее изменение в индикатор;

8) Управление (содержит кнопки активации/деактивации индикатора / , а также кнопки **Редактировать** и **Удалить**).

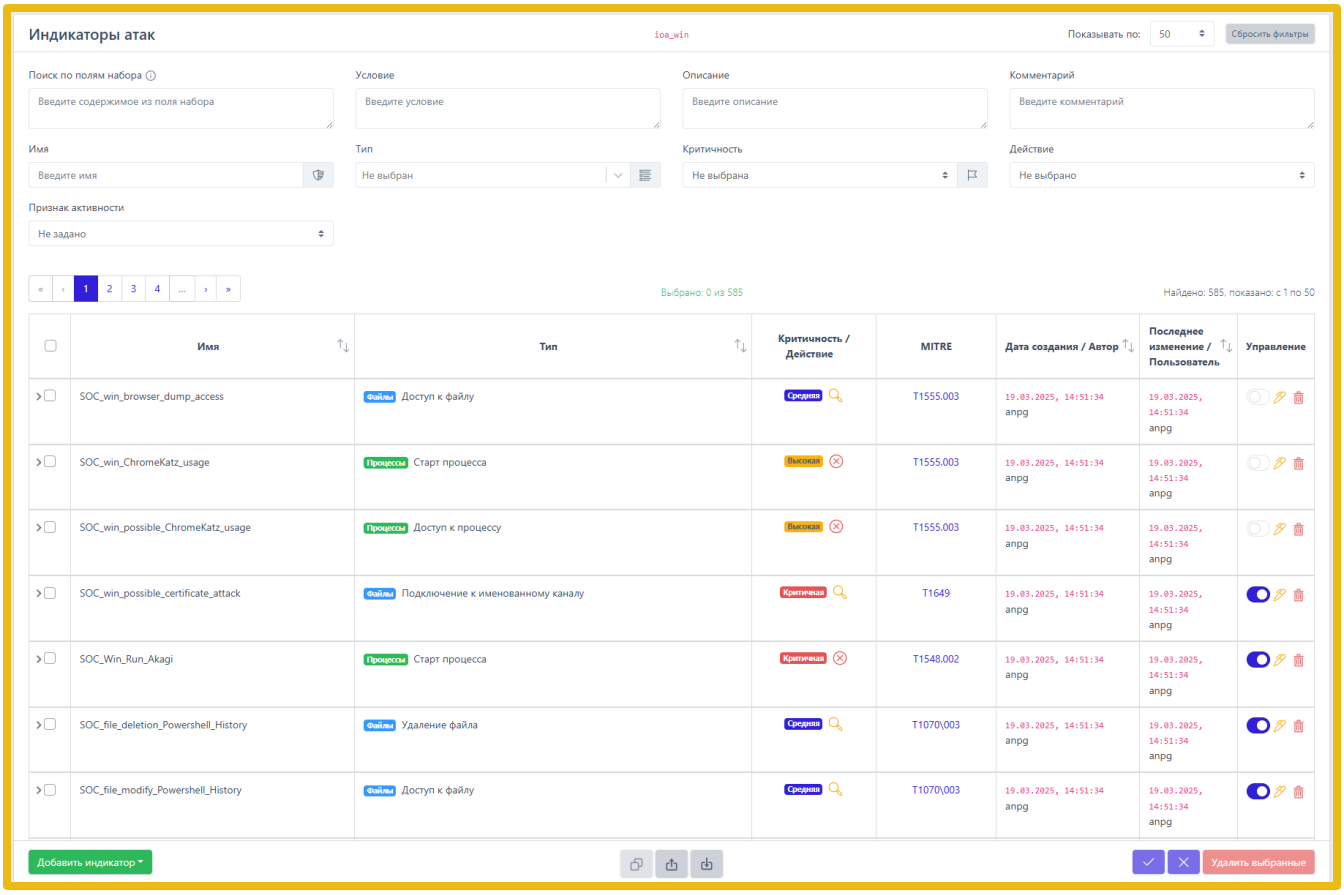


Рисунок 36 – Страница с правилами индикации атак, входящими в набор

Также, как и на странице с наборами, здесь присутствует фильтр поиска по текстовым полям набора, а также фильтры поиска по отдельным полям вместе с уточняющими фильтрами с выпадающими списками.

Рядом с кнопкой выбора содержится значок раскрытия дополнительной информации об индикаторе , который содержит следующие поля (рис. 37):

1) Условие;

2) Описание;

3) Комментарий;

4) Поле с информацией о том, действует ли блокировка в контексте критических системных процессов.

Условие	`key icontains "SOFTWARE\\Classes\\"`
Описание	
Комментарий	
Блокировка действует и в контексте критических системных процессов	Нет

Рисунок 37 – Дополнительная информация об индикаторе атак

Для добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы.

Добавить индикатор можно двумя способами (рисунок 38):

1) Создать новый индикатор;

2) Импортировать индикатор из sigma-правила.

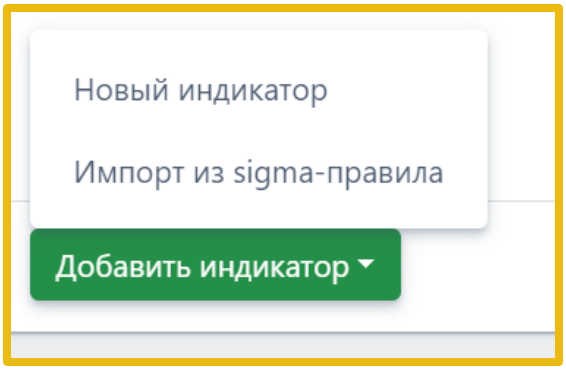


Рисунок 38 – Окно выбора способа добавления индикатора атаки

При выборе способа Новый индикатор откроется окно Добавить индикатор.

В открывшемся окне **Добавить индикатор** (рис. 39) следует прописать условия, на основании которых будет срабатывать правило.

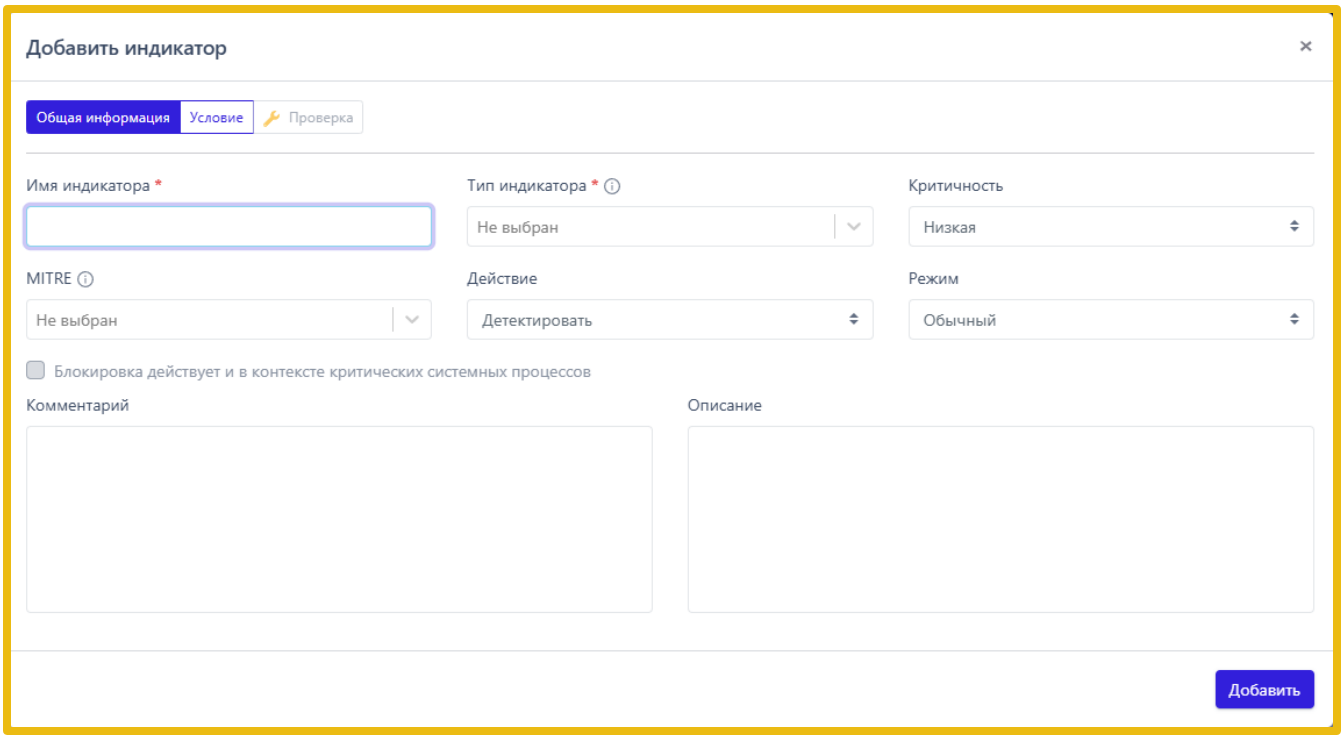


Рисунок 39 – Добавление индикатора

В окне **Добавить индикатор** имеются поля, отмеченные символом * . Этот символ означает, что при добавлении индикатора поля не могут быть пустыми. При попытке добавления индикатора с незаполненными полями индикатор не будет добавлен, а незаполненные поля будут выделены красной рамкой.

Важно

Имя индикатора атак не должно превышать 200 символов (байтов), запись в поле **MITRE** не должна превышать 255 символов (байтов).

При создании индикатора атаки в ОС Windows для всех типов индикаторов, кроме типа **Старт процесса**, возможно написать такой индикатор, при срабатывании которого будет блокироваться критический системный процесс, что крайне опасно и может привести к блокировке всей работы и установке ОС в состояние «Синего экрана».

При установке галочки в поле **Блокировка действует и в контексте критического системного процесса** аналитик должен осознавать, что он соглашается с тем, что описанное выше состояние допустимо и может произойти на хосте, для которого будет применяться данный индикатор.

Для ОС Windows критическими системными считаются следующие процессы:

1) Процесс System (ядро ОС);

2) Процесс с ненулевым уровнем защиты (PPL, Windows 8.1+);

3) Trustlet-процесс Windows 10+ (https://learn.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes)

4) Процессы: csrss.exe, smss.exe, lsass.exe, services.exe, wininit.exe, winlogon.exe, logonui.exe, lsm.exe, sppsvc.exe (идентифицируются по полному пути);

5) Библиотека lsm.dll (идентифицируется по полному пути) внутри хост-процесса (svchost.exe).

Заполнение поля **Условие** можно выполнить двумя способами:

– ручной ввод условия;

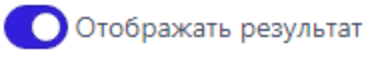
– ввод условия с помощью конструктора.

Переключение между способами осуществляется с помощью кнопок **Ручной ввод** и **Конструктор** (

). Выбранный способ написания условия подсвечивается синим цветом.

Важно

Записи в полях **Условие, Описание** и **Комментарий** не должны превышать 32 тысячи 767 символов (байтов).

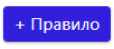
Для удобства при написании условия можно использовать кнопку 

. При включении кнопки условие отображается в нижней части конструктора. Это позволяет аналитику детально рассмотреть приоритеты в условии, после чего скорректировать его, если это необходимо.

В конструкторе возможно создавать правила с использованием модели данных Sysmon. Полный список операторов представлен в разделе **Состав операторов**

Поле для ввода значений позволяет вводить произвольные значения для событий из схемы данных Sysmon.

Поле выбора значения логического оператора позволяет выбрать из двух значений AND (И), OR (ИЛИ).



– кнопка для добавления строчки правила.

! – кнопка для добавления отрицания группы.

+ Группа – кнопка для добавления группы правил в условии.

При выборе способа добавления индикатора **Импорт из sigma-правила**, открывается окно, представленное на рисунке 40.

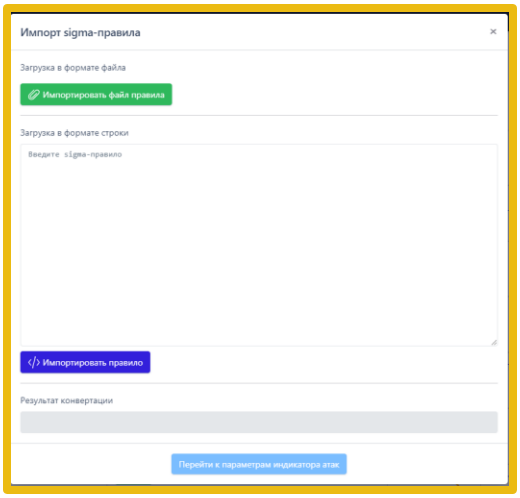


Рисунок 40 – Окно добавления индикатора с помощью импорта из sigma-правила

Sigma-правило, на основании которого будет создан индикатор атак, может быть добавлено в формате файла, либо в формате строки.

Для создания индикатора на основе Sigma-правила следует перейти на сайт https://github.com/SigmaHQ/sigma/tree/master/rules/windows и, выбрав одно из правил, нажать по иконке </> Импортировать правило (рис. 41).

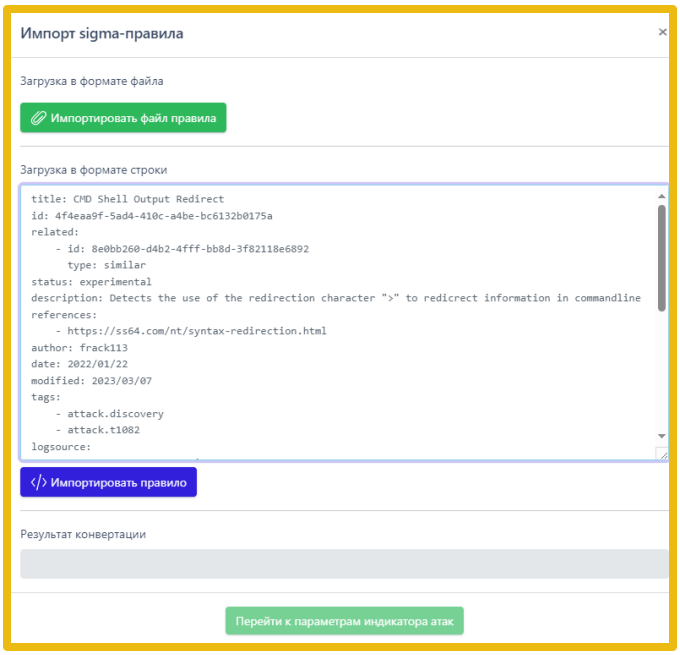


Рисунок 41 – Импорт Sigma-правила с помощью загрузки в формате строки для создания индикатора атаки

При удачной конвертации правила в поле **Результат конвертации** появится запись **Успешная конвертация**. Далее для редактирования индикатора на основе sigma-правила следует нажать по иконке Перейти к параметрам индикатора атак. Откроется окно **Добавить индикатор** с информацией из того sigma-правила, на основании которого создан индикатор. Дальнейшие действия по редактированию и сохранению индикатора атак аналогичны действиям, описанным в этом разделе выше.

Кроме описанной выше процедуры можно воспользоваться импортом yml-файла с правилом, скачав его по ссылке с sigma-правилами и загрузив в формате файла с помощью кнопки Импортировать файл правила.

Проверка условия индикатора атаки

Условия индикатора проверяются с помощью утилиты **Проверка синтаксиса**. Область с информацией по проверке условия отображается в нижней части окна **Добавить индикатор** во вкладке **Условие**. Проверка запускается перед добавлением индикатора или после нажатия кнопки </>. В случае написания некорректного условия индикатора атаки поле ввода будет подсвечено рамкой красного цвета. Если условие не содержит ошибок, то поле ввода подсвечивается рамкой зеленого цвета.

Редактирование и удаление индикатора атаки

Для редактирования индикатора необходимо нажать кнопку **Редактировать** в строке выбранного индикатора атаки и в открывшемся окне **Редактировать индикатор** внести необходимые изменения.

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении индикатора. Редактировать индикатор можно только в ручном режиме, при переключении на режим конструктора условие индикатора будет полностью изменено.

Для удаления индикатора атаки необходимо выбрать его с помощью кнопки выбора, установив флажок, после чего нажать кнопку **Удалить выбранные**. Для завершения операции ее необходимо подтвердить в открывшемся окне **Подтверждение действия**.

Ретроспективный анализ индикаторов атак

Ретроспективный анализ правила позволяет проверять срабатывания вновь создаваемых правил на массиве событий телеметрии, сохраненных в системе. Ретроанализатор позволяет проверить индикатор и понять, к чему приведет его создание, сколько сработок будет сгенерировано.

Подразумевается, что значительное количество срабатываний правила будет говорить о том, что оно нуждается в доработке.

Ретроспективный анализ индикаторов атак доступен во вкладке **Проверка** на страницах **Редактировать индикатор** и **Добавить индикатор.** Для того, чтобы проверить правило, необходимо выбрать период проверки и нажать кнопку **Запустить проверку.** В случае, если будет достигнуто 500 и более срабатываний правила, проверка будет приостановлена, так как считается, что такое количество срабатываний свидетельствует о необходимости редактирования правила.

11.10.2. Индикаторы компрометации

Индикаторы компрометации (IOC в международной терминологии или ИК в терминологии Программы) – это артефакты известной вредоносной активности.

Артефакты разделены по типам:

– имя файла (поддерживаются также имена именованных каналов Windows);

Примечание

Под именем файла подразумевается абсолютное имя файла, базовое имя или имя файла, написанное с помощью регулярного выражения, например, *file.txt.

– хеш-суммы, рассчитанные по алгоритмам SHA-256 (SHA-1, MD5 будут отслеживаться, если включена соответствующая настройка в профиле безопасности агента);

– IP-адрес;

– доменное имя;

– URL (на данный момент под URL подразумевается доменное имя и порт);

– сетевая сигнатура.

Важно

Сетевой артефакт – записи IP-адресов и доменных имен не должны превышать 255 символов (байтов), сетевых сигнатур 1023 символа (байта), URL 32 тысячи 767 символов (байтов).

С каждым индикатором связано действие, которое необходимо предпринять в отношении него – «Детектировать» или «Блокировать». Детектирование подразумевает генерацию события, в котором указывается сработавший индикатор компрометации, при этом в Программе будет создан инцидент.

Сетевые и файловые ИК объединяются по полю **rul**, то есть при изменении правила ( ), в рамках сессии браузера индикаторы компрометации будут объединяться по этому правилу. Например, у нас есть правило, в котором мы детектируем ИК-домен, после его изменения на любой другой домен в рамках одной сессии мы получим объединение сработок в один инцидент. Кроме того, в Программе создаются кроссагентские инциденты, когда, например, все агенты защищаемой инфраструктуры обращаются к одному вредоносному домену (будет сформирован один инцидент).

Важно

Более специфичная запись сетевого индикатора компрометации (более длинное доменное имя, комбинация с портом) имеет приоритет над менее специфичной.

Работа со списком ИК обеспечивается посредством конфигурационного файла, доступного для просмотра и редактирования из графического интерфейса.

В графическом интерфейсе индикаторы компрометации представлены в виде таблицы с наборами.

Таблица наборов индикаторов имеет следующие столбцы:

– Название набора;

– Количество записей (правил в наборе);

– Привязано агентов (количество агентов, которым назначен данный набор правил);

– Управление.

Имеется возможность добавления/редактирования как самого набора, так и правил, входящих в набор, а также копирование индикатора из одного набора в другой, сохранение правил индикации (экспорт) с последующим импортом.

Правила в наборе представлены в виде таблицы со следующими столбцами:

– Имя индикатора;

– Тип артефакта;

– Артефакт;

– Действие;

– Комментарий;

– Дата создания/Автор;

– Последнее изменение/Пользователь;

– Управление.

В таблице наборов имеется набор с индикаторами, установленными по умолчанию.

Пример таблицы одного из наборов ИК представлен на рисунке 42.

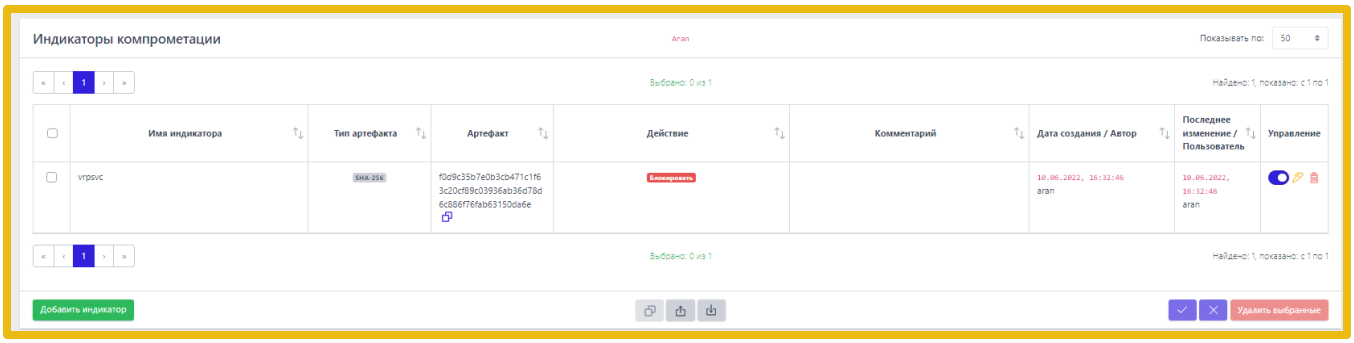


Рисунок 42 – Индикаторы компрометации

ИК, обрабатываемые Программой, подразделяются на сетевые и файловые. Особенностью работы с файловыми индикаторами является то, что все файлы, находящиеся на конечных точках с установленным на них агентом, проверяются по имени файла или по хешам, если выполнены условия, описанные ниже.

Важно

Файловые индикаторы компрометации (кроме индикаторов по имени файла (поле **name**)), работают только для исполняемых файлов и файлов с активным содержимым. Исполняемые файлы анализируются по содержимому в момент запуска (файлы типа EXE, DLL, SYS, COM, OCX, SCR, CPL), а файлы с активным содержимым анализируются по расширению в момент доступа к файлу. Соответствующие расширения файлов с активным содержимым должны быть указаны в профиле безопасности агента (например, PDF, PS1, PSM1, CMD и т.д. Исполняемые файлы проверяются Программой по умолчанию.

При обращении к файлу, хеш-сумма которого совпадает с хеш-суммой, указанной в индикаторе компрометации, обращение блокируется, а в модуле администрирования формируется (или дополняется) инцидент, объединяющий в себе все события, соответствующие индикатору. Эти события могут иметь разный тип в зависимости от выполняемой операции: открытие файла, чтение, удаление, а также могут относиться к разным процессам в системе. Блокируются все операции с файлом, изолируя его "по месту", без перемещения в карантин. Запуск исполняемого файла, хеш которого присутствует в перечне индикаторов компрометации, будет блокироваться монитором файловой системы на самом раннем этапе запуска, когда системный объект **процесс** для него еще не сформирован.

Важно

Если в профиле безопасности агента установлен режим «только детектирование», то действие «блокировать» для индикаторов компрометации, применяемых на агенте, будет переопределено на действие «детектировать».

На странице **Наборы индикаторов компрометации** в разделе **Индикаторы компрометации** содержится информация об объектах (или артефактах), которые являются источником компрометации.

Обнаружение событий, связанных с описанными в наборах компрометации артефактами, вызывает определенное действие, зафиксированное в наборе. Таким действием может быть блокирование или детектирование вызываемого артефактом процесса.

Информация на странице представлена в табличном виде. Если присутствует хотя бы один несохраненный набор индикаторов компрометации, то в верхней части таблицы появится значок предупреждения .

В шапке таблицы представлены следующие поля:

– кнопка выбора (отмечена элементом);

– Название набора;

– Количество записей;

– Привязано агентов;

– Управление.

Название набора – в поле отображается название набора индикаторов компрометации, при нажатии ЛКМ на название набора происходит переход на страницу изменения набора.

Количество записей – в поле отображается количество индикаторов, сохраненных в наборе.

Привязано агентов – в поле отображается количество привязанных к набору агентов. При нажатии ЛКМ на число агентов происходит переход к странице **Агенты**, на которой в таблице будут показаны привязанные к набору агенты.

Управление – в поле отображаются кнопки операций с набором индикаторов компрометации: **Редактировать** ( ), **Удалить** ( ) и **Передать набор** ( ).

Редактировать – при нажатии кнопки открывается окно **Редактировать набор**. В поле **Имя** отображается название набора, для его изменения необходимо ввести в строке с именем набора новое имя и нажать кнопку Сохранить.

Передать набор – кнопка отображается в поле **Управление** при условии, что изменения в наборе индикаторов компрометации не были переданы агентам, привязанным к этому набору.

Также, как и на странице **Индикаторы атак**, на страницах **Наборы индикаторов компрометации** и **Индикаторы компрометации** пользователь может выполнить сквозной поиск по текстовым полям всех индикаторов компрометации. Поиск по полям набора осуществляется без учета регистра в полях **Имя индикатора**, **Артефакт**, **Комментарий**.

В нижней части страницы находятся кнопки Добавить набор и Удалить выбранные наборы. Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Добавить набор** в строке **Имя** ввести название нового набора.

Если к новому набору требуется добавить индикаторы из наборов, созданных и сохраненных в Программе ранее, то в поле **Базовый набор** необходимо выбрать из выпадающего списка набор, который станет основой для нового набора.

Добавление базового набора является опциональным условием. Если в окне **Добавить набор** не ввести значение имени нового набора, то кнопка **Добавить** не будет активна.

Для удаления одного или нескольких наборов индикаторов компрометации необходимо отметить флажками соответствующие им кнопки выбора, после чего нажать кнопку **Удалить выбранные наборы.**

Переход на страницу с таблицей **Индикаторы компрометации** происходит при нажатии ЛКМ на названии набора в таблице **Наборы индикаторов компрометации**.

В области **Индикаторы компрометации** аналитик может:

– просматривать информацию об индикаторах, входящих в выбранный набор;

– изменять индикаторы компрометации, входящие в выбранный набор;

– экспортировать индикаторы в файлы различных форматов;

– импортировать данные из файла в набор индикаторов;

– копировать индикаторы выбранного набора в другие наборы индикаторов компрометации;

– сохранять набор с добавленными индикаторами компрометации;

– удалять из набора выбранные ИК.

– активировать/деактивировать выбранные ИК.

После добавления или изменения индикаторов слева от названия набора появится значок ⚠ с предупреждающим сообщением **Набор не применен**. Сообщение появляется при наведении курсора мыши на предупреждающий значок.

Шапка таблицы с индикаторами содержит следующие поля:

1) Кнопка выбора (отмечена элементом ▢);

2) Имя индикатора;

3) Тип артефакта;

4) Артефакт;

5) Действие;

6) Комментарий;

7) Дата создания/Автор;

8) Последнее изменение/Пользователь;

9) Управление.

Имя индикатора – поле содержит произвольное название индикатора, заданное пользователем. Поле поддерживает работу с сочетаниями клавиш Ctrl+V, Ctrl+Z, Ctrl+Y, Ctrl+X, Ctrl+A.

Тип артефакта – поле содержит тип объекта, являющегося индикатором компрометации. Каждый индикатор компрометации основывается на определенном типе артефакта. Тип артефакта задается при создании или изменении индикатора компрометации. В Программе предусмотрено несколько типов артефактов:

1) **Имя файла** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано имя файла, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

2) **SHA-256** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму sha-256, для объекта, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

3) **SHA-1** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму sha-1, для объекта, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

4) **MD5** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму MD5, для объекта, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;



Важно

Чтобы выполнялись проверки по SHA-1 и MD5 в профиле безопасности агента должны быть включены соответствующие опции.

5) **IP-адрес** – в качестве индикатора компрометации в поле **Артефакт** будет выбран IP-адрес сетевого соединения, при взаимодействии с которым Программа создаст инцидент и выполнит предусмотренное действие;

6) **Доменное имя** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано имя домена, при взаимодействии с которым Программа создаст инцидент и выполнит предусмотренное действие;



Важно

Домен и IP-адрес могут быть написаны в индикаторе вместе с портом (<IP/домен>:<порт>).

7) **URL** – в качестве индикатора компрометации будет выбран унифицированный указатель ресурса в сети Интернет;



Важно

Тип артефакта **URL** на данный момент не поддерживается агентом.

8) **Сетевая сигнатура** – в качестве индикатора компрометации в поле **Артефакт** будет выбрана сетевая сигнатура, при обнаружении которой система создаст инцидент и выполнит предусмотренное действие (под сетевой сигнатурой подразумеваются сигнатуры в формате Snort).



Важно

В UDP и ICMP сетевые сигнатуры работают только в режиме детектирования (DETECT).

Артефакт – в поле отображается наименование артефакта. Название артефакта должно соответствовать выбранному типу артефакта. Если указать тип артефакта **Доменное имя**, то название артефакта должно соответствовать правилам написания доменных имен, к примеру, **example.com**. Дополнительно поле содержит элемент , позволяющий скопировать в буфер обмена имя артефакта. Поле **Артефакт** поддерживает работу с сочетаниями клавиш Ctrl+V, Ctrl+Z, Ctrl+Y, Ctrl+X, Ctrl+A.

Действие – в поле отображается действие, которое должна осуществить Программа при обнаружении события, связанного с выбранным индикатором компрометации.

В качестве ответа на вредоносную или потенциально вредоносную активность в Программе предусмотрены следующие действия для индикаторов компрометации:

1) Блокировать – в этом случае активность будет запрещена;

2) Детектировать – в этом случае активность будет разрешена, но Программа уведомит пользователя об обнаружении детектируемого события, создав инцидент.

Комментарий – в поле отображается произвольный комментарий к выбранному индикатору компрометации. Поле **Комментарий** заполняется при необходимости во время редактирования или добавления нового индикатора. Поле **Комментарий** поддерживает работу с сочетаниями клавиш Ctrl+V, Ctrl+Z, Ctrl+Y, Ctrl+X, Ctrl+A.



Важно

Запись в поле **Комментарий** не должна превышать 32 тысячи 767 символов (байтов).

Дата создания/Автор – в поле отображается имя пользователя, создавшего индикатор компрометации, и время его создания.

Последнее изменение/Пользователь – в поле отображается время последнего изменения индикатора и имя пользователя, внесшего изменение.

Управление – в поле отображаются кнопки активировать/деактивировать (/) индикатор компрометации, **Редактировать** и **Удалить** .

Для редактирования индикатора компрометации необходимо нажать кнопку **Редактировать**. В открывшемся окне **Редактировать индикатор** необходимо изменить одно или несколько полей, требующих изменения или корректировки, и нажать кнопку **Сохранить.**

Поля формы **Редактировать индикатор** идентичны полям шапки таблицы индикаторов, описанным выше.

Для удаления индикатора компрометации необходимо нажать кнопку **Удалить** .

В нижней части таблицы находятся кнопки операций с индикаторами:

1) Добавить индикатор;
2) Передать набор агентам – ;
3) Копировать выбранные элементы в другой набор – ;
4) Экспортировать набор в файл – ;
5) Импортировать данные из файла в набор (поддерживаемые форматы: csv, json) – ;
6) Активировать выбранный элемент (группу элементов) – ;
7) Деактивировать выбранный элемент (группу элементов) – .

Для добавления индикатора в области **Индикаторы компрометации** необходимо нажать кнопку Добавить индикатор. Далее в открывшемся окне **Добавить индикатор** необходимо заполнить представленные поля и нажать кнопку Добавить (рис. 43).

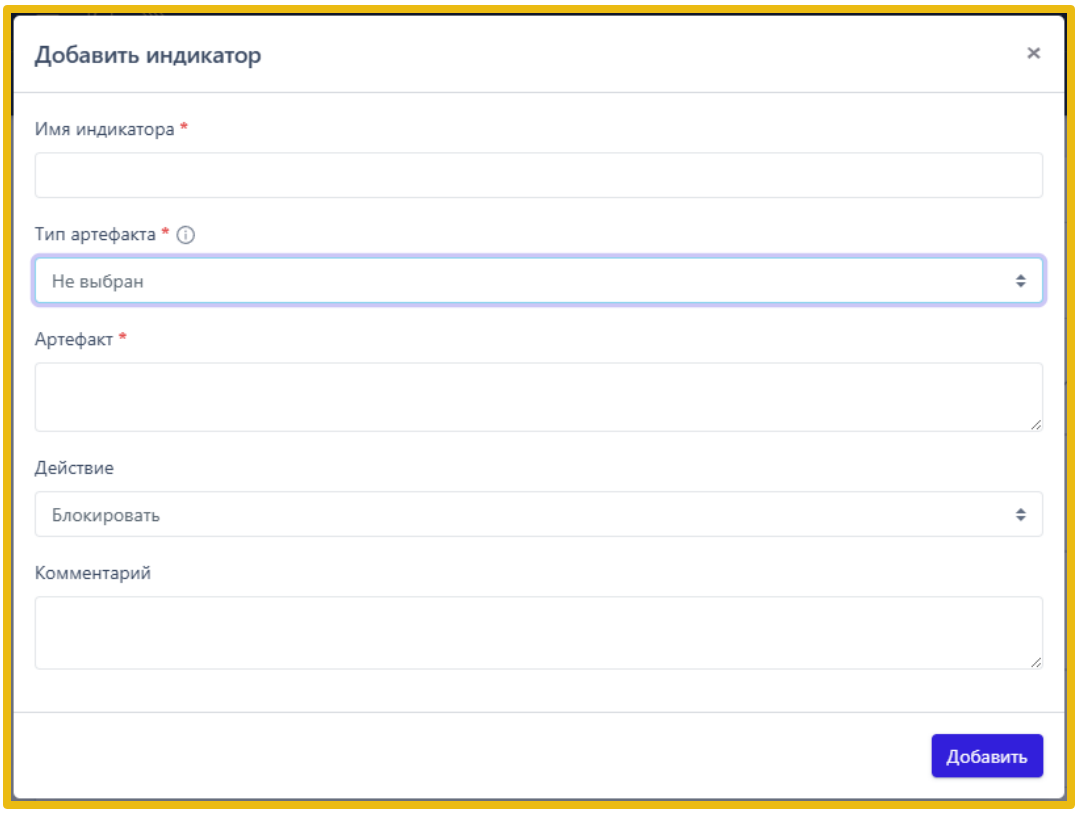


Рисунок 43 – Окно «Добавить индикатор»

Файловые индикаторы компрометации (типы артефакта **Файл**, **SHA-256**, **SHA-1** и **MD5**) содержат флаг **Блокировка действует и в контексте критических системных процессов**. При создании индикатора компрометации в ОС Windows, возможно написать такой индикатор, при срабатывании которого будет блокироваться критический системный процесс, что крайне опасно и может привести к блокировке всей работы и установке ОС в состояние «Синего экрана». При установке галочки в поле **Блокировка действует и в контексте критического системного процесса** аналитик должен осознавать, что он соглашается с тем, что описанное выше состояние допустимо и может произойти на хосте, для которого будет применяться данный индикатор.

Для ОС Windows критическими системными считаются следующие процессы:

1) Процесс System (ядро ОС);

2) Процесс с ненулевым уровнем защиты (PPL, Windows 8.1+);

3) Trustlet-процесс Windows 10+ (https://learn.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes)

4) Процессы: csrss.exe, smss.exe, lsass.exe, services.exe, wininit.exe, winlogon.exe, logonui.exe, lsm.exe, sppsvc.exe (идентифицируются по полному пути);

5) Библиотека lsm.dll (идентифицируется по полному пути) внутри хост-процесса (svchost.exe).

Важно

Если задано действие **Блокировать**, но опция **Блокировка действует и в контексте критических системных процессов** не установлена, то монитор файловой системы будет переопределять действие на **Детектировать** в контексте системного процесса (или компонента).

Для передачи изменений в наборах индикаторов агентам необходимо нажать кнопку **Передать набор агентам** (). Кнопка не будет отображаться на странице до внесения очередных изменений в набор.

Для копирования индикаторов из одного набора в другой необходимо отметить флажками кнопки выбора для индикатора или индикаторов, которые нужно скопировать в другой набор. После выбора индикаторов следует нажать кнопку **Копировать выбранные элементы в другой набор**  .

В открывшемся окне **Выбор набора** необходимо в поле **Набор** выбрать из выпадающего списка набор индикаторов компрометации. В этот набор будут скопированы выбранные ранее индикаторы. Для завершения операции нужно нажать кнопку  . Для отмены операции необходимо нажать кнопку или кнопку закрытия окна .

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл**  . Далее в открывшемся списке форматов файла необходимо выбрать формат, в котором будут сохранены данные из набора. После выбора формата созданный файл в указанном формате будет сохранен в папку, в которую настроена загрузка файлов в операционной системе.

Для импорта данных из файла с индикаторами необходимо нажать кнопку  (**Импортировать данные из файла в набор, поддерживаемые форматы: csv, json**). После нажатия кнопки открывается окно проводника, в котором необходимо выбрать импортируемый файл, после чего импортировать данные из файла в выбранный набор индикаторов компрометации. После завершения операции импорта индикаторы компрометации из импортируемого файла добавятся в выбранный набор.

Для временной активации/деактивации одного или нескольких индикаторов можно воспользоваться кнопками  , предварительно отметив элемент или группу элементов флагом.

Появится окно подтверждения активации либо деактивации. Для подтверждения действий следует нажать кнопку **Выполнить**. После выполнения операций появятся всплывающие окна, а в таблице индикаторов в столбце **Последнее изменение/Пользователь** будут отображаться дата, время и имя пользователя, производившего действия.

11.10.3. YARA-правила

YARA – это движок поиска по сигнатурам. Вы пишете правило вида «если в файле/памяти встречается такая-то строка, такой-то набор байтов и при этом выполняется условие X — это вредонос Y». RT Protect EDR использует YARA в двух сценариях: проверка файлов и проверка памяти процессов. Это два независимых механизма с разными наборами правил.

В веб-консоли есть два типа объектов:

YARA-наборы для файлов — применяются автоматически ко всем файлам, к которым обращаются процессы.

YARA-наборы для памяти — применяются по команде пользователя (memscan) при сканировании памяти конкретного процесса.

YARA-правила (файлы)

YARA-правила для файлов – это программные элементы, позволяющие определить сигнатуры файлов, которые Программа в случае их обнаружения в защищаемой инфраструктуре отметит как вредоносные.

YARA-правила, как и индикаторы компрометации по хешу, по умолчанию применяются только к исполняемым файлам (PE), к другим файлам могут применяться только после добавления соответствующих расширений в профиле безопасности агента. Матчинг PE-файлов по сохраненным в Программе YARA-правилам возможен только при запуске таких файлов. Под запуском PE-файлов подразумевается исполнение программ, загрузка динамических библиотек (или драйверов) для исполнения их кода. В случае с файлами с потенциально активным содержимым, если соответствующие расширения указаны в профиле безопасности агента (например, файлы с расширениями pdf, ps1, psm1 и т.д.), анализ по YARA-правилам выполняется при любом открытии документов или скриптов, когда осуществляется доступ к их содержимому.

Кроме того, в RT Protect EDR осуществляется отложенное сканирование файлов. Отложенное сканирование работает не для всех файлов, а только для тех, которые обозначены в профиле безопасности, как файлы с потенциально активным содержимым (ps1, docm, xlsm, pdf и т.д.). Отложенное сканирование осуществляется для всех файлов, появляющихся на диске: скачанные из браузера, сохраненные из почты, распакованные из архива, скопированные с флэш-носителя. При этом существует лимит очереди, в которую попадают такие файлы, лимит ограничен 1000 файлов, поэтому при распаковке архива с большим количеством скриптов (больше 1000), часть файлов будет убрана из очереди и не пройдет проверку. Если при отложенной проверке обнаруживается вредонос, то в инциденте будет указан процесс, создавший файл, например, если файл был скачан браузером, то этот браузер и отобразится в инциденте в поле **Процесс**.



Важно

В YARA-правилах в секции **meta** есть поля **severity** и **action**, которые поддерживаются Программой. Аналитик может задавать критичность YARA-правила (normal, guarded, elevated, high или severe, что означает в терминах Программы **Информация**, **Низкая**, **Средняя**, **Высокая** или **Критичная** критичность) и действие, которое будет выполнено при срабатывании (**block** или **detect,** что означает **Блокировать** или **Детектировать**)

По умолчанию при срабатывании YARA-правила (в случае отстутствия заданной критичности в секции **meta**) формируется обнаружение с критичностью **Критичная**, что в свою очередь приведет к созданию инцидента в Программе (инцидент создается при наличии обнаружения с критичностью **Средняя** и выше).

Необходимо отметить, что исполняемые файлы с доверенной подписью по умолчанию не сканируются при запуске по YARA-правилам.

В Программе предусмотрены YARA-правила в наборе, полученном при установке сервера, а также инструментарий для создания новых правил. Таблица с наборами YARA-правил включает в себя структурные элементы, идентичные элементам таблицы наборов индикаторов компрометации. Подробную информацию об этих элементах и работе с ними можно узнать в пункте 11.10.2.

В таблице с наборами можно фильтровать наборы по именам правил и названиям наборов, причем в фильтре **Имя правила** должны указываться имена правил целиком, только в этом случае будет осуществлен поиск. Имя правила указывается без слова rule.



```
rule ZeuS {
    meta:
        author = "NDA0E"
        yarahub_author_twitter = "@NDA0E"
        date = "2024-09-20"
        description = "Detects ZeuS"
        yarahub_uuid = "5f4ca030-2799-47d0-907a-942f84cff1c7"
        yarahub_license = "CC0 1.0"
        yarahub_rule_matching_tlp = "TLP:WHITE"
        yarahub_rule_sharing_tlp = "TLP:WHITE"
        yarahub_reference_md5 = "5a869577bc8122b96a3c8fdb26c2c10e"
        malpedia_family = "win.zeus"

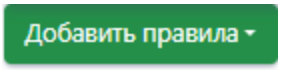
    strings:
        $str1 = "*<input *value=\"" ascii
        $str2 = "*<option  selected" ascii
        $str3 = "*<select" ascii
        $str4 = "Ik{wvAapcgd1)%" ascii

    condition:
        all of them and
        uint16(0) == 0x5a4d
}
```

Рисунок 44 – Имя правила

Поиск по названию набора осуществляется без точного совпадения.

При нажатии ЛКМ на имени набора открывается страница **YARA-правила** для выбранного набора, которая включает в себя следующие кнопки операций:

1) 

– при нажатии кнопки аналитик может выбрать создать ли ему новый файл с YARA правилами или загрузить файлы в набор, при выборе нового файла открывается окно, в котором аналитик может добавить одно или несколько правил, при этом необходимо учитывать, что все имена правил в одном файле должны быть уникальными, в случае нарушения этого правила Программа выдаст ошибку (рис. 45).

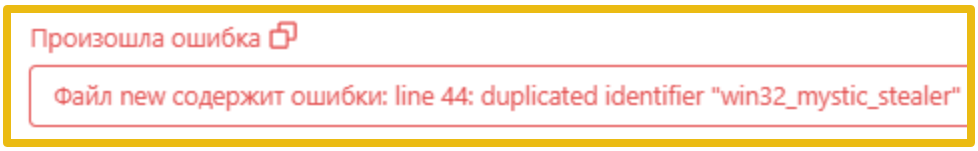


Рисунок 45 – Сообщение о повторяющемся имени правила

Кроме того, если имена YARA-правил будут повторяться в рамках набора (в разных файлах), то при попытке передачи набора агентам будет выведено сообщение об ошибке (рис. 46).

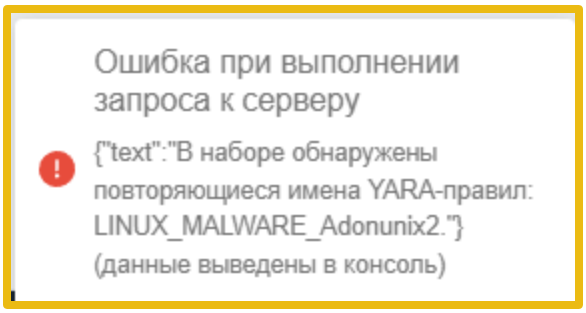


Рисунок 46 – Ошибка при повторяющемся имени правила в наборе

2) Передать набор агентам –  (кнопка отображается, если в файле YARA были изменения, кнопка позволяет применить изменения в наборе для агентов, привязанных к этому набору).

3) Копировать/переместить выбранные элементы в другой набор () – перемещает или копирует выбранный файл или файлы с правилами YARA из одного набора в другой.

4) Экспортировать набор в файл формата JSON –  .

5) Импортировать данные из файла в набор (поддерживаемые форматы: JSON) –  .

6) Активировать YARA-правило –  (все правила, указанные в файле, будут активированы).

7) Деактивировать YARA-правило –  (все правила, указанные в файле, будут деактивированы).

8) Редактировать () – открывает окно редактирования YARA-правил.

9) Удалить () – удаляет файл с YARA-правилами.

Кроме указанных выше кнопок на странице **YARA-правила** в строке с именем файла присутствует значок просмотра (), который позволяет прочесть информацию о YARA-правиле, не заходя в окно редактирования правил.

Для загрузки YARA-файла или нескольких YARA-файлов на сервер с хоста аналитика необходимо выполнить следующие операции:

1) Нажать кнопку **Добавить правила** и выбрать операцию **Загрузить файлы**;

2) В открывшемся окне **Загрузить файлы YARA** нажать кнопку **Выбрать файлы** и в окне Проводника выбрать один или несколько YARA-файлов для загрузки (файлы с расширениями .yar или .yara);

3) Далее нажать кнопку Загрузить файлы на сервер.

Важно

YARA-правила работают на агенте только в том случае, если в профиле безопасности выбранного агента установлен режим глубокого сканирования, включающий в себя YARA-правила, то есть выбраны режимы **YARA-правила** или **ML и YARA-правила**. При этом необходимо учитывать, что режим глубокого сканирования дает повышенную нагрузку на файловый монитор, а значит, и на Программу и ОС в целом.

В одном файле могут быть сотни, тысячи правил (набор с YARA-правилами не должен превышать размер в 1 ГБ). Обязательным условием для сохранения файла является задание его имени в соответствующей строке. Имена правил, сохраняемые в файл, должны быть уникальными, то есть не иметь повтора в рамках одного или нескольких правил, входящих в файл или набор. Для YARA-правил в рамках наборов это утверждение не распространяется – в разных наборах могут содержаться YARA-правила с одинаковыми именами.

Важно

Имена файлов с YARA-правилами не должны превышать длину в 300 символов (байтов).

Аналитик может воспользоваться функцией загрузки файла формата .yar или .yara при создании нового файла с YARA-правилами в окне **Добавить YARA-правила**. Чтобы загрузить файл с компьютера аналитика, необходимо нажать кнопку  , после чего выбрать соответствующий файл в открывшемся окне и нажать кнопку **Открыть**.

Аналитик может фильтровать правила и файлы на странице по имени файла (поле **Имя** в таблице с правилами), имени правила, а также по признаку активности правила. При этом поиск по имени правила требует ввода полного имени и является зависимым от регистра, а поиск по имени файла от регистра не зависит и не требует ввода полного имени.

Подробнее об условиях и структуре YARA-правил можно узнать в разделе 7 и в официальной документации YARA.

YARA-правила (память)

YARA-правила для памяти – это программные элементы, которые позволяют определить вредоносные сигнатуры внутри памяти процесса путем ее сканирования.

Важно

Если не указан действие (action) в секции meta, то при срабатывании у YARA-правил для памяти будет выбрано действие по умолчанию детектировать (detect).

Правила в разделе «YARA-правила (память)» используются для сканирования памяти процесса по требованию по команде memscan с указанием конкретного процесса..

Наборы YARA-правил для памяти формируются также, как и наборы YARA-правил для файлов. Доступны следующие операции с наборами:

1) Добавление набора;
2) Применение всех наборов (сохранение изменений, произведенных в наборах);
3) Удалить выбранные наборы;
4) Редактировать отдельный набор (изменение имени набора);
5) Удалить отдельный набор;
6) Передать отдельный набор агентам.

Для работы внутри отдельного набора необходимо кликнуть по имени набора с YARA-правилами. Откроется страница **YARA-правила (память)** (рис. 47).

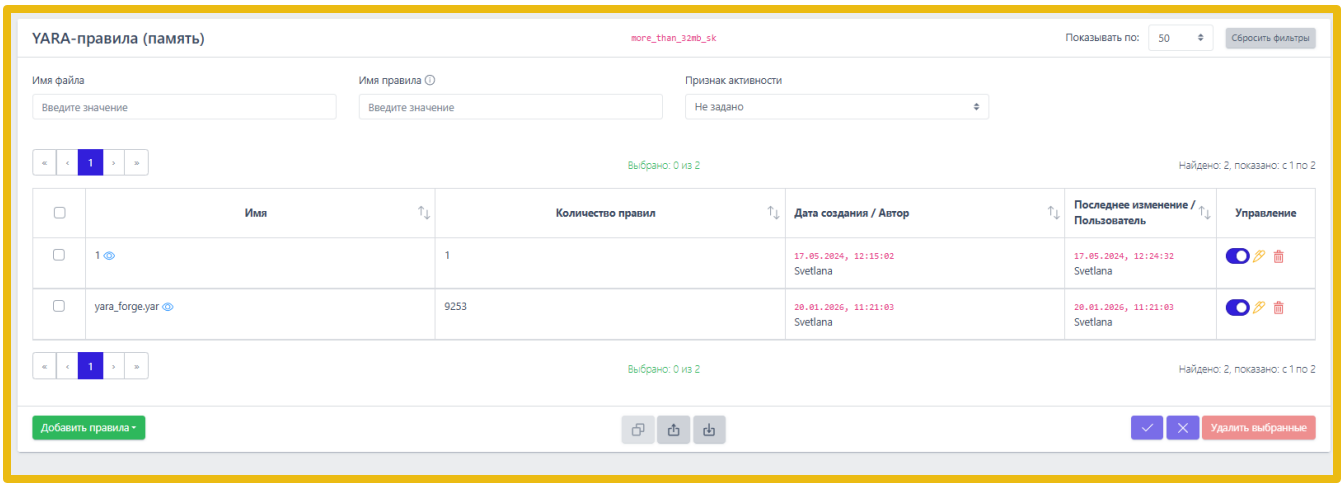


Рисунок 47 – YARA-правила (память)

Операции, которые можно выполнить на странице, представлены в таблице 53.

Таблица 53 – Операции на странице YARA-правила (память)

Операция	Шаги
Добавить YARA-правило или несколько правил в формате одного файла	1. Нажать кнопку Добавить правила. 2. Выбрать пункт **Новый файл**. Откроется окно **Добавить YARA-правила**. 3. В открывшемся окне ввести имя файла. 4. Нажать кнопку **Загрузить файл** ( ) и выбрать .yar или .yara-файл и нажать кнопку **Открыть**. Текст правила будет загружен в окно **Добавить YARA-правила**. 5. Если правило(а) прописываются вручную, то записать текст одного или нескольких правил в окне **Добавить YARA-правила**. 6. Нажать кнопку **Сохранить**.
Добавить YARA-правило или несколько правил в формате загрузки нескольких файлов	1. Нажать кнопку Добавить правила. 2. Выбрать пункт Загрузить файлы. Откроется окно Загрузить файлы YARA. 3. Нажать кнопку **Выбрать файлы**. В открывшемся окне выбрать один или несколько файлов в формате .yar или .yara, после чего нажать кнопку **Открыть**. При выборе нескольких файлов необходимо зажать клавишу Ctrl или Shift. 4. Нажать кнопку Загрузить файлы на сервер.

Операция	Шаги
Передать набор агентам (применить изменения в YARA-правилах набора на агентах)	1. Нажать кнопку Передать набор агентам ().
Копировать или переместить выбранные элементы в другой набор	1. Отметить флажком () одно или несколько правил. 2. Нажать кнопку Копировать/Переместить выбранные элементы в другой набор (). Откроется окно Выбор набора. 3. В строке **Набор** выбрать набор, в который должны быть скопированы/перемещены правила. Если требуется переместить выбранные элементы с удалением из текущего набора, то следует установить флажок **Переместить и удалить выбранные элементы из текущего набора**. 4. Нажать кнопку **Выбрать**.
Экспортировать набор с правилами в файл	1. Нажать кнопку **Экспортировать набор в файл** (). Файл сохранится в папку автосохранения (чаще всего **Загрузки**)
Импортировать данные из файла в набор	1. Нажать кнопку Импортировать данные из файла в набор, поддерживаемые форматы: JSON. 2. В открывшемся окне выбрать файл для импорта и нажать кнопку **Открыть**.
Деактивировать один или несколько элементов (файлов с YARA-правилами)	1. Выбрать один или несколько элементов, установив флажок (); 2. Нажать кнопку Деактивировать выбранные элементы (). Откроется окно Подтверждение действия. 3. Нажать кнопку **Подтвердить**.
Активировать один или несколько элементов (файлов с YARA-правилами)	1. Выбрать один или несколько деактивированных элементов, установив на них флажок (); 2. Нажать кнопку Активировать выбранные элементы (). Откроется окно Подтверждение действия.

Операция	Шаги
	3. Нажать кнопку **Подтвердить**.
Удалить один или несколько выбранных элементов (файлы с YARA-правилами)	1. Выбрать один или несколько, установив на них флажок (); 2. Нажать кнопку Удалить выбранные. Откроется окно Подтверждение действия. 3. Нажать кнопку **Подтвердить**.
Деактивировать файл с YARA-правилами	1. В строке с выбранным файлом нажать кнопку **Деактивировать YARA-правила (память)** (). Откроется окно **Подтверждение действия**. 2. Нажать кнопку **Подтвердить**.
Редактировать файл с YARA-правилами	1. В строке с выбранным файлом нажать кнопку **Редактировать** (). Откроется окно **Редактировать YARA-правила**. 2. Выполнить необходимые изменения YARA-правил и нажать кнопку **Сохранить**.
Удалить файл с YARA-правилами	1. В строке с выбранным файлом нажать кнопку **Удалить** ().Откроется окно **Подтверждение действия**. 2. Нажать кнопку **Подтвердить**.

Файлы и правила на странице можно фильтровать с помощью фильтров:

1) Имя файла;
2) Имя правила;
3) Признак активности.



Важно

При поиске по имени правила необходимо вводить полное имя правила с учетом регистра.

11.10.4. Журналы

Во многих случаях для определения аномальной активности в защищаемой инфраструктуре аналитику могут понадобиться события, которые относятся к подсистеме журналирования Windows. Раздел **Журналы** позволяет подключать к EDR внешние источники событий операционной системы и приложений помимо собственной телеметрии агента (процессы, файлы, сеть, реестр). Это даёт аналитику единую ленту: и поведенческие события агента, и записи системных журналов, и строки произвольных лог-файлов приложений.

Поддерживаются два типа источников, представленные в таблице 54:

Таблица 54 – Типы источников событий Журналы

Тип источника	Что собирает	Подтип события в ленте
ETW-источник	События журналов Windows через механизм ETW / Windows Event Log (Application, Security, System и т. д.)	Событие журнала
Файл	Строки текстового лог-файла (стриминг лог-файла)	Строка лог-файла

ETW (Event Tracing for Windows) — встроенная в Windows подсистема трассировки. Через неё операционная система и приложения публикуют события: входы пользователей, изменения учётных записей, ошибки служб, действия ПО безопасности и многое другое. Каждый поставщик событий (провайдер) идентифицируется именем (например, Microsoft-Windows-Security-Auditing) или GUID. EDR подписывается на нужные провайдеры и принимает их события в реальном времени.

Важно

ETW является механизмом ОС Windows. На Linux-агентах ETW-источники не применяются; для них необходимо использовать сбор лог-файлов.

После установки на хосте агент регистрирует ETW-провайдер RT Protect EDR. В этом журнале аналитик может просмотреть сообщения с ошибками, предупреждениями, информацией и т.д. Для просмотра журнала на агенте необходимо перейти в **Панель управления/Средства администрирования Windows/Просмотр событий/Журналы приложений и служб/RT Protect EDR**.

Для просмотра журнала на сервере управления необходимо выполнить фильтрацию по DSL-запросу **winlog.provider_name:*RT*** на странице **Активность**.

Чтобы создать или изменить набор с правилами обнаружения событий подсистемы журналирования аналитику необходимо перейти в раздел **Журналы**, где находятся наборы журналов

Аналитик может выполнить поиск по подстроке без учета регистра по текстовому содержимому в поле **Имя журнала**. Кроме того, доступен поиск по названию набора на странице **Наборы журналов**, и уточняющие фильтры **Имя журнала/Файла**, **Уровень** и **Признак активности** на странице **Журналы**.

На странице **Наборы журналов** пользователю доступны те же операции, что и на других страницах с наборами:

1) Добавление новых наборов;

2) Редактирование имен наборов ();

3) Удаление выбранных наборов или удаление отдельного набора ();

4) Передать изменения всех наборов агентам () или передать отдельный набор привязанным агентам ().

Для перехода к странице **Журналы** необходимо нажать ЛКМ на имени набора.

На странице **Журналы** в табличном виде отображается информация о конкретном наборе журналов.

Пользователь Программы, используя инструментарий, описанный ранее в пункте 11.10.2, может выполнить на странице следующие операции:

– добавить новое правило или несколько правил;

– редактировать или удалить существующее правило/правила;

– выполнить экспорт/импорт файла с набором;

– копировать элементы одного набора или весь набор в другой набор;

– активировать/деактивировать правило в наборе.

В таблице **Журналы** отображаются следующие поля:

1) Поля кнопки выбора ();

2) Имя журнала/Файла;

3) Ключевые слова (любые);

4) Ключевые слова (все);

5) Уровень;

6) Фильтр кодов событий;

7) Дополнительные параметры;

8) Дата создания/Автор;

9) Последнее изменение/Пользователь;

10) Управление.

Имя журнала/Файла – в поле отображается имя провайдера событий подсистемы ETW или имя файла (с которого будет осуществляться стриминг логов).

Ключевые слова (любые) – в поле отображается информация о любых ключевых словах, на основе которых будут обнаруживаться события выбранного журнала. В Программе доступна настройка детектирования событий по ключевым словам, для определенных журналов (ETW-провайдеров), задавать ключевые слова необязательно.

Ключевые слова (все) – в поле отображается информация о всех ключевых словах, на основе которых будут обнаруживаться события выбранного журнала. В Программе доступна настройка детектирования событий по ключевым словам, для определенных журналов (ETW-провайдеров), задавать ключевые слова необязательно.

Уровень – в поле отображается уровень обнаруживаемого события журнала ETW, заданный пользователем Программы. Доступны следующие уровни событий: **Подробно**, **Информация**, **Предупреждение**, **Ошибка** и **Критическая ошибка**. При выборе уровня **Информация** пользователю будет показаны все события вышестоящего уровня, наряду с уровнем **Информация**, то есть **Предупреждение**, **Ошибка**, **Критическая ошибка**. При выборе уровня **Предупреждение**, будут также отображаться уровни **Ошибка** и **Критическая ошибка** и так далее.

Фильтр кодов событий – в поле прописываются коды событий, согласно которым будут фильтроваться события выбранного провайдера. Правила записи кодов событий отображается при наведении курсора на значок ⓘ в окне добавления журнала (рис 48).

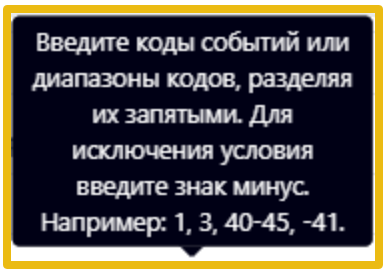


Рисунок 48 – Правила записи кодов событий

Дополнительные параметры – в поле отображается информация о дополнительных параметрах детектирования ETW-событий.

Доступны для выбора следующие параметры:

1) SID пользователя;

2) ID терминальной сессии;

3) Стек вызовов;

4) Исключить события с нулевым значением KEYWORD;

5) Порядковый номер процесса;

6) Ключ события;

7) Исключить события от приватных процессов.

Чтобы добавить нового провайдера событий подсистемы ETW, в соответствии с настройками которого будут обнаруживаться события на агенте, необходимо в нижней части страницы нажать кнопку Добавить журнал. Пользователю доступно следующие режимы добавления журнала:

– по GUID;

– по имени канала;

– режим добавления файла.

Для режима **GUID** обязательными к заполнению являются поля **Имя провайдера** и **GUID провайдера**. Для режима **Имя канала** обязательным для заполнения является поле **Имя канала**.

Для режима добавления файла обязательным является поле **Имя файла**. Журналирование по имени файла означает, что пользователь может отслеживать все изменения в этом файле с помощью раздела **Журналы**. Это может быть нужно аналитику, так как многие программы пишут логи в обычные текстовые файлы.

С помощью функции журналирования по имени файла можно следить за новыми записями, сообщающими о том, что происходит внутри соответствующих приложений. В поле **Имя файла** необходимо указать путь к файлу, например, C:\nginx\logs\access.log или C:\Myapp\logs*.log (можно использовать маску, чтобы следить за всеми файлами в папке). Дополнительно можно задать фильтры. Для файлового журнала фильтрация применяется в виде регулярного выражения. Это могут быть выражения для включения записей и выражения для исключения записей, разделенные символом перевода строки. Например, в первом случае в конфигурации указано **ERROR|Critical**, то в поток данных попадут только строки, содержащие слова ERROR или Critical, а во втором случае попадут все строки, кроме тех, что содержат слова ERROR или Critical. Оба фильтра необязательны. Без фильтров на странице **Активность** будут отображаться все строки файла.

После появления нового журнала в Программе и передачи конфигурации с журналом на конечную точку агент будет автоматически читать новые строки в этом журнале. Строки появятся в EDR на странице **Активность** в виде отдельных событий источника **Журналы**. Строки лог-файла отображаются с подтипом «Строка лог-файла». В описании события показывается имя файла и сам текст строки.

Для копирования или перемещения журнала из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ).

Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с журналами в файл следует нажать кнопку **Экспортировать набор в файл** ( ).

Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта журналов из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** ( ). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные журналы, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать журналы из выбранного набора, необходимо нажать кнопку / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( ).

Для удаления журналов из набора необходимо отметить флажками журналы, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить журналы по отдельности с помощью кнопки **Удалить** ( ).

Рекомендации по работе с журналами

1) Необходимо сужать поток событий журнала с помощью фильтров. Для ETW следует поднимать уровень важности и использовать включение/исключение записей, а для файлов необходимо задавать значения в фильтрах по содержимому лог-файла. Это уменьшает «шум» и нагрузку на подсистему журналирования.

2) Необходимо точно указыватье путь к файлу. Источник «Файл» читает конкретный файл, поэтому аналитик должен убедиться, что у агента есть доступ к этому файлу, и что приложение пишет именно по выбранному пути.

3) Необходимо разделять Windows и Linux. ETW-источники имеют смысл только для Windows, для Linux-хостов следует использовать лог-файлы.

4) Следует проверять регулярные выражения на реальных строках лога перед массовым назначением набора, так как неверный шаблон может отсечь нужные записи.

11.10.5. Встроенные правила аналитики на агенте

Встроенные правила на агенте с описанием представлены в таблице 55.

Таблица 55 – Встроенные правила на агенте

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
RT_win_PE_base64_reg_value	Обнаружена запись исполняемого файла в реестр	T1112	Правило срабатывает при записи данных PE-файла (в кодировке base64) в значение реестра Windows.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
RT_win_hidden_reg_value	Обнаружена запись скрытого значения в реестр	T1112, T1564,	Правило срабатывает при создании значения реестра с именем, длина которого отлична от нуля, первым символом которого выступает null-символ (символ с кодом 0). Редактор реестра не может корректно отобразить такое значение ключа реестра, поэтому оно получается скрытым.
RT_win_SAM_access	Обнаружено обращение к конфиденциальным данным реестра	T1012, T1003 /002	Правило срабатывает при доступе к данным из реестра Windows по путям HKLM\\sam или HKLM\\security\\policy\\secrets, кроме случаев, когда такой доступ выполняет LSASS или антивирусный компонент.
RT_win_pwsh_encoded_command	Обнаружена попытка запуска закодированной PowerShell команды	T1059/001	Правило срабатывает, если запускается процесс PowerShell, в командной строке которого есть вхождения подстрок -enc или /enc (без учета регистра, кроме encoding и /encoding)
RT_win_cmdl_tampering	Обнаружена подмена командной строки процесса	T1036	Правило срабатывает при обнаружении изменения командной строки процесса относительно той, которая была указана при создании процесса.
RT_win_illegal_proc_unprotection	Обнаружено несанкционированное понижение уровня защиты процесса	T1548	Правило срабатывает при обнаружении понижения уровня защиты процесса относительно того, который был задан при создании процесса.
RT_win_illegal_proc_protection_elevation	Обнаружено несанкционированное повышение уровня защиты процесса	T1548	Правило срабатывает при обнаружении повышения уровня защиты процесса относительно того, который был задан при создании процесса.
RT_win_proc_hollowing	Обнаружена попытка подмены исполняемого образа методом Process Hollowing	T1055/012, T1036	Правило срабатывает, если оказывается, что по базовому адресу размещения исполняемого файла процесса в памяти отсутствует спроецированный исполняемый образ. Это может означать, что исходный исполняемый образ выгружен, а вместо него развернут иной (вредоносный) исполняемый код методом reflective PE load, т.е. прямой модификацией памяти.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
RT_win_proc_tampering	Обнаружена попытка подмены исполняемого образа	T1055, T1036	Правило срабатывает, если оказывается, что по базовому адресу размещения исполняемого файла процесса в памяти спроецирован иной (вредоносный) образ.
ProcessCallbackMiss	Отсутствуют функции слежения за процессами	T1562	Не найдена точка встраивания мониторинга активности процессов. Возможное вмешательство в работу агента извне.
ImageCallbackMiss	Отсутствуют функции слежения за исполняемыми образами	T1562	Не найдена точка встраивания мониторинга загружаемых DLL. Возможное вмешательство в работу агента извне.
ThreadCallbackMiss	Отсутствуют функции слежения за нитями	T1562	Не найдена точка встраивания мониторинга активности нитей. Возможное вмешательство в работу агента извне.
ObjectCallbackMiss	Отсутствуют функции слежения за доступом к объектам ОС	T1562	Не найдена точка встраивания мониторинга доступа к процессам/нитям. Возможное вмешательство в работу агента извне.
RegistryCallbackMiss	Отсутствуют функции слежения за реестром	T1562	Не найдена точка встраивания мониторинга реестра. Возможное вмешательство в работу агента извне
FileSystemCallbackMiss	Отсутствуют функции слежения за файловой активностью	T1562	Не найдена точка встраивания мониторинга файлов. Возможное вмешательство в работу агента извне.
NoProcessCallbackArray	Не удалось найти свои функции слежения за процессами		Внутренняя проблема агента. Правило срабатывает, если агент не может поставить на контроль свою точку встраивания мониторинга процессов. Дальнейший контроль точки встраивания будет невозможен. Необходимо обратиться к разработчикам.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
NoImageCallbackArray	Не удалось найти свои функции слежения за образами		Внутренняя проблема агента. Правило срабатывает, если агент не может поставить на контроль свою точку встраивания мониторинга загружаемых DLL. Дальнейший контроль точки встраивания будет невозможен. Необходимо обратиться к разработчикам.
NoThreadCallbackArray	Не удалось найти свои функции слежения за нитями		Внутренняя проблема агента. Правило срабатывает, если агент не может поставить на контроль свою точку встраивания мониторинга активности нитей. Дальнейший контроль точки встраивания будет невозможен. Необходимо обратиться к разработчикам.
CollidingCallbackArrays	Внутренняя ошибка поиска своих функций слежения		Внутренняя проблема агента. Правило срабатывает, если агент не может поставить на контроль свои точки встраивания в систему. Дальнейший контроль точек встраивания будет невозможен. Необходимо обратиться к разработчикам.
DriverVerificationEnabled	Включена верификация драйвера		В режиме верификации агент не может поставить на контроль свои точки встраивания в систему. Дальнейший контроль точек встраивания будет невозможен.
DriverCodeIntegrityViolation	Нарушена целостность драйвера	T1562	Правило срабатывает при обнаружении модификации кода драйвера в памяти. Возможное вмешательство в работу агента извне.
ServiceCodeIntegrityViolation	Нарушена целостность службы	T1562	Правило срабатывает при обнаружении модификации кода службы в памяти. Возможное вмешательство в работу агента извне.
RT_win_illegal_procexp_driver_load	Обнаружена попытка несанкционированной загрузки драйвера ProcExp	T1204/002, T1562	Правило срабатывает, если драйвер утилиты Process Explorer загружается нелегально. Данный драйвер в таком сценарии часто используется для противодействия средствам защиты.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
RT_win_potential_mirror_dump_LSASS_prepare	Обнаружена попытка дампа LSASS	T1003/001	Правило срабатывает на подготовительный этап техники типа mirror dump дампа LSASS. Поскольку при этом дамп происходит по инициативе самого процесса LSASS (внедренного в него кода), то обнаруживается попытка открытия из LSASS стороннего процесса с правами PROCESS_DUP_HANDLE (0x40)
RT_win_mirror_dump_LSASS	Обнаружена попытка дампа LSASS	T1003/001	Правило срабатывает, когда процесс LSASS (внедренный в него код) производит дупликацию своего описателя для стороннего процесса с правами на чтение памяти, что характерно для техники mirror dump дампа LSASS.
RT_win_read_ntdll	Обнаружен подозрительный доступ к файлу ntdll.dll	T1106	Правило срабатывает на операцию чтения системного файла ntdll.dll, не связанную с его загрузкой в память для исполнения кода. Чтение может производиться с целью получения информации о номерах системных вызовов конкретной версии ОС, а также другой системной информации.
RT_win_read_ntoskrnl	Обнаружен подозрительный доступ к файлу ntoskrnl.exe	T1106	Правило срабатывает на операцию чтения системного файла ntoskrnl.exe, не связанную с его загрузкой в память для исполнения кода. Чтение может производиться с целью получения информации о номерах системных вызовов конкретной версии ОС, а также другой системной информации.
Ransomware	Обнаружен процесс-шифровальщик	T1486	Правило генерируется подсистемой Антишифр как результат оценки поведения процесса на предмет его схожести со злонамеренным шифрованием или уничтожением данных.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
MaliciousDomain	Обнаружено обращение к вредоносному доменному имени		Обнаружение формируется на основе вердикта, вынесенного в отношении доменного имени TI-платформой. Подавить обнаружение можно с помощью механизма сетевых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю сетевую аналитику для заданного процесса.
MaliciousFile	Обнаружен вредоносный файл		Обнаружение формируется на основе вердикта, вынесенного в отношении хеша файла TI-платформой. Подавить обнаружение можно с помощью механизма файловых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю аналитику статического содержимого файлов для заданного процесса.
MaliciousIp	Обнаружен вредоносный IP-адрес		Обнаружение формируется на основе вердикта, вынесенного в отношении IP-адреса TI-платформой. Подавить обнаружение можно с помощью механизма сетевых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю сетевую аналитику для заданного процесса.
MLStaticDetection	Обнаружен файл с потенциально вредоносным содержимым (анализ с помощью ML)		Обнаружение формируется на основе вердикта, вынесенного в отношении исполняемого файла статическим анализатором на основе машинного обучения. Подавить обнаружение можно с помощью механизма файловых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю файловую аналитику для заданного процесса.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
SuspiciousFile	Обнаружен подозрительный файл		Обнаружение формируется на основе вердикта, вынесенного в отношении хеша файла TI-платформой. Подавить обнаружение можно с помощью механизма файловых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю аналитику статического содержимого файлов для заданного процесса.
SuspiciousDomain	Обнаружено обращение к подозрительному доменному имени		Обнаружение формируется на основе вердикта, вынесенного в отношении доменного имени TI-платформой. Подавить обнаружение можно с помощью механизма сетевых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю сетевую аналитику для заданного процесса.
SuspiciousIp	Обнаружено обращение к подозрительному IP-адресу		Обнаружение формируется на основе вердикта, вынесенного в отношении IP-адреса TI-платформой. Подавить обнаружение можно с помощью механизма сетевых исключений. Кроме того, с помощью группы флагов 'Исключение анализа *' исключений для программ можно подавить всю сетевую аналитику для заданного процесса.
RT_win_illegal_CSS_process_access	Недопустимый доступ к критическому системному процессу	T1003	Правило срабатывает на операцию открытия сторонним процессом процесса LSASS с правом PROCESS_CREATE_PROCESS, что характерно для техник дампа LSASS, построенных на клонировании адресного пространства процесса.
RT_win_handle_theft_LSASS	Кража описателя процесса LSASS (потенциальный дампинг памяти LSASS)	T1003/001	Правило срабатывает при обнаружении дуплицирования описателя процесса LSASS (но не им самим) для стороннего процесса с правами на чтение памяти.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
RT_win_inject	Обнаружено внедрение стороннего кода в процесс	T1055	Событие возникает, если в процессе создается нить другим процессом (кроме самой первой нити, которая всегда создается родительским процессом в дочернем). Критичность и действие в отношении данного события определяются настройками в Профиле безопасности агента.
RT_win_open_proc	Обнаружено открытие процесса	T1057	Событие возникает, если один процесс открывает другой процесс с правами внедрения кода, чтения/записи памяти или управления. Критичность и действие в отношении данного события определяются настройками в Профиле безопасности агента.
RT_win_open_thread	Обнаружено открытие нити процесса	T1057	Событие возникает, если один процесс открывает нить другого процесса с правами изменения контекста или управления. Критичность и действие в отношении данного события определяются настройками в Профиле безопасности агента.
RT_win_raw_disk_write	Обнаружено прямое обращение к диску (запись)	T1006	Событие возникает при обнаружении прямой (минуя ФС) записи на диск. Данное поведение является легитимным для утилит управления дисками, а также соответствующих компонентов ОС. Критичность и действие в отношении данного события определяются настройками в Профиле безопасности агента.
RT_win_raw_disk_read	Обнаружено прямое обращение к диску (чтение)	T1006	Событие возникает при обнаружении прямого (минуя ФС) чтения с диска. Данное поведение является легитимным для утилит управления дисками, а также соответствующих компонентов ОС. Критичность и действие в отношении данного события определяются настройками в Профиле безопасности агента.
RT_win_anonymous_assembly_load	Загрузка анонимной сборки	T1620	Правило срабатывает при обнаружении загрузки .NET-сборки в процесс бесфайловым способом (например, из потока данных в памяти).

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
RT_win_pwsh_assembly_load	Загрузка движка PowerShell в процесс	T1059/001	Правило срабатывает при обнаружении загрузки .NET-сборки движка PowerShell (System.Management.Automation.dll) в процесс.
RT_win_potential_priv_escalation	Потенциальное повышение привилегий	T1548	Правило обнаруживает создание процесса от имени СИСТЕМА (или др. привилегированных УЗ) с подменной цепочкой родителей, указывающей на explorer.exe. Правило отражает факт повышения привилегий, не идентифицируя конкретный способ такого повышения. Правило будет срабатывать при использовании утилиты PsExec и ей подобных.
IllegalNativeServiceChildProcess	Попытка запуска недопустимого дочернего процесса службой	T1211	Правило обнаруживает нелегитимный запуск дочернего процесса службой агента. Может являться признаком вмешательства в работу агента извне.
ShellCodeInsideNativeService	Попытка запуска недопустимого дочернего процесса службой	T1055, T1562	Правило обнаруживает создание службой агента нити, адрес точки входа которой не принадлежит области памяти исполняемого образа. Может являться признаком вмешательства в работу агента извне.
SuspiciousNativeServiceImageLoad	Загрузка подозрительного образа в процесс службы	T1055, T1562	Правило срабатывает, если в процесс службы загружается исполняемый образ (DLL) с признаками подмены образа или неподписанный доверенной ЭП и не из каталога Windows, или загрузку осуществляет сторонний процесс.
IllegalNativeServiceNetworkInteraction	Попытка недопустимого сетевого взаимодействия со стороны службы	T1211	Правило обнаруживает нелегитимное сетевое соединение службы агента. Может являться признаком вмешательства в работу агента извне.
SaveFileToAgentDir	Попытка сохранения файла в директорию агента	T1562	Правило срабатывает при обнаружении файловой операции с компонентами агента.
AgentFileModify	Попытка модификации файла агента	T1562	Правило срабатывает при обнаружении файловой операции с компонентами агента.

Название правила	Расшифровка правила	Соответствие технике MITRE	Описание
AgentFileDeleteOrRename	Попытка удаления или переименования файла агента	T1562	Правило срабатывает при обнаружении файловой операции с компонентами агента.
AgentFileChangeSecurity	Попытка изменения атрибутов безопасности файла агента	T1562	Правило срабатывает при обнаружении файловой операции с компонентами агента.
RT_win_potential_DCSync	Сетевое правило обнаружения атаки DCSync	T1003/006	Правило срабатывает, когда по сети к контроллеру домена приходит запрос репликации секретов DSGetNCChanges, которому предшествовала привязка к интерфейсу DRSUAPI в той же TCP-сессии
RT_win_remote_SAM_access	Правило обнаружения удаленного доступа к реестровым кустам с учетными данными	T1012,T1003/002	Правило срабатывает, когда служба удалённого реестра (Remote Registry) читает значение из реестрового куста с учётными данными — HKLM\SAM или HKLM\SECURITY\Policy\Secrets

11.11 Добавление файлов или программ в список исключений

Исключения – это программные элементы, которые позволяют переопределить логику определенного события, например, сделать так, чтобы файл, который изначально система определила вредоносным, воспринимался ей далее безопасным. Кроме того, исключения позволяют ограничить работу программы с помощью помещения её в «черный» список, при этом инцидент в Программе создаваться не будет.

Исключения необходимы в случае появления ложных срабатываний.

Ложные срабатывания можно разделить на два типа:

1) Статические – срабатывания, основанные на анализе содержимого исполняемых файлов (или файлов с потенциально активным содержимым, например, PDF и др.);

2) Поведенческие – такие срабатывания возникают в результате анализа действий процессов.

Чтобы добавить программу или файл в список исключений (если произошло ложное срабатывание), аналитик может воспользоваться функционалом разделов **Исключения для файлов** и **Исключения для программ**.

Чтобы добавить исключение, нужно выбрать набор с правилами и добавить файл или программу в исключения по имени или хешу, а в случае с программой можно дополнительно добавить ее по командной строке.

Аналитик может осуществлять поиск по текстовым полям без учета регистра во всех наборах с исключениями. Кроме того, на странице с наборами аналитик может фильтровать наборы по их названию, а при переходе на страницу с исключениями может воспользоваться уточняющими фильтрами. Список их разнится в зависимости от типа исключения.

11.11.1. Механизм работы файловых исключений

Механизм файловых исключений предназначен для переопределения логики обработки файлов с потенциально активным содержимым (далее просто «файлы») со стороны агента EDR, которая реализуется перед запуском этих файлов. Среди файлов с активным содержимым можно выделить отдельную группу – исполняемые файлы, т.е. файлы программ (динамических библиотек, драйверов). Под термином «запуск» подразумевается исполнение программ (исполняемых файлов), загрузка динамических библиотек (или драйверов) для исполнения их кода, любое открытие PDF-документов или скриптов (если применены соответствующие настройки в профиле безопасности агента), подразумевающее доступ к их содержимому, что трактуется тоже как попытка запуска.

В отсутствии файлового исключения для заданного файла агент при попытке запуска этого файла перед его запуском синхронно (т.е. в режиме реального времени) производит следующие действия:

1) Проверка файла по набору индикаторов компрометации (на основе имени файла или хеша от его содержимого), назначенному агенту;

2) Для исполняемых файлов выполняется статический анализ содержимого файла с использованием модели машинного обучения;

3) Сканирование содержимого файла по набору YARA-правил, назначенному агенту.



Важно

Кроме синхронной проверки механизм файлового сканирования предполагает также проверку в отложенном режиме, когда проверка происходит при создании или модификации файла.

Если по результатам проверок, перечисленных выше, запуск файла не блокируется, то для исполняемых файлов в потоке событий появляется событие о запуске программы или загрузке динамической библиотеки (драйвера), содержащее в числе прочего хеш исполняемого файла (sha-256 и, опционально, sha-1, md5 или imphash, что определяется настройками профиля безопасности агента).

Когда данное событие доставляется на сервер EDR, он производит обращение к TI-платформе для проверки этого хеша (sha-256). Вердикт платформы предусматривает несколько вариантов дальнейшего развития событий согласно уровню опасности: «безопасный», «подозрительный» и «опасный».

Получив вердикт в ответ на свой запрос, сервер EDR связывает его с исходным событием и, если вердикт не «безопасный», то регистрирует инцидент ИБ. При получении «опасного» вердикта сервер EDR дополнительно отправляет команду на принудительное завершение соответствующей программы на агенте (если проверка была инициирована событием запуска программы). «Подозрительный» вердикт не подразумевает дополнительных действий со стороны сервера EDR, кроме как регистрацию инцидента ИБ.

При наличии файлового исключения для заданного файла (идентифицируется по имени (в том числе по имени именованного канала) или хешу от содержимого) описанная выше логика изменяется согласно действию, которое предписывается исключением. Если указано действие **Разрешить**, то все проверки, описанные выше, пропускаются (в том числе для исполняемых файлов пропускается взаимодействие с TI-платформой). В данном случае исключение работает в классическом понимании – исключает потенциально ложные срабатывания по содержимому файла (неправильный или нерелевантный индикатор компрометации, неточное YARA-правило, ошибочная оценка модели машинного обучения и т.д.). Если же указано действие **Блокировать**, то запуск файла безальтернативно блокируется.

При этом все описанные выше проверки опять же не выполняются. Однако такая блокировка не генерирует инцидент ИБ – в потоке событий лишь появляется событие о срабатывании исключения для файла с соответствующим предпринятым действием (если не включена опция **Не отправлять события**).

Совет

Такой режим работы с исключениями для файлов может использоваться для реализации политики предотвращения запуска нежелательного ПО, которое в то же время не относится к вредоносному в общем смысле, и, соответственно, попытки запуска которого не должны расцениваться как инцидент ИБ.

Ниже приведены практические примеры использования файловых исключений для решения задач по обеспечению ИБ и соблюдения регламентов по использованию ПО в компаниях.

1. Ложное срабатывание для загружаемой библиотеки msi.dll на платформе Windows.

В реальном контуре зафиксирован поток инцидентов ИБ, вызванных «подозрительным» вердиктом TI-платформы для библиотеки msi.dll (sha256 b98aab78e5ef705e67a1f2ad79d1c66cf7360e0be5a843846e5ec402cbd07c21) платформы Windows (рис. 49).

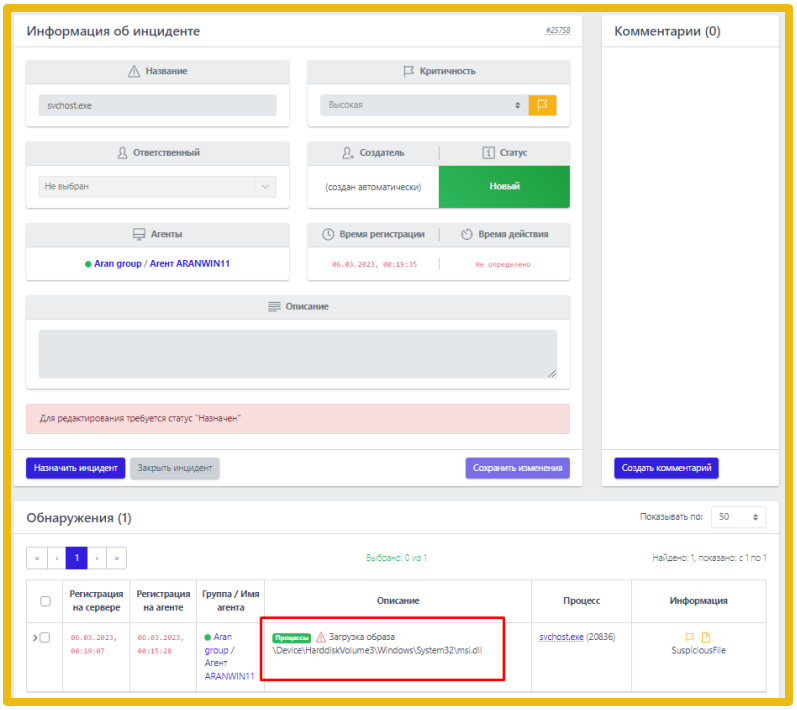


Рисунок 49 – Инцидент с загрузкой образа msi.dll

Данный вердикт обусловлен ошибочным индикатором компрометации в ленте, предоставляемой провайдером MalwareBazaar (рис. 50).

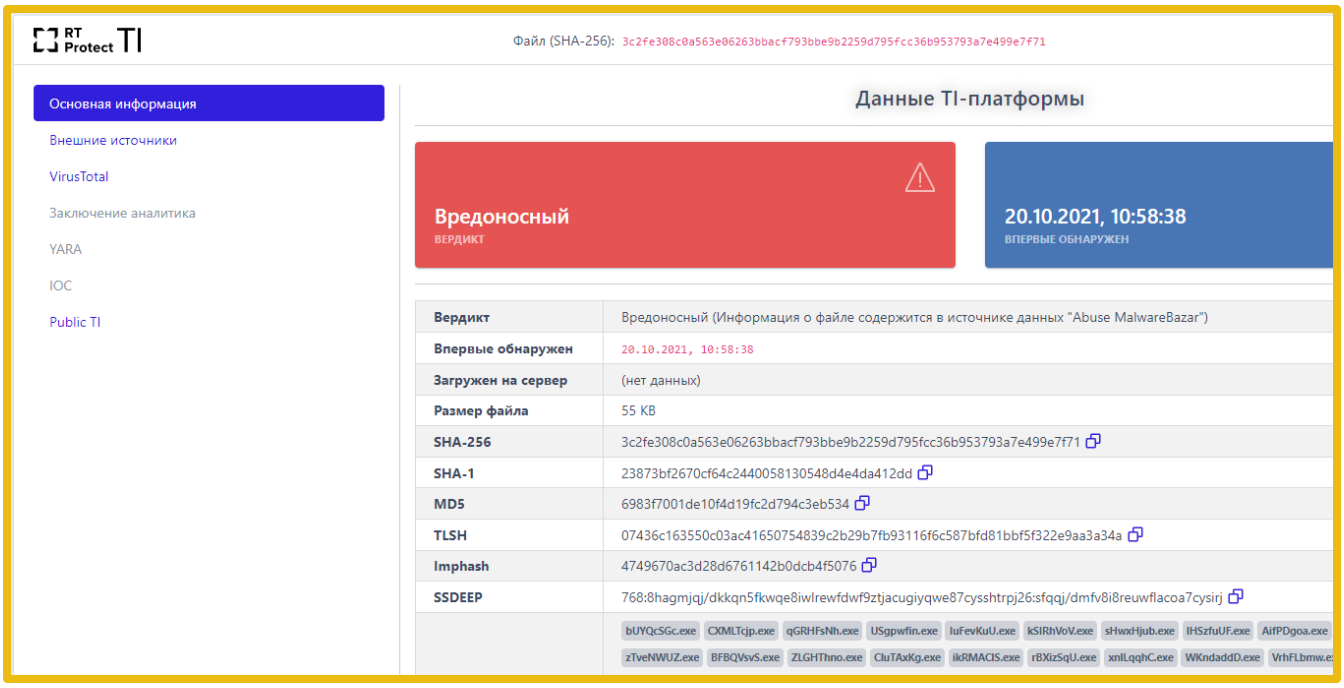


Рисунок 50 – Вердикт TI-платформы

Для решения проблемы создано файловое исключение со статусом **Разрешить** для указанного выше хеша (рис. 51).

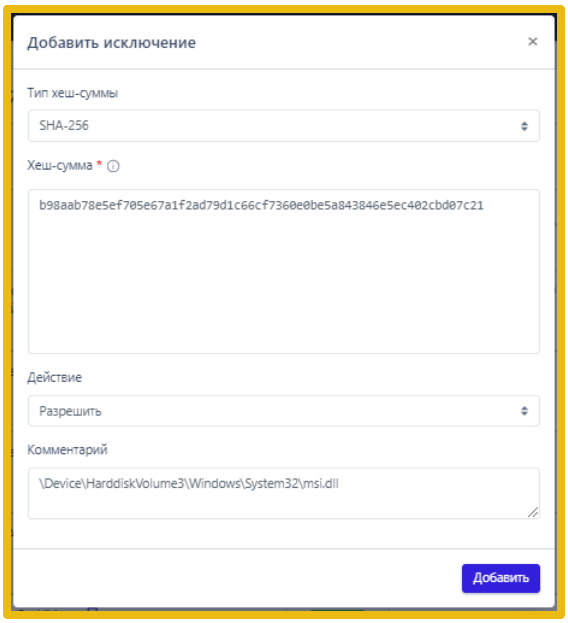


Рисунок 51 – Добавление файлового исключения

2. Запрет использования медиа-приложения MediaGet в компании.

Администратором безопасности в потоке событий обнаружено использование приложения MediaGet (ПО для Windows) в компании, в то время, как такое использование нежелательно (рис. 52).

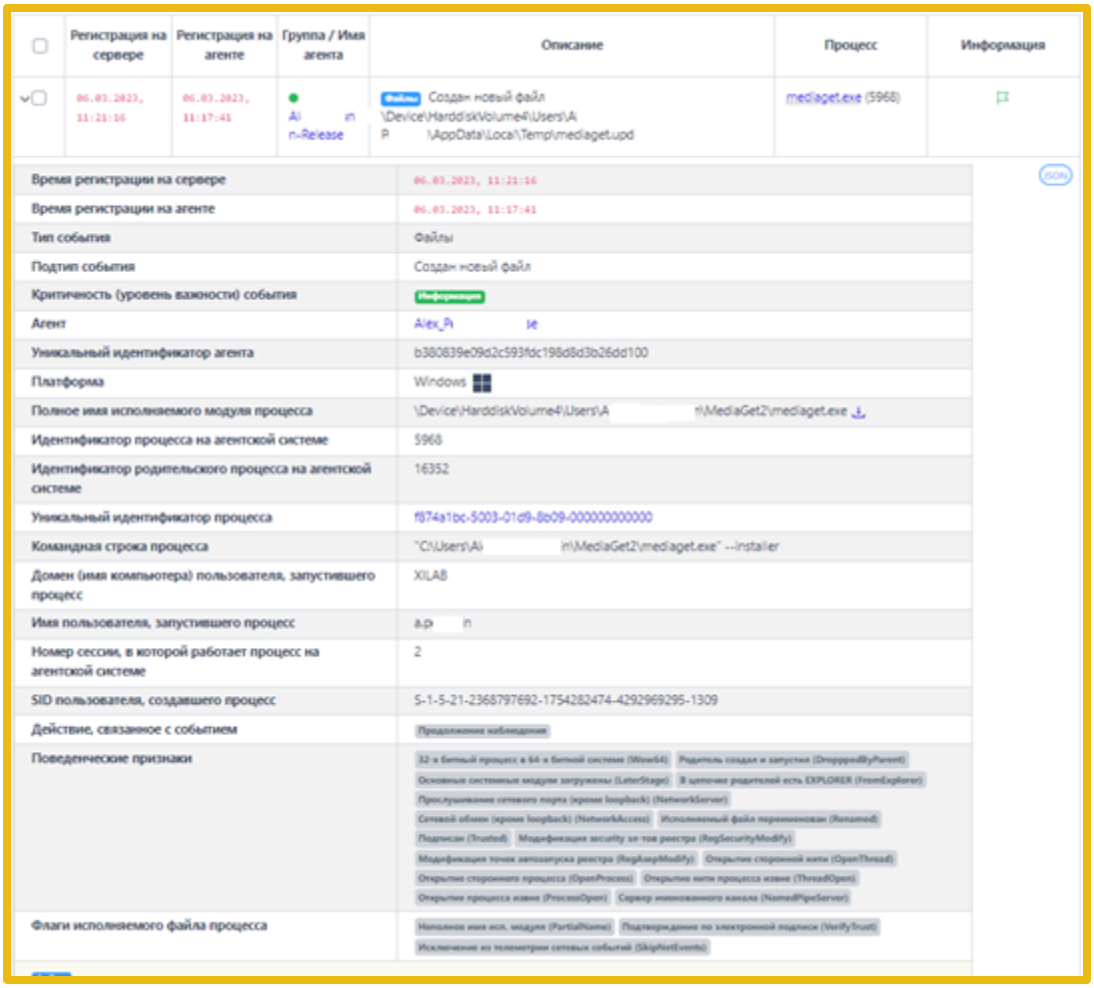


Рисунок 52 – Событие старта процесса mediaget.exe

Администратор может заблокировать использование конкретной версии программы MediaGet путем добавления в файловые исключения хеша ее исполняемого файла с действием **Блокировать** (рис. 53).

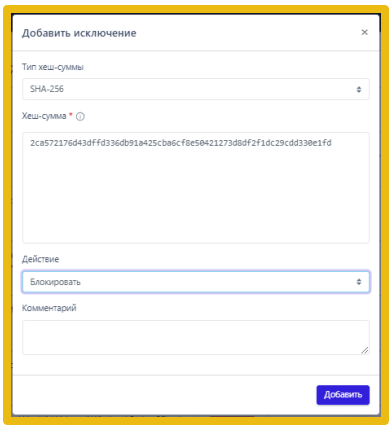


Рисунок 53 – Добавление блокирующего исключения

Кроме того, администратор может заблокировать любой запуск программы по имени ее исполняемого файла – mediaget.exe (рис. 54).

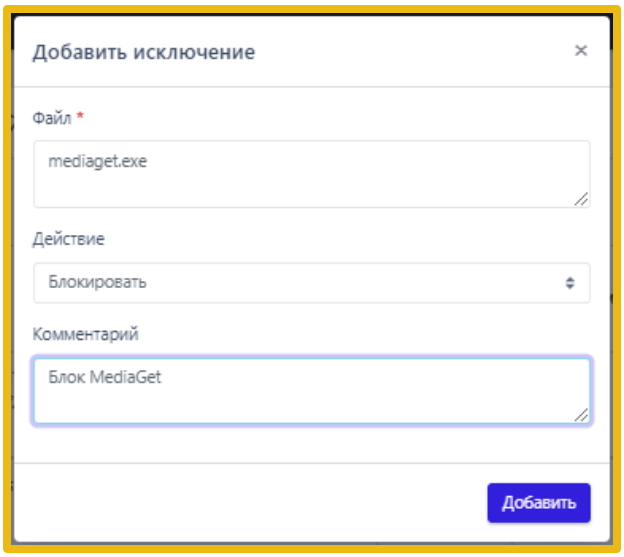


Рисунок 54 – Исключение по имени файла

В том или ином случае последующий запуск ПО MediaGet после создания исключения будет невозможен, а в числе событий при попытке такого запуска будет присутствовать событие о срабатывании соответствующего исключения (рис. 55 и рис. 56).

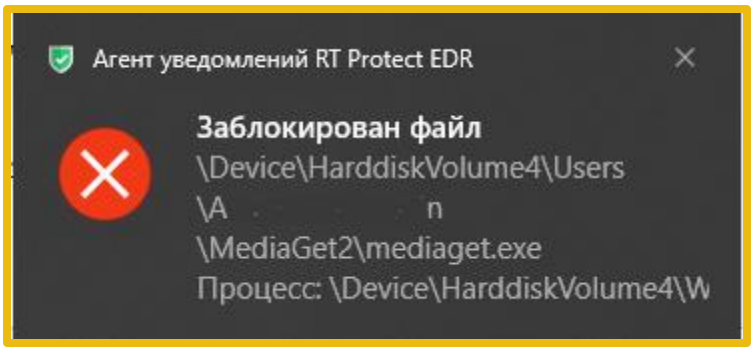


Рисунок 55 – Сообщение о невозможности запуска файла на агенте

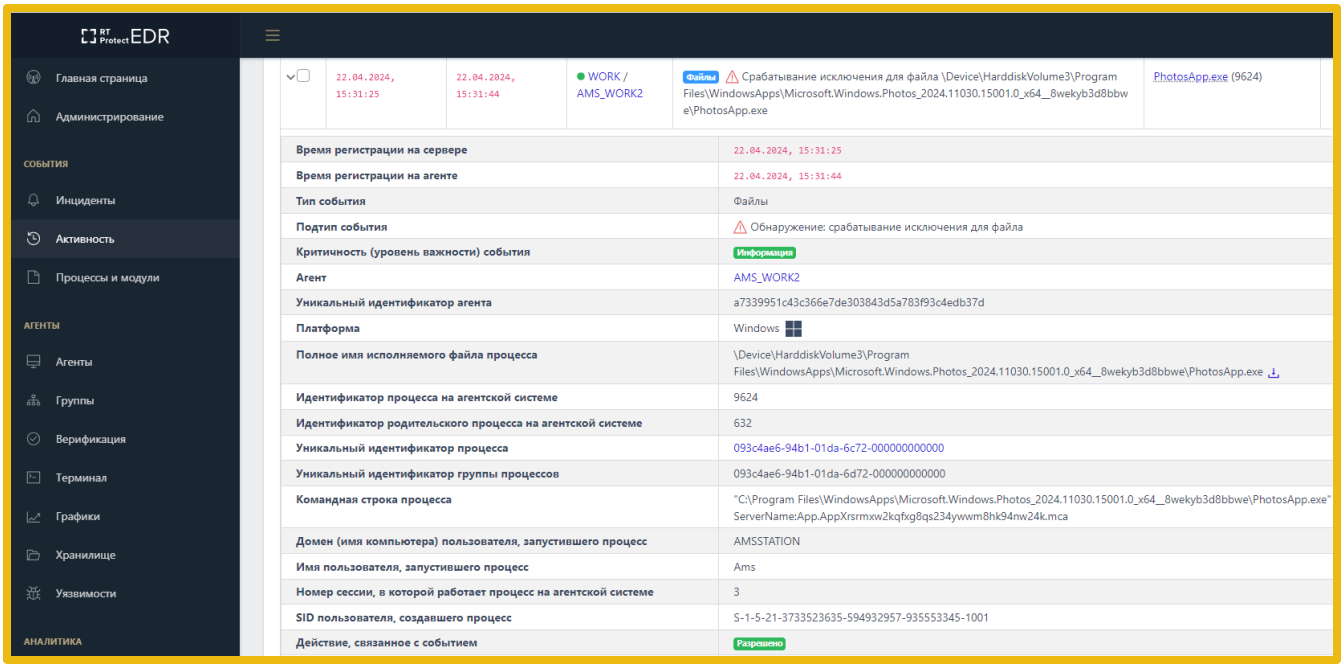


Рисунок 56 – Срабатывание исключения для файла

11.11.2. Добавление исключений для файла

Исключения для файлов основываются на статических проверках содержимого файлов. Для каждого события-обнаружения может существовать только один тип исключения. Тип исключения определяется как файловое для следующих типов событий:

– срабатывание индикатора компрометации для файла (для событий-обнаружений файлового монитора);

– файл классифицирован как вредоносный (ML на агенте) (для событий-обнаружений файлового монитора);

– файл классифицирован как вредоносный (YARA-правила) (для событий-обнаружений файлового монитора);

– события-обнаружения монитора процессов с подтипом **Старт процесса**, у которых в поле **rul** указано правило **SuspiciousFile** или **MaliciousFile**;

– события-обнаружения монитора процессов с подтипами Загрузка образа, Загрузка образа в сторонний процесс и Загрузка драйвера, у которых в поле rul указано правило SuspiciousFile или MaliciousFile.

Элементы на странице **Исключения для файлов**:

1) Название набора;

2) Отображение количества выбранных элементов;

3) Кнопка выбора элементов таблицы ( );

4) Элементы навигации и фильтрации;

5) Поле Комментарий;

6) Поле Дата создания/Автор;

7) Поле Последнее изменение/Пользователь;

8) Элементы активации/деактивации правила в наборе (/ ,);

9) Элементы поля **Управление** ( );

10) Кнопки применения конфигурации правил, копирования, экспорта и импорта ( ).

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение** и выбрать тип добавляемого исключения: **Файл** или **Хеш** (рис. 57).

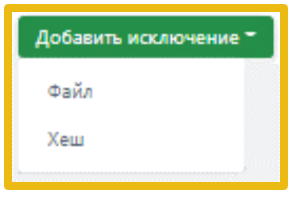


Рисунок 57 – Добавить исключение для файла (выбор типа)

Далее в открывшемся окне **Добавить исключение** необходимо заполнить поля с параметрами исключения. В зависимости от выбора типа исключения окно **Добавить исключение** будет содержать поля с различными параметрами.

Для типа **Файл** необходимо определить следующие параметры (рис. 58):

– Файл;

– Действие;

– установить значение опции **Не отправлять события**;

– если выбрано действие Блокировать, то установить значение опции **Блокировка действует и в контексте критических системных процессов**;

Важно

При срабатывании блокировки по исключению будет блокироваться критический системный процесс, что крайне опасно и может привести к блокировке всей работы и установке ОС в состояние «Синего экрана». При установке галочки в поле **Блокировка действует и в контексте критического системного процесса** аналитик должен осознавать, что он соглашается с тем, что описанное выше состояние допустимо и может произойти на хосте, для которого будет применяться данный индикатор.

– Для ОС Windows критическими системными считаются следующие процессы:

– 1) Процесс System (ядро ОС);

– 2) Процесс с ненулевым уровнем защиты (PPL, Windows 8.1+);

– 3) Trustlet-процесс Windows 10+ (https://learn.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes)

– 4) Процессы: csrss.exe, smss.exe, lsass.exe, services.exe, wininit.exe, winlogon.exe, logonui.exe, lsm.exe, sppsvc.exe (идентифицируются по полному пути);

– 5) Библиотека lsm.dll (идентифицируется по полному пути) внутри хост-процесса (svchost.exe).

– Комментарий.

Важно

Запись в поле **Комментарий** не должна превышать 32 тысячи 767 символов (байтов).

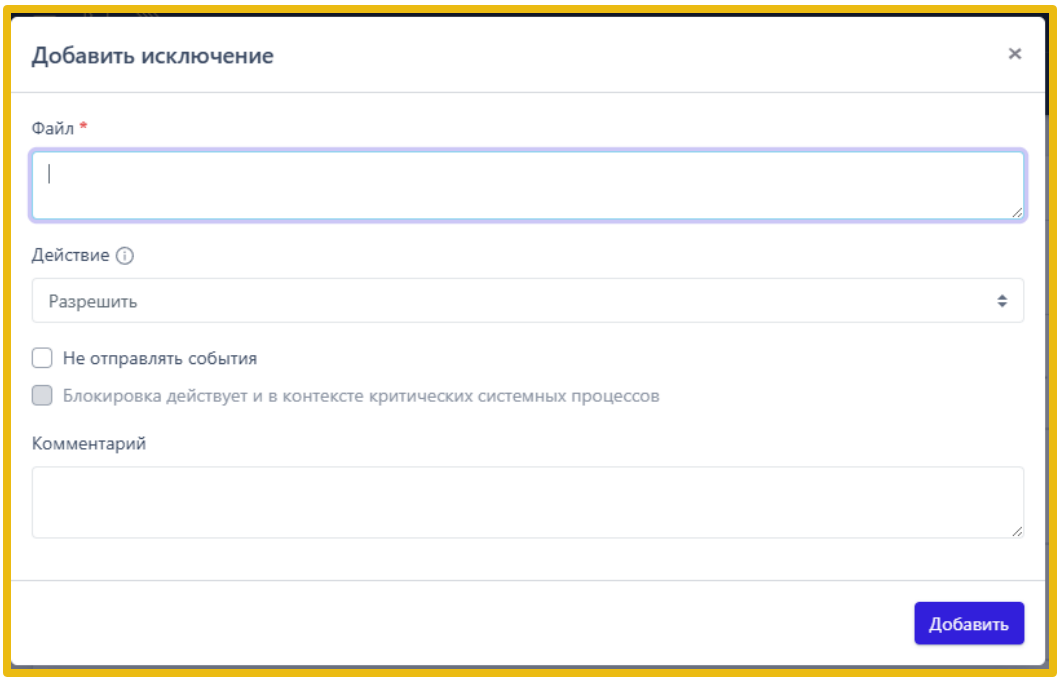


Рисунок 58 – Добавление исключения (файл)

Для типа **Хеш** необходимо определить следующие параметры (рис. 59):

– **Тип хеш-суммы** (SHA-256, MD5 или SHA-1);

– Хеш-сумма;

– Действие;

– установить значение опции **Не отправлять события**;

– если выбрано действие Блокировать, то установить значение опции **Блокировка действует и в контексте критических системных процессов** (если это требуется);

– Комментарий.

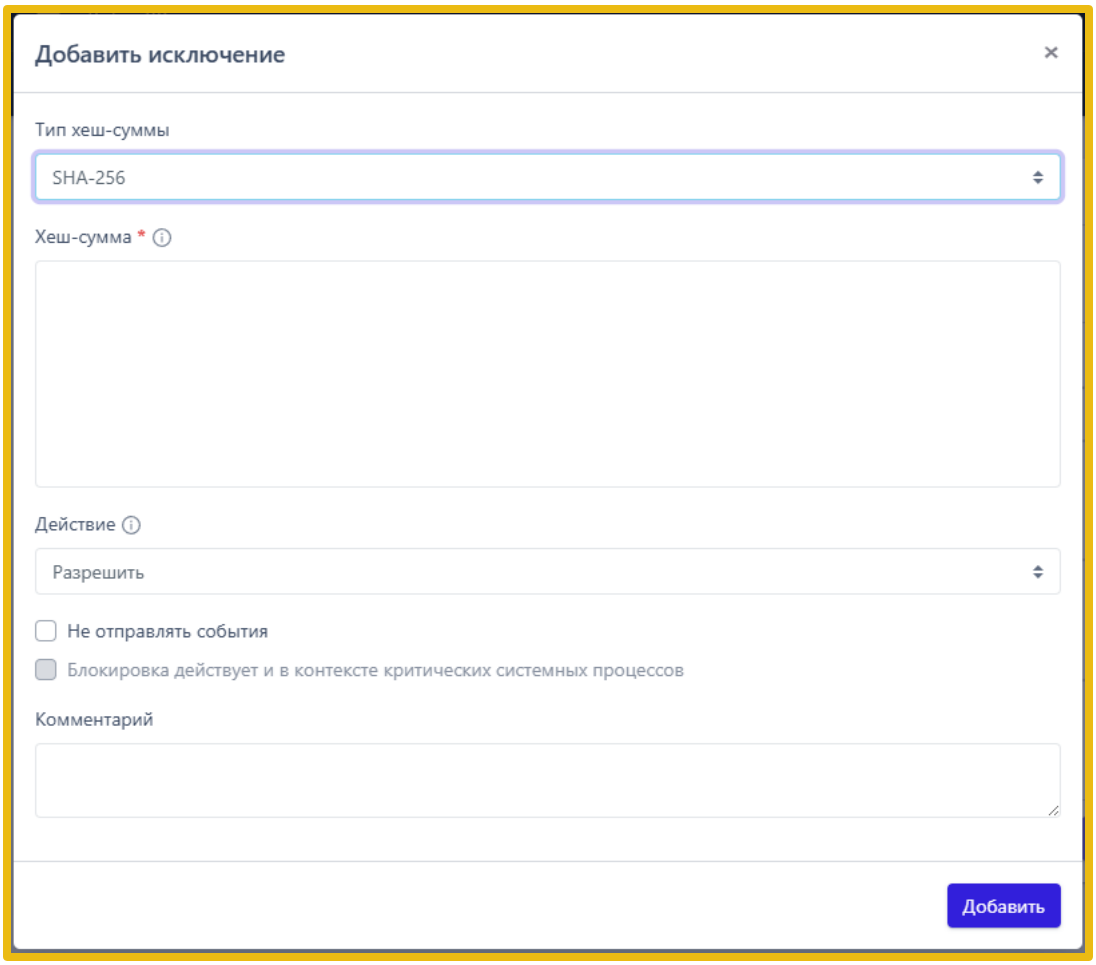


Рисунок 59 – Добавление исключения (хеш)

По умолчанию в Программе подсчитываются хеш-суммы по алгоритму SHA-256. Для подсчета хеш-сумм по алгоритмам SHA-1 и MD5 необходимо установить соответствующие флажки в профиле безопасности агента.

Файл – в поле прописывается имя файла или имя именованного канала, которое необходимо добавить в исключения. Имя файла или именованного канала после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Значение**. Поле является обязательным для заполнения, на что указывает значок *. Имя файла или имя именованного канала может задаваться с помощью регулярного выражения (файловые регулярные выражения Windows, допускающие использование символов ? для пропуска любого символа и * для пропуска последовательности символов любой длины, в т.ч. нулевой). Имя файла является менее точным способом подавления, его необходимо использовать в том случае, если имеется много экземпляров одной программы, на которой проявляется ложное срабатывание (рис. 60).

Важно

Имя файла или именованного канала не должно превышать 32 тысячи 767 символов (байтов).

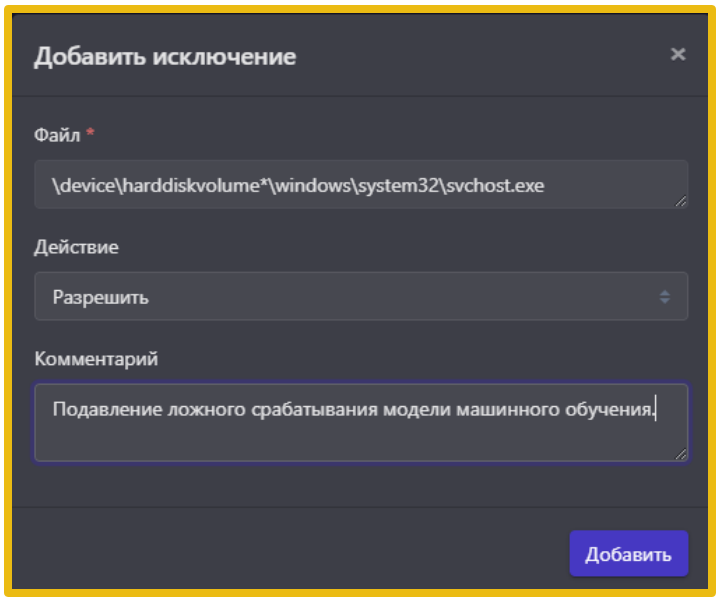


Рисунок 60 – Добавление исключения по файлу

Путь до файла должен быть указан в формате ссылки на устройство (как это выглядит на рисунке 60). Необходимо указывать максимально полное имя. Например, для исключения, представленного на рисунке 60, строка ***svchost.exe** (или **svchost.exe**) является менее удачным вариантом, так как для любого файла с таким именем будут подавляться статические проверки, чем могут воспользоваться злоумышленники. Иерархия пути здесь обеспечивает некоторую защиту от этого. Квантификатор * все еще оставляет злоумышленнику возможность в любой вложенной директории повторить часть пути **\windows\system32\svchost.exe** и для такого файла будут отключены статические проверки (пример такого пути **c:\temp\windows\system32\svchost.exe**). В связи с этим, если требуется исключение для файлов, расположение которых предполагается только на системном томе, необходимо в качестве ссылки на системный том использовать переменные окружения: **%systemdisk%**, **%systemdrive%**. Учитывая сказанное, для примера выше наиболее удачным вариантом указания пути до файла является: **%systemdisk%\windows\system32\svchost.exe**. Также необходимо отметить, что при обработке путей исключения регистр символов не учитывается.

Совет

Если в качестве файла добавить каталог в **Исключения для файлов** со статусом **Разрешено**, то для всех его элементов будет отключена проверка статического содержимого: по yara-правилам, ML, IOC по хешу (в т.ч. средствами TI-платформы). Кроме того, события, связанные с загрузкой DLL из этого каталога, не будут отправляться, если в профиле безопасности агента включен флажок **Исключить события загрузки известных модулей**

Действие – в поле устанавливается действие Программы в случае обнаружения файла с указанным именем или хеш-суммой. Предусмотрены следующие действия: **Блокировать, Разрешить**, **Продолжение наблюдения**. Выбранное действие после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Действие.** В случае с блокированием будет остановлен запуск файла. При этом поля **rsn** и **rul** в событии будут содержать информацию, определяющую, почему принято блокирующее решение.

Важно

Действие **Разрешить** означает, что в контексте события сработала логика «белого» списка, и то или иное действие было разрешено. При этом поля **rsn** и **rul** будут содержать информацию, определяющую, почему принято разрешающее действие. **Продолжение наблюдения** в контексте события телеметрии означает, что никакого действия, связанного с событием, не предпринято. В контексте обнаружения означает, что логика обнаружения не предписывает никакого действия, кроме фиксации самого факта обнаружения, следовательно обнаруженная активность не блокируется, что не отменяет самого факта ее обнаружения. При этом для события телеметрии поля **rsn** и **rul**, как правило (но необязательно), не заполняются, а для обнаружения поле **rul** содержит правило, идентифицирующее обнаружение, а поле **rsn**, как и в других случаях, содержит причину, по которой установлена такая реакция на обнаружение.

Опция **Не отправлять события** позволяет существенно изменить нагрузку по отправляемым событиям, связанным с тем или иным файлом, при этом необходимо учитывать, что сочетание выключенной опции и действия **Продолжение наблюдения** считается недопустимым, все остальные сочетания допустимы. Включение опции позволяет не отправлять события соответствующего типа на сервер.

Комментарий – в поле прописывается произвольный комментарий. Для добавления нового файла-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром. Комментарий после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Комментарий**.

Тип хеш-суммы – в поле устанавливается тип хеш-суммы файла. В Программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256**, **SHA-1** и **MD5** (при этом необходимо учитывать, что должна быть включена соответствующая опция в профиле безопасности агента). Тип хеш-суммы после добавления исключения отображается в таблице **Исключения для файлов** в поле **Тип**.

Хеш-сумма – в поле прописываются значения хеш-сумм для файлов, которые необходимо добавить в исключения. После добавления исключения значение хеш-суммы отображается в таблице **Исключения для файлов** в поле **Значение**. Поле является обязательным для заполнения, на что указывает знак * . Метод добавления исключения по хеш-сумме является более безопасным, чем метод добавления исключения по имени файла, так как основан на содержимом файла.

Важно

Можно добавить несколько хешей, по одному в каждой строке. Запись не должна превышать 32 тысячи 767 символов (байтов).

Чтобы завершить операцию добавления исключения, необходимо после ввода параметров в окне **Добавить исключение** нажать кнопку Добавить .

В поле **Значение** таблицы с исключениями для файлов отображается значок , который позволяет скопировать значение исключения в буфер обмена.

Для внесения изменений в исключение для файла необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключения для файлов** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

Удалить исключение можно, выбрав в таблице с исключениями необходимое правило и нажав кнопку .

В зависимости от типа исключения, которое можно увидеть в поле **Тип** таблицы **Исключения для файлов**, окно **Редактировать исключение** (рис. 61 и рис. 62) будет содержать разный набор полей, соответствующий окну **Добавить исключение** (см. рис. 58 и рис. 59).

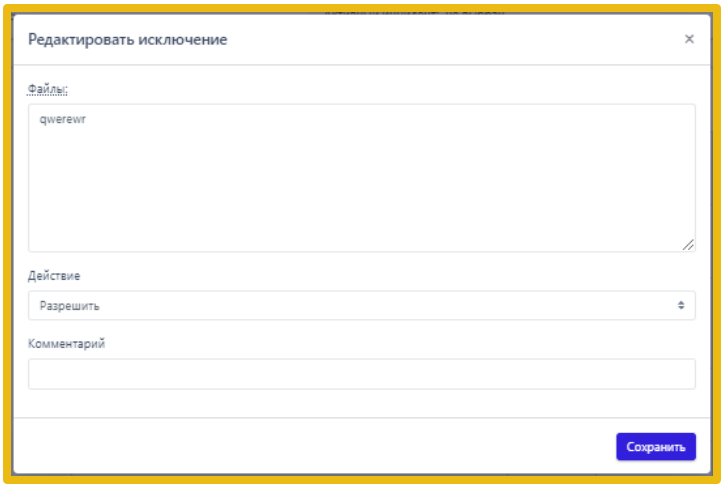


Рисунок 61 – Редактировать исключение (тип имя файла)

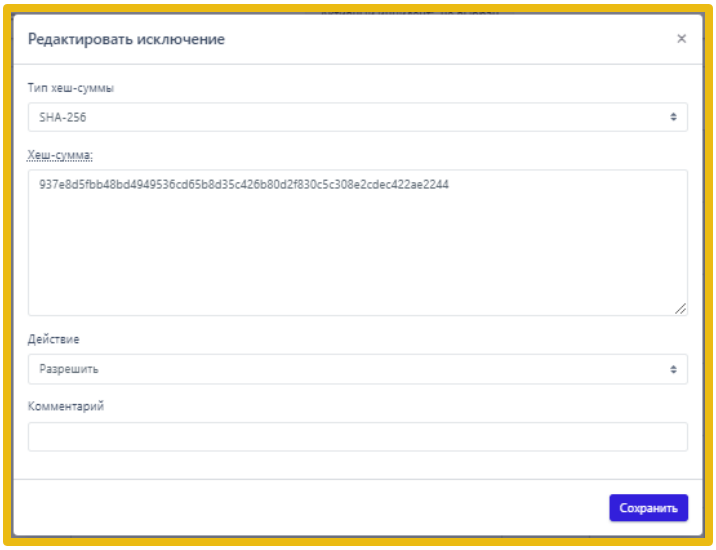


Рисунок 62 – Редактировать исключение (тип хеш-сумма)

Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений необходимо нажать кнопку **Закрыть окно** – ✕. После добавления файла в список исключений и сохранения набора с добавленным исключением необходимо передать этот набор для соответствующего агента или агентов.

Примечание

Если требуется применить конфигурацию с исключением сразу на несколько агентов, то для этого следует перейти на страницу **Агенты**, отметить флажком агентов, для которых нужно применить исключение, и с помощью кнопки **Применить конфигурацию** (⚙) назначить сохраненную ранее конфигурацию с исключением.

11.11.3. Исключения для программ

Исключения для программ – это программные элементы, которые позволяют управлять поведением процессов, управлять телеметрией и задействуют механизм идентификации программ. Это позволяет определить особенности исполнения программы.

Совет

При создании исключения необходимо руководствоваться общим принципом: чем точнее условия, описанные в исключении, тем лучше правило.

Чтобы аналитику добавить исключение для программы, ему необходимо перейти на страницу **Наборы исключений для программ**.

Для перехода к странице следует выбрать на панели управления раздел **Исключения для программ**. Здесь содержатся наборы с правилами, в каждый из них можно сохранить список исполняемых файлов, запуск которых должен соответствовать тем или иным настройкам безопасности. Для этого в Программе предусмотрена система флагов, устанавливающих параметры безопасности для исполняемых файлов. Исключающие флаги определяют, какие проверки необходимо выключить для указанного исполняемого файла и порождаемого им процесса.

В список исключений для программ можно вносить исполняемые файлы без настройки для них каких-либо определенных условий, задаваемых флагами. Наличие этой возможности позволяет аналитику настроить EDR для уменьшения количества ложных срабатываний, а в случае необходимости, заблокировать ту или иную программу в целях обеспечения безопасности.

Важно

При написании исключений для программ можно подавить срабатывание заданного индикатора атак для определенной программы или компонента, а можно и полностью отключить ту или иную категорию аналитики с помощью флага в блоке «Управление аналитикой», например, исключить анализ файловой активности – тогда для данной программы перестанут проверяться файловые индикаторы компрометации, YARA-правила, и не будет производиться анализ файловых артефактов средствами TI-платформы.

На странице **Наборы исключений для программ** пользователю доступны следующие операции:

– добавление новых наборов исключений (кнопка **Добавить набор**);

– редактирование имен наборов исключений ( );

– удаление выбранных наборов исключений (или кнопка **Удалить выбранные**);

– поиск по полям набора (поиск осуществляется внутри наборов по подстроке без учета регистра в полях **Значение**, **Издатель ЭП**, **Правила**, **Комментарий**);

– передача наборов агентам (применение изменений в наборе или во всех наборах на привязанных к ним агентах, кнопки и).

Для добавления программы в список исключений аналитику необходимо нажать ЛКМ на имени набора в поле **Название набора**, после чего откроется страница **Исключения для программ**. Информация о правилах с исключениями представлена в табличном виде.

Аналитику доступны те же операции, что и в разделе **Исключения для файлов** (см. пункт 11.11.2):

– добавление новых исключений;

– редактирование исключений;

– активация/ деактивация правила;

– копирование набора исключений;

– экспорт/импорт файлов с набором исключений;

– удаление исключений из набора.

Кроме того, на странице возможно осуществлять поиск по полям набора (поиск осуществляется по подстроке без учета регистра в полях **Значение**, **Издатель ЭП**, **Правила**, **Комментарий**).

Для добавления в набор нового исключения для программы необходимо нажать кнопку **Добавить исключение** и в открывшемся списке выбрать тип добавляемого исключения: **Файл**, **Хеш** или **Командная строка**.

Далее в открывшемся окне **Добавить исключение** необходимо установить параметры, в соответствии с которыми будет функционировать программа, внесенная в список исключений.

В зависимости от выбора типа исключения (**Файл**, **Хеш** или **Командная строка**) окно **Добавить исключение** будет содержать поля с различными параметрами.

Для типа исключений **Файл** необходимо определить следующие параметры:

– Файл;

– Флаги;

– Издатель ЭП;

– Правила;

– Комментарий.



Важно

Запись в поле **Комментарий** не должна превышать 32 тысячи 767 символов (байтов).

Для типа исключений **Хеш** необходимо определить следующие параметры:

– Тип хеш-суммы;

– Хеш-сумма;

– Флаги;

– Издатель ЭП;

– Правила;

– Комментарий.

Для типа исключений **Командная строка** необходимо определить следующие параметры:

– Командная строка прародителя;

– Командная строка родителя;

– Командная строка процесса;

– Флаги;

– Издатель ЭП;

– Правила;

– Комментарий.

Файл – в поле прописываются имена исполняемых файлов, которые необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для программ** в поле **Значение**, а в поле **Тип** будет указан тип исключения.



Важно

Правила указания имени файла при создании исключений для программ такие же, как и при создании исключения для файла. Т.е. регистр символов не учитывается, поддерживаются переменные окружения: **%systemdisk%**, **%systemdrive%**, допускается использовать символы ? и *, а также указывать имя файла программы без пути. Имя файла не должно превышать 255 символов (байтов).

Тип хеш-суммы – в поле устанавливается тип хеш-суммы исполняемого файла. В программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256**, **SHA-1** и **MD5**. Тип хеш-суммы после добавления исключения отображается в таблице **Исключения для программ** в поле **Тип**.

Хеш-сумма – в поле прописываются значения хеш-сумм для исполняемых файлов, которые необходимо добавить в исключения. После добавления исключения значение хеш-суммы отображается в таблице **Исключения для программ** в поле **Значение.** Хеш-значение является наиболее точным способом идентификации программ при создании исключений для программ.

Важно

Запись в поле **Хеш-сумма** не должна превышать 32 тысячи 767 символов (байтов).

Командная строка (прародителя, родителя и процесса) – в поле прописывается значение командной строки в соответствии с правилами записи, справка о правилах записи командной строки появляется при наведении курсора мыши на значок ⓘ (рис. 63).

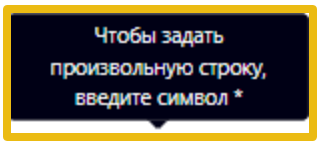


Рисунок 63 – Правила записи командной строки в исключениях для программ

Важно

Запись в поле **Коммандная строка процесса**, **родителя** или **прародителя** не должна превышать 32 тысячи 767 символов.

После добавления исключения значение командной строки отображается в таблице **Исключения для программ** в поле **Значение**. При создании правила на основе командной строки все 3 поля для ввода командных строк («Командная строка прародителя», «Командная строка родителя», «Командная строка процесса») являются обязательными.

Т.е. если мы хотим сделать правило для некоторой программы по командной строке её запуска, также необходимо указать командные строки запуска ее родительского процесса, а также прародительского. В случае, если значение каких-либо из указанных командных строк не важны, в качестве их значений следует использовать символ *(см. рис. 63).



Примечание

При использовании идентификации исключения на основе имени файла или командной строки необходимо стараться вводить как можно более полные значения путей и командных строк.

Путь \device\harddiskvolume*\windows\system32\svchost.exe является более безопасным, нежели *\svchost.exe (или просто svchost.exe).

То же касается и командных строк: “c:\Windows\System32\DISM.exe /Apply-Ffu /ImageFile:flash.ffu /ApplyDrive:\\.\PhysicalDrive0” – более безопасно, чем “c:\Windows\System32\DISM.exe *\\.\PhysicalDrive0”. И тем более, безопаснее варианта: “ *DISM.exe *\\.\PhysicalDrive0”. Пути для командных строк следует брать из соответствующего события, поскольку некоторые пути могут начинаться с префикса \??\. Могут быть и другие отличия. В правилах необходимо указывать именно так, как этот путь видит агент. Для командных строк переменные окружения не поддерживаются. Регистр символов, также, как и для путей, не учитывается.

Флаги – в поле определяются условия, согласно которым будут исполняться файлы, добавленные в список исключений для программ.

В Программе предусмотрены следующие типы флагов:

1) Управляющие поведением процессов (каждый флаг определяет право совершения процессом соответствующего потенциально опасного действия):

– разрешение внедрения кода в сторонние программы;

– разрешение записи памяти сторонних программ;

– разрешение чтения памяти сторонних программ и управления ими;

– право взаимодействия с критическими системными программами;

– разрешение прямого доступа к диску для чтения;

– разрешение прямого доступа к диску для записи;

2) Вспомогательные для механизма идентификации программ:

– компонент имеет 32-х битную и 64-х битную версию (позволяет одним правилом указать, что исключение относится и к версии программы, расположенной в директории System32, и к версии из директории SysWOW64);

– подтверждение по электронной подписи (позволяет указать, что действие разрешается для программы, исполняемый файл которой подписан любой валидной электронной подписью; для указания конкретного издателя необходимо использовать поле «Издатель ЭП» (при этом устанавливать флаг не обязательно, его наличие подразумевается автоматически));

– антивирусный компонент;

– запрет внедрения DLL;

3) Управляющие потоком телеметрии (позволяют для указанного процесса исключать из потока события указанного типа или разрешают отправку всех событий процессов, даже при включенной опции их подавления в профиле безопасности агента):

– исключение из телеметрии входящих сетевых событий;

– исключение из телеметрии исходящих сетевых событий;

– исключение из телеметрии файловых событий;

– исключение из телеметрии событий реестра Windows;

– исключение из телеметрии событий поведения;

– исключение всей телеметрии;

– запрет принудительного подавления событий;

4) Управляющие потоком аналитической активности (позволяют для указанного процесса исключить из потока события указанного типа, связанные со сработками аналитических правил):

– исключение анализа файловой активности (отключает срабатывание YARA-правил, индикаторов компрометации, также отключает срабатывание AMSI для выбранного процесса, если при этом отключена вся телеметрия для этого процесса);

– исключение анализа входящей сетевой активности;

– исключение анализа исходящей сетевой активности;

– исключение матчинга индикаторов атак;

– исключение анализа событий DNS.



Совет

Чтобы не создавалось событие сработки исключения для того или иного правила, необходимо указать его имя в строке **Правила**, поставив перед ним знак минус.

В случае с файловой активностью для заданной программы будут исключены проверки по индикаторам компрометации и YARA-правилам/ML, если режим сканирования по YARA-правилам и ML включен для соответствующего профиля. В этом же случае будут исключены проверки хешей на TI-платформе.

Для сетевой активности запрет аналитики для заданной программы отменяет проверку по индикаторам компрометации (IP, домены, сетевые сигнатуры), соответственно, на TI-платформе проверка по IP-адресам и доменам также будет отключена. Исключение матчинга индикаторов атак для заданной программы позволяет отменить для нее проверки по всем индикаторам атак, назначенным в конфигурации правил агента(ов).

Примечание

Написание в строке **Правила** идентификатора подавления **AMSI** приведет к отключению для указанного процесса проверок по AMSI.

Идентификатор подавления **ArwEngineEnable** отключает проверки Антишифра для выбранного процесса. Необходимо помнить, что с помощью **ArwEngineEnable** будет не только отключен модуль Антишифр для выбранного процесса, но и отключен модуль ремедиации, так как он является частью Антишифра.

Идентификатор подавления **RemEngineEnable** отключает ремедиацию для выбранного процесса, резервное копирование отключается и восстановление становится невозможным.

Идентификатор подавления **RemRegistry** отключает резервирование реестра на уровне отдельного процесса.

Идентификатор подавления **RemFiles** отключает резервирование файлов на уровне отдельного процесса.

Идентификатор подавления **SuppressIPCAnalysis** исключает обработку межпроцессного взаимодействия для выбранного процесса.

Все установленные для добавляемого исключения флаги будут отображаться в таблице **Исключения для программ** в поле **Флаги**.

Издатель ЭП – в поле прописывается имя издателя электронной подписи для исполняемого файла. После добавления исключения имя издателя отобразится в таблице **Исключения для программ** в поле **Издатель ЭП**. Добавление издателя электронной подписи к любому из доступных способов идентификации значительно повышает его безопасность.

Правила – используется совместно с флагом **Исключение матчинга индикаторов атак**. Если поле Правила оставить пустым, но при этом установить флаг **Исключение матчинга индикаторов атак**, подавляются срабатывания всех правил ИА для попадающих под исключение процессов.

В поле **Правила** прописывается название правила индикации, работу которого требуется подавить с помощью исключения для программ (например, «CmdLineTampering»). Правила «MaliciousFile», «SuspiciousFile», «MaliciousDomain», «SuspiciousDomain», «MaliciousIP», «SuspiciousIP», «MLStaticDetection» относятся к

срабатываниям на основе анализа содержимого файлов и подавляться должны с помощью файловых исключений. Сюда же относятся обнаружения на основе YARA-сигнатур, но имена таких правил указываются в метаданных YARA-сигнатуры, т.е. они не фиксированы. YARA-сигнатуры фигурируют в рамках единственного события файлового монитора – **Обнаружение: Файл классифицирован как вредоносный (YARA-правила)**.

Можно добавлять несколько правил и издателей через разделитель точка с запятой (;) без пробелов между ними.

Важно

Общие записи в полях **Издатель ЭП** и **Правила** не должны превышать 32 767 символов (байтов). При этом отдельное правило должно быть не больше 200 символов, а отдельный Издатель ЭП не более 63 символов.

Комментарий – в поле прописывается произвольный комментарий. Для добавления новой программы-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром. Комментарий после добавления исключения будет отображаться в таблице **Исключения для программ** в поле **Комментарий**.

Чтобы завершить добавление исключения для программы необходимо после ввода всей необходимой информации в окне **Добавить исключение** нажать кнопку **Добавить**.

Для внесения изменений в исключение для программы аналитику следует нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключения для программ** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

В зависимости от типа исключения, которое можно увидеть в поле **Тип** в таблице **Исключения для программ**, окно **Редактировать исключение** (рис. 64, 65, 66) будет содержать разный набор полей, соответствующий набору полей окна **Добавить исключение**.

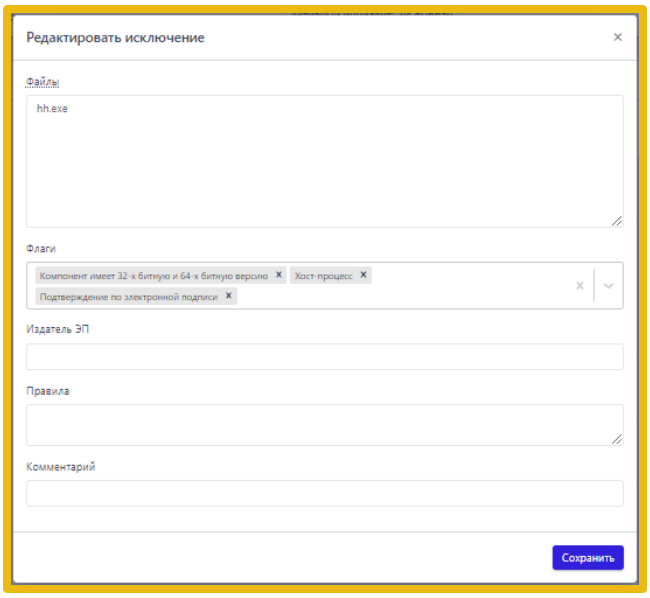


Рисунок 64 – Редактировать исключение для программы (файл)

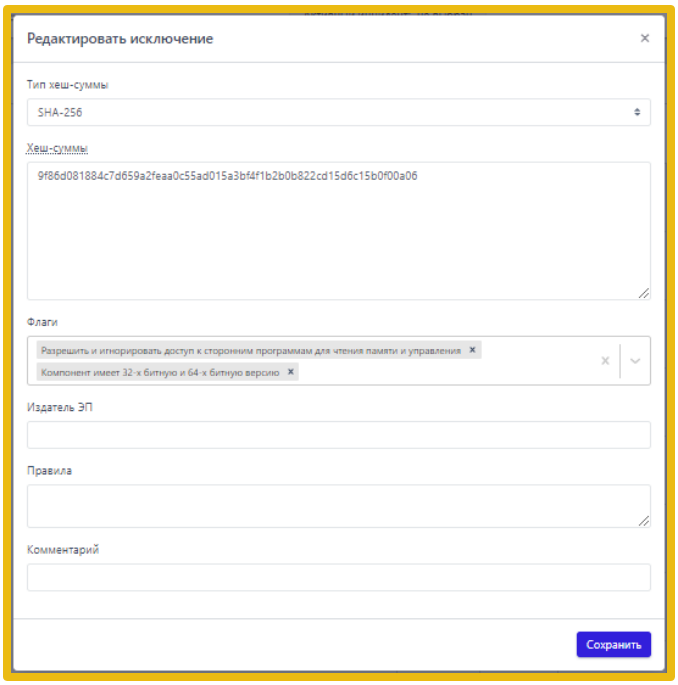


Рисунок 65 – Редактировать исключение для программы (хеш)

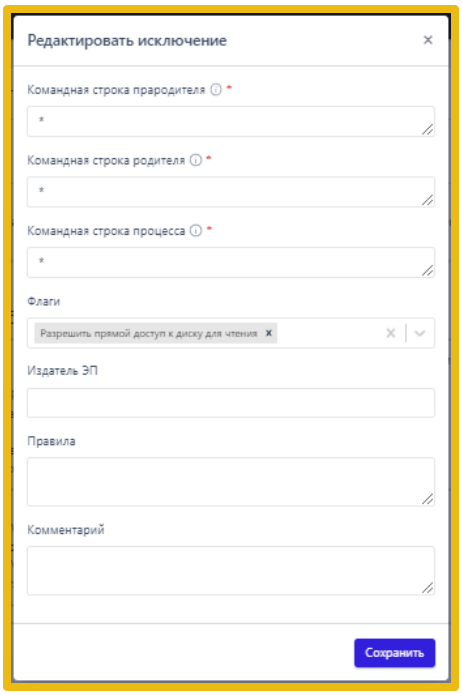


Рисунок 66 – Редактировать исключение для программы (командная строка)

Для завершения редактирования необходимо нажать кнопку Сохранить после внесения изменений в редактируемый элемент. Для отмены изменений следует нажать кнопку закрытия окна ✕.

После добавления программы в список исключений и сохранения набора с добавленным исключением необходимо применить этот набор для соответствующего агента или агентов.

Для этого следует перейти на страницу **Настройка агента**, выбрать нужного агента из списка и в области **Конфигурации** применить измененный набор исключений для программ (рис. 67).

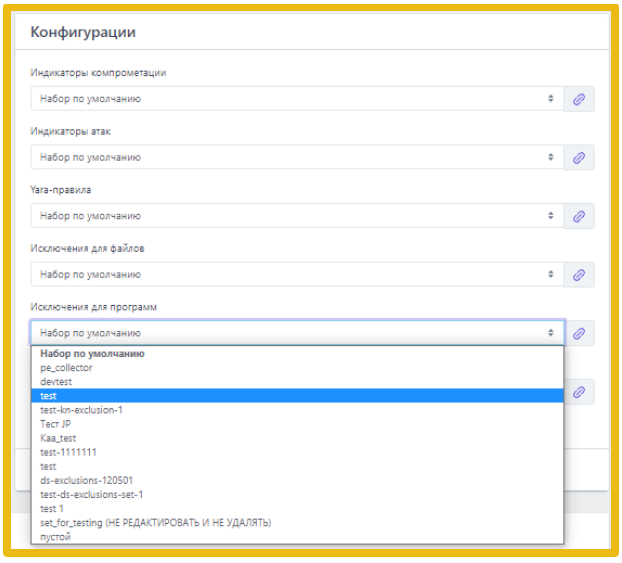


Рисунок 67 – Изменение конфигурации правил на агенте

Правило с добавленным исключением будет применяться для выбранного агента после применения конфигурации, для этого аналитику необходимо нажать кнопку 

. Если требуется применить конфигурацию с исключением сразу на несколько агентов, то для этого следует перейти на страницу **Список агентов**, отметить флажком агентов, для которых нужно применить исключение, и с помощью кнопки **Применить конфигурацию** ( ) назначить сохраненную ранее конфигурацию с исключением.

Следует также рассмотреть сценарий, когда с помощью управляющих флагов (**Разрешить внедрение кода в сторонние программы**, **Разрешить запись памяти сторонних программ**, **Разрешить доступ к сторонним программам для чтения памяти и управления**, **Право взаимодействия с критическими системными программами**, **Разрешить прямой доступ к диску для чтения**, **Разрешить прямой доступ к диску для записи**) необходимо разрешить определенное действие для хост-процессов.

К таким процессам в системе RT Protect EDR относятся:

– svchost.exe;

– rundll32.exe;

– dllhost.exe;

– taskhostw.exe;

– taskhost.exe.

Если действие, которое требуется разрешить, совершается самим этим процессом (инициатором соответствующего вызова является исполняемый модуль этого процесса), то все сказанное ранее про составление правила исключения остается справедливым. Если же действие совершается от имени определенной DLL, запускаемой с помощью хост-процесса, то в качестве правила идентификации должны использоваться либо имя, либо хеш этой DLL (инициатора операции).

11.11.4. Добавление исключений для файла с помощью мастера исключений

Добавлять исключения для файлов, обнаруживаемых на агентах, в Программе можно в автоматизированном режиме с помощью мастера исключений. Создание исключений для файла предусмотрено для следующих типов обнаружений (соответствуют названию правила, на основе которого событие попало в инцидент):

1) События-обнаружения монитора процессов с подтипом **Старт процесса**, у которых в поле **rul** указано правило **SuspiciousFile** или **MaliciousFile**;

2) События-обнаружения монитора процессов с подтипами Загрузка образа, Загрузка образа в сторонний процесс и Загрузка драйвера, у которых в поле rul указано MLStaticDetection;

3) События срабатываний YARA-правил;

4) События срабатываний индикаторов компрометации для файла;

5) События срабатываний ML на агенте.

Тем самым, создавая исключение, аналитик разрешает работу файла, несмотря на то, что статический анализ этого файла показывает потенциальную опасность для защищаемой инфраструктуры, это дает возможность аналитику быстро подавлять ложноположительные срабатывания.

Мастер исключений доступен на странице **Инцидент** в поле **Информация** события, включенного в инцидент, или на странице **Активность** также в поле **Информация**.

Чтобы добавить обнаруженный файл в исключения, необходимо нажать кнопку **Ложное срабатывание** (), после чего откроется окно **Мастер создания исключений**.

Здесь аналитику необходимо предпринять несколько шагов:

1) Выбрать тип создаваемого исключения (хеш или файл);

2) Выбрать набор с исключениями (по умолчанию выбирается действующий набор с исключениями того агента, на котором возник инцидент, при этом необходимо помнить, что создавать исключения во внешних наборах нельзя, такие наборы помечаются соответствующим значком);

3) Выбрать действие (по умолчанию выбирается действие **Разрешить**);

4) Написать комментарий (если это необходимо);

5) Нажать кнопку **Добавить**.

После завершения операции произойдет автоматический переход на страницу **Исключения для файлов** в тот набор, в котором было добавлено исключение.

В некоторых случаях аналитику вместо разрешающего исключения может понадобиться создать запрещающее исключение. От индикатора компрометации оно будет отличаться тем, что по такому событию инцидент создаваться не будет. Для создания блокирующего исключения необходимо вместо действия **Разрешить** выбрать в мастере исключений действие **Блокировать**.

11.11.5. Добавление исключений для программ в режиме мастера исключений

Подобно добавлению файлов в режиме мастера исключений программные исключения также можно добавлять с помощью мастера со страницы **Активность**. Использование мастера исключений для программ возможно для событий-обнаружений, у которых заполнено поле **rul**, кроме событий-обнаружений следующих типов:

– события-обнаружения файлового монитора с подтипами Срабатывание индикатора компрометации для файла, Файл классифицирован как вредоносный (ML на агенте) и Файл классифицирован как вредоносный (YARA-правила);

– события-обнаружения сетевого монитора с подтипом **Срабатывание индикатора компрометации**;

– события-обнаружения, у которых поле rul равно SuspiciousFile, MaliciousFile, SuspiciousDomain, MaliciousDomain, SuspiciousIp, MaliciousIp.

При обнаружении соответствующих событий на странице **Активность** в поле **Информация** появляется кнопка **Исключить как ложное срабатывание** ( ).

При нажатии кнопки открывается окно **Мастер создания исключения для программ** со следующими полями:

1) Тип создаваемого исключения;
2) Командная строка прародителя;
3) Командная строка родителя;
4) Командная строка процесса;
5) Издатель ЭП;
6) Правило (rul);
7) Комментарий;
8) Набор.

На этом этапе можно поменять тип создаваемого исключения с командной строки на файл. Обязательным для выбора является назначение набора с исключениями, при этом необходимо учитывать, что во внешние наборы сохранить исключение нельзя.

При выборе типа исключения **Файл** набор полей изменится на следующие:

1) Тип создаваемого подключения;

2) Файл (содержит полное имя файла);

3) Правило;

4) Комментарий (заполняется автоматически командной строкой процесса);

5) Набор.

После выбора типа создаваемого подключения и набора необходимо нажать кнопку **Далее**. Откроется окно **Добавить исключение**. На этом этапе можно установить флаги, согласно которым будут исполняться файлы, добавленные в список исключений для программ, а также изменить информацию в остальных полях (**Правила**, **Коммментарий** и т.д.). Для завершения операции необходимо нажать кнопку **Добавить**.

11.12 Добавление сетевых исключений

11.12.1. Общая информация

Сетевые исключения — это элементы Программы, позволяющие управлять списками глобальных и локальных IP-адресов и доменов с помощью переопределения логики событий, то есть разрешая или блокируя доступ к IP-адресам или доменам.



Важно

Блокирование сетевого соединения происходит на транспортном уровне.

Аналитик может задавать артефакты «черного» и «белого списков», где в «черный» список будут входить запрещенные IP-адреса или домены, а в «белый» список разрешенные, доступ к которым разрешается даже при наличии индикаторов компрометации или данных TI-платформы с вердиктом «Вредоносный». Использование сетевых исключений как элементов «белого списка» позволяет подавлять сетевые срабатывания TI-платформы или индикаторов и снижать количество анализируемой системой информации, так как при сетевом взаимодействии с элементами «белого списка» агент не анализирует данные потока (не производит матчинг сетевых сигнатур).

Блокирующие сетевые исключения («черный» список) позволяют ограничивать доступ к сетевым ресурсам без создания инцидентов.

На странице **Наборы сетевых исключений** представлены имена наборов исключений, в которых указываются IP-адреса, URL-адреса и доменные имена в качестве идентификаторов при создании исключений. Предусмотрены следующие действия при создании сетевых исключений для взаимодействия с перечисленными выше артефактами: **Блокировать, Разрешить (всегда)**, **Продолжение наблюдения**, **Разрешить (кроме изоляции)**.



Важно

Тип артефакта **URL** поддерживается не всеми версиями агента.

При создании сетевого исключения, действия, которые следует прописать в соответствующем поле имеют следующий смысл:

– **Блокировать** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем блокируется, при этом (в отличие от действия **Блокировать** в индикаторах) не создается событий с критичностью **Средняя** или выше, которые необходимы для создания инцидента, создается событие с критичностью **Низкая**;

– **Разрешить (всегда)** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем разрешается, при этом функциональность сохраняется даже тогда, когда агент изолирован);

– **Продолжение наблюдения** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем разрешается, при этом связанные с артефактом события создаваться и отправляться на сервер не будут);

– **Разрешить (кроме изоляции)** (означает, что взаимодействие машины, на которой установлен агент с указанным в исключении IP-адресом, URL-адресом или доменным именем разрешается, кроме того случая, когда машина, на которой установлен агент, находится в режиме изоляции.

Важно

Более специфичная запись сетевого исключения (более длинное доменное имя, комбинация с портом) имеет приоритет над менее специфичной.

11.12.2. Добавление сетевых исключений с помощью мастера исключений

Сетевые исключения могут быть добавлены со страниц **Активность** или **Инцидент** с помощью мастера исключений. Принцип его работы не отличается от создания файловых исключений: при нажатии кнопки открывается окно **Мастер создания сетевых исключений** с предзаполненными полями, в котором аналитик может изменить набор, куда будет сохранено исключение. После нажатия кнопки **Далее** открывается второе окно **Добавить исключение**, в котором необходимо выбрать одно из доступных для сетевых исключений действий в сочетании с опцией отправки событий.

Опция позволяет оптимизировать отправку событий, связанных со статическими проверками домена, URL-адреса или IP-адреса (проверка по индикаторам компрометации). Сочетание действия **Продолжать наблюдение** и отключенная опция **Не отправлять события** является невозможным.

Создать сетевое исключение возможно для следующих типов событий:

– события-обнаружения сетевого монитора с подтипом **Срабатывание индикатора компрометации**;

– события-обнаружения сетевого монитора с подтипом **Исходящее подключение** и **Входящее подключение**, у которых в поле rul указано **SuspiciousIp** или **MaliciousIp**;

– события-обнаружения сетевого монитора с подтипом Исходящее подключение, Входящее подключение, SSL HELLO, DNS-запрос, у которых в поле rul указано SuspiciousDomain или MaliciousDomain.

11.12.3. Наборы сетевых исключений

Страница **Наборы сетевых исключений** включает в себя следующие структурные элементы:

– таблица с наборами сетевых исключений;

– кнопка Добавить набор;

– кнопка Передать все наборы агентам;

– кнопка Удалить выбранные наборы;

– кнопка Редактировать;

– кнопка **Удалить**;

– кнопка Передать набор.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. На этом этапе можно добавить к новому набору исключения для файлов из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Для завершения операции необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Сетевые исключения** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

11.12.4. Страница «Сетевые исключения»

На странице **Сетевые исключения** можно выполнять следующие операции:

– просматривать сетевые исключения в выбранном наборе;

– добавлять новое исключение по IP-адресу;

– добавлять новое исключение по доменному имени;

– применять изменения в наборе исключений;

– копировать/перемещать выбранные исключения из одного набора в другой;

– экспортировать набор с исключениями в файл;

– импортировать исключения из файла в набор;

– активировать/деактивировать исключения в наборе;

– редактировать исключение;

– удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения.

При добавлении исключения необходимо обратить внимание на флаг **Не отправлять события**, который позволяет включить или отключить функцию отправки событий, связанных с доменом, URL или IP-адресом. При этом в комбинациях, предусмотренных для артефактов и флага **Не отправлять события** есть недопустимая комбинация: действие **Продолжение наблюдения** и отключенная опция **Не отправлять события**.

Важно

Домен и IP-адрес могут быть написаны в исключении вместе с портом (<IP/домен>:<порт>).

В одном исключении можно написать несколько доменов или IP-адресов, каждое новое значение следует писать в новую строку. Ввод в поле **Значение** (IP-адрес, домен или URL) ограничен тридцатью двумя тысячами символов.

Чтобы завершить операцию добавления исключения, после ввода параметров в окне **Добавить исключение** следует нажать кнопку Добавить.

В поле **Значение** таблицы с сетевыми исключениями отображается элемент , который позволяет скопировать IP-адрес, URL-адрес или доменное имя в буфер обмена.

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Сетевых исключений** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ).

Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** ( ).

Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** ( ). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( )

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ( ).

При добавлении/редактировании исключения, если в обязательном для заполнения поле было введено не валидное значение, появляется надпись о некорректно введенном значении (IP-адреса или доменного имени) и исключение не будет создано. Данное утверждение представлено на рисунке 68.

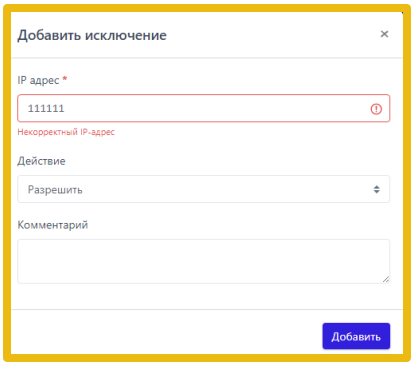


Рисунок 68 – Ввод некорректных параметров при добавлении исключения

11.13 Добавление исключений индикаторов атак

11.13.1. Общая информация

Исключения индикаторов атак – это программные элементы, позволяющие переопределить логику индикаторов атак, то есть исключить блокирующее или детектирующее действие при совпадении с условием исключения, способ подавить ложное срабатывание конкретного правила IOA в конкретном контексте, не отключая само правило глобально. Поскольку ИА-исключение полностью убирает событие, оно радикальнее,

чем исключение для программы (где событие фиксируется). Если важно сохранить видимость события в телеметрии, то иногда предпочтительнее использовать исключение для программ.

Исключение работает по имени и типу индикатора, к условию которого добавляется условие исключения, поэтому важно указывать правильные имя и тип индикатора атак, то есть имя и тип исключения индикаторов атак должны соответствовать имени и типу исключаемого индикатора.

В Программе предусмотрена возможность исключать группу индикаторов атак подстановкой символа *, например, soc_indicator* будет применяться для всех правил, в имени которых содержится часть soc_indicator. Кроме подстановочного знака * (любые символы или их отсутствие) в работе с исключениями для индикаторов атак может использоваться знак ? (один любой символ).

Исключения можно создавать только для индикаторов атак, созданных в режиме **Обычный**.

11.13.2. Наборы исключений индикаторов атак

Страница **Наборы исключений индикаторов атак** включает в себя следующие структурные элементы:

- таблица с наборами исключений для индикаторов атак;
- кнопка Добавить набор;
- кнопка Передать все наборы агентам;
- кнопка Удалить выбранные наборы;
- кнопка Редактировать;
- кнопка **Удалить**;
- кнопка Передать набор.

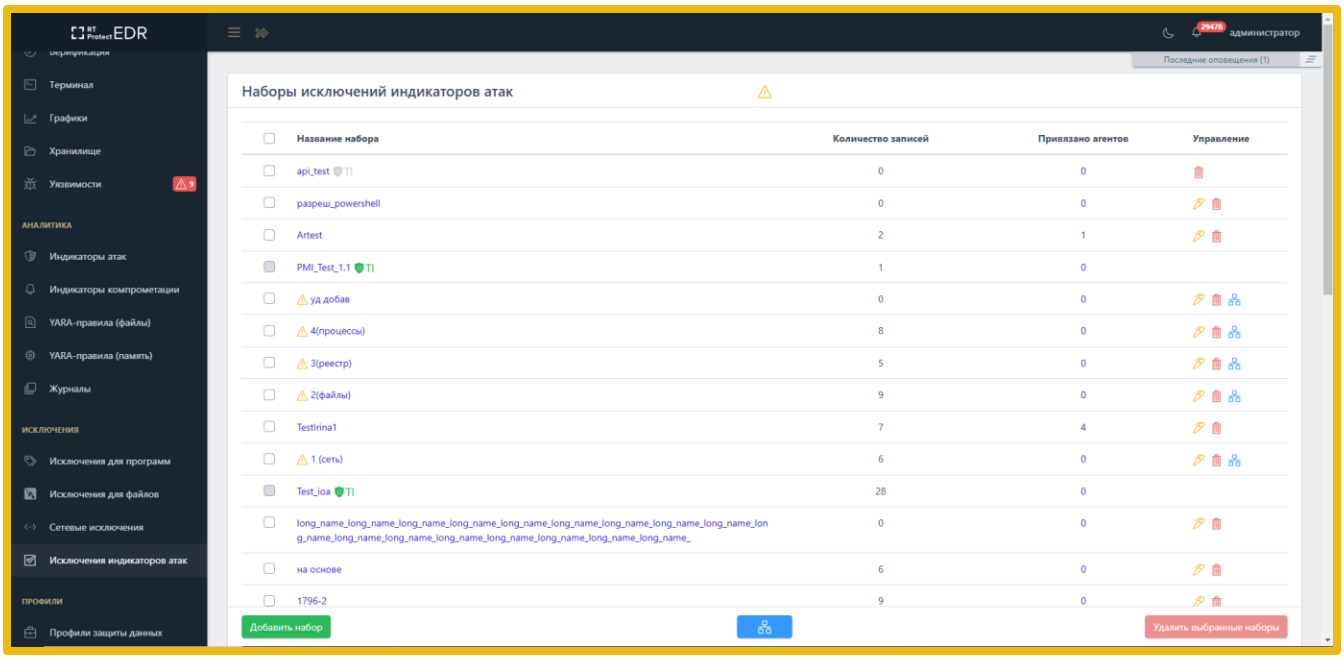


Рисунок 69 – Страница «Наборы исключений индикаторов атак»

Чтобы добавить новый набор с исключениями для индикаторов атак, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. На этом этапе можно добавить к новому набору исключения из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор.** Чтобы завершить операцию, необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Исключения индикаторов атак** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

11.13.3. Страница «Исключения индикаторов атак»

На странице **Исключения индикаторов атак** можно выполнять следующие операции:

– просматривать исключения индикаторов атак в выбранном наборе;

– добавлять новое исключение индикатора атак;

– применять изменения в наборе исключений;

– копировать/перемещать выбранные исключения из одного набора в другой;

– экспортировать набор с исключениями в файл;

– импортировать исключения из файла в набор;

– активировать/деактивировать исключения в наборе;

– редактировать исключение;

– удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения. Добавить условие исключения индикатора атак можно как вручную, так и с помощью конструктора. Также, как и для индикаторов атак, в исключениях для них доступна функция проверки синтаксиса.



Важно

При заполнении поля **Тип индикатора атаки** можно выбрать параметр **Универсальный тип индикатора**. При выборе данного параметра исключение будет действовать для всех типов индикаторов атак.

В списке исключений индикаторов атак в наборе тип исключения, созданного для универсального типа индикатора, будет отображаться как **Универсальный**.

Чтобы завершить операцию добавления исключения, после ввода параметров в окне **Добавить исключение** следует нажать кнопку Добавить.

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключений индикаторов атак** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ). Далее выбрать набор, в который будет копироваться выбранный элемент.

Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** ( ). Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** ( ). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( )

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ( ).

11.14 Особенности работы Программы с антивирусными средствами сторонних производителей

11.14.1. Общая информация

Антивирусные компоненты (процессы и модули), отмечаются в системе RT Protect EDR специальным признаком – AVEngine.

Этот признак учитывается, чтобы избегать конфликтов с антивирусами в следующих случаях:

– при контроле межпроцессного взаимодействия – чтение/запись памяти процессов и внедрении кода;

– при анализе файловой активности на предмет выявления вредоносных паттернов подсистемой защиты от вирусов-шифровальщиков;

– при срабатывании индикаторов компрометации – блокирующее действие переопределяется;

– при получении команды от TI-платформы на уничтожение процесса – команда переопределяется.

Также признак можно использовать, например, при написании индикаторов атак, чтобы переопределить логику индикатора для антивирусного ПО.

В остальном антивирусные процессы с точки зрения реагирования ничем не отличаются от других – например, если индикатор атак предписывает блокировать запуск процесса или пользователь отправляет команду на уничтожение процесса, то желаемое действие будет выполнено. Также запуск антивирусного процесса будет заблокирован, если его хеш или имя файла добавлено в перечень индикаторов компрометации или файловые исключения с действием **Запрещено**.

11.14.2. Срабатывание антивирусных средств при работе с веб-приложением RT Protect EDR

Срабатывание антивирусных средств при работе с веб-приложением EDR возникает в том случае, если в данных, получаемых фронтендом от сервера (в основном они приходят в формате JSON) содержится какая-то информация, которую антивирусное средство распознает как потенциально опасную. Это может быть хеш, имя файла, командная строка и т.д. (ниже такие информационные фрагменты называются артефактами).

Список экранов приложения, где высока вероятность срабатывания антивирусных средств:

– **Инциденты**, **Инцидент** (incidents, incident): внутри инцидентов могут содержаться артефакты;

– (!) любой экран (edr/*): в оповещении о новом инциденте содержится информация об инциденте (нотификации в правом верхнем углу);

– **Активность** (events): внутри событий могут содержаться артефакты;

– **Оповещения** (user-messages): внутри оповещений содержится информация об инцидентах;

– **Артефакты TI**: внутри событий могут содержаться артефакты;

– **Процесс** (process): в информации о процессе могут содержаться артефакты;

– **Журнал** (users-actions): в событиях журнала могут содержаться артефакты (внутри инцидентов и тд);

– отчет TI-платформы (ti): в отчете могут содержаться артефакты.

Список экранов приложения, где вероятность срабатывания ниже:

– **Уязвимости** (vuln): в информации об уязвимостях могут содержаться артефакты;

– **Хранилище** (storage): файлы могут определяться как вредоносные;

– **Агенты**, **Агент** (agents): из-за виджета сканера уязвимостей на экране **Агент**;

– **Терминал** (terminal): внутри команд могут содержаться артефакты;

– **Главная страница** (dashboard): в некоторых местах могут быть артефакты (например, топ-10 модулей);

– экраны наборов и элементов (config-set, config-item): внутри элементов наборов могут содержаться артефакты.

Список экранов приложения, где вероятность срабатывания можно считать нулевой:

– Пользователи (Users);

– Профиль пользователя (user-profile);

– **Группы** (groups);

– **Верификация** (verification);

– **Графики** (charts);

– **Дистрибутивы** (distributions);

– **Лицензия** (license);

– экраны профилей (profile);

– экраны множеств профилей и наборов (profiles, config-sets);

– экран сброса пароля (reset-password).



Важно

Таким образом, для полного исключения ложных срабатываний антивирусных средств при работе с веб-приложением EDR целесообразно добавить в исключения соответствующий домен/адрес полностью: <host/IP>/*.

11.14.3. Особенности выполнения действия блокирования для антивирусных решений.

В некоторых случаях к заблокированному модулю процесса может обращаться антивирусное средство. Для того, чтобы это было возможно, в Программе предусмотрено внутреннее исключение, которое создает событие для подобного обращения. Если событие блокирования возникает в контексте антивирусного процесса (такие процессы отмечаются в системе флагом AVEngine), то блокирующее действие переопределяется на **Продолжать наблюдение** и критичность события сбрасывается на уровень **Информация**,

при этом в причине события указывается **Исключение для программ**. Такая логика характерна для всех аналитических правил, кроме файловых исключений.

11.15 Операции со списком агентов

На странице **Агенты** пользователь Программы может выполнить следующие действия:

– скачать список агентов в формате CSV;

– фильтровать агентов с помощью фильтров, представленных на странице;

– добавить агентов в существующую или вновь создаваемую группу;

– передать конфигурацию с аналитическими наборами или профилями выбранным агентам;

– изолировать выбранных агентов или отменить изоляцию ранее изолированных агентов;

– отключить или включить автоматическое обновление выбранных агентов;

– включить или отключить защиту выбранных агентов (защитные функции драйвера будут включены/отключены);

– зафиксировать состав ПО выбранных агентов в качестве золотого образа;

– включить или отключить парольную защиту от удаления агентов;

– отключить отслеживание состава ПО выбранных агентов;

– установить или изменить критичность агента;

– выполнить команду для выбранных агентов;

– исключить выбранных агентов из определенной группы;

– удалить агентов из модуля администрирования (после удаления агент попадает на повторную верификацию);

– принудительно синхронизировать конфигурацию агентов;

– объединять агентов для дальнейшего изучения информации по ним по определенным признакам с помощью DSL-запросов;

Совет

Последнее может быть полезным аналитику, так как позволяет формировать выборки, исходя из сложного условия по активности, происходящей на агентах, например, DSL-запрос «sha256:x» покажет список агентов, на которых произошли события с указанным хешем x (поле sha256 события).

Также в качестве примера можно привести следующие выборки (рис. 70).

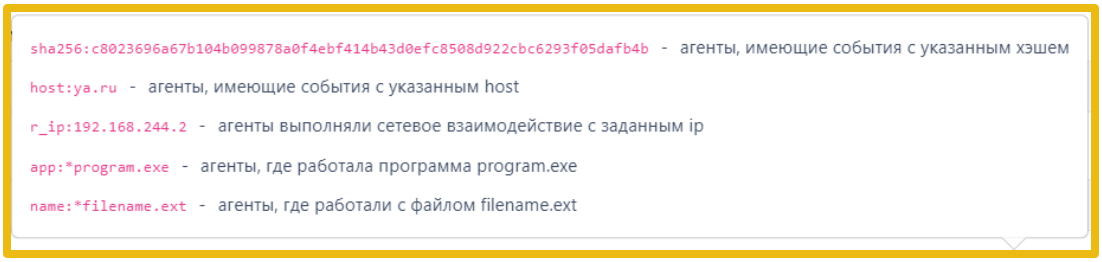


Рисунок 70 – Запросы DSL на странице «Агенты»

В результате отправки запроса формируется список агентов, на которых присутствует активность, соответствующая запросу. Это позволяет обнаруживать аномальную активность на агентах, определять, каких агентов затронули те или иные события или действия, выполнять команды для определенной группы агентов, для которой задан фильтр с помощью DSL-запроса.

Введенный DSL-запрос создает выборку над базой событий, из которой делается агрегация агентов, подлежащих отображению. При этом в поле **События** выборки по запросу пользователь может увидеть, сколько событий, соответствующих запросу, произошло на агенте. Нажимая на ссылку с количеством событий в поле **Совпадения по DSL**, пользователь сразу перейдет на страницу **Активность** с соответствующей фильтрацией по имени агента, DSL-запросом, а также трехмесячным периодом регистрации событий. Подробная информация о DSL-запросах приведена в подразделе 11.26.

На странице можно отследить состояния агентов при наличии на агентах ошибок (прикладных или системных). Для этого используется значок . Под прикладными ошибками понимаются ошибки службы, под системными – ошибки драйвера. При возникновении этих ошибок, необходимо собрать логи агента (команда **get-log**) и передать их представителям разработчиков Программы.

Совет

Чтобы убрать значок на агенте, необходимо выполнить для этого агента команду **reset-errors** в онлайн-терминале.

Чтобы добавить выбранных агентов в группу, необходимо отметить флажками нужных агентов и с помощью кнопки **Добавить в группу** выполнить одну из предложенных операций: добавить агентов в выбранную группу или добавить их во вновь создаваемую группу.

Команда особенно полезна, когда требуется объединить большое количество агентов по определенному признаку в группу, чтобы в дальнейшем применять групповые команды. Сначала с помощью настройки фильтров, например, отфильтровав всех агентов по домену, необходимо сформировать группы, к которым будут применяться команды, а потом уже применять различные команды для этих групп.

Чтобы применить конфигурацию с набором для определенных агентов, необходимо выбрать их, отметив флажками, после чего нажать кнопку **Применить конфигурацию** (). Откроется окно **Применение параметров конфигурации**, в котором нужно выбрать соответствующие наборы правил, исключений и профили, после чего нажать кнопку **Сохранить**. Кроме ручного назначения наборов можно воспользоваться шаблоном, ранее созданным в разделе **Конфигурации**, для этого необходимо выбрать соответствующий шаблон в строке **Шаблон конфигурации**, при этом будут заблокированы поля с выбором наборов.

По отношению к наборам, ранее привязанным к агентам, пользователь может выполнить следующие действия:

– заменить наборы;

– вставить наборы в начало (выбранные наборы будут поставлены перед ранее привязанными наборами), порядок наборов важен, так как анализаторы работают с первым одинаковым элементом из двух разных наборов, например, одному и тому же домену может быть присвоено в одном наборе действие **Разрешить**, а в другом **Блокировать**, соответственно, будет выполнено действие для домена из набора, проанализированного первым;

– удаление наборов (выбранные наборы будут удалены из списка ранее привязанных к агентам наборов).

Чтобы изолировать агентов, необходимо отметить их флажками, после чего нажать кнопку **Изолировать выбранных агентов** (), далее ввести произвольный комментарий в окне **Переход к изоляции агентов** и нажать кнопку **Отправить**. Изоляция агентов может эффективно работать в связке с DSL-запросом, например, когда известна информация о компрометации одного агента, то с помощью запроса можно определить, на каких еще агентах в сети был замечен артефакт компрометации и тут же изолировать скомпрометированные машины.

Для отмены изоляции необходимо отметить флажками выбранных агентов, после чего нажать кнопку **Отменить изоляцию выбранных агентов** () и подтвердить операцию в открывшемся окне, нажав кнопку **Выполнить**.

Чтобы отключить автоматическое обновление для выбранных агентов, необходимо отметить их флажками и нажать кнопку **Отключить автоматическое обновление выбранных агентов** (), после чего подтвердить выбранную операцию, нажав кнопку **Выполнить**. Для включения автоматического обновления необходимо отметить агентов флажками, после чего нажать кнопку **Включить автоматическое обновление выбранных агентов** () и подтвердить операцию, нажав кнопку **Выполнить**.

Чтобы включить защиту на агенте, необходимо отметить его флажком и нажать кнопку **Включить защиту выбранных агентов** (), после чего подтвердить операцию в открывшемся окне. При отключенной защите агент не блокирует действия, которые EDR считает опасными или потенциально опасными.

Чтобы отключить защиту на агенте, необходимо отметить его флажком и нажать кнопку **Отключить защиту выбранных агентов** (), после чего подтвердить операцию в открывшемся окне.

Важно

Отключение защиты на агентах приводит к выгрузке драйвера, поэтому события любых источников, кроме событий журналов, перестанут поступать на сервер для таких агентов.

Чтобы зафиксировать списки ПО на выбранных агентах (создать золотой образ), необходимо отметить агентов флажками и нажать кнопку **Зафиксировать состав ПО выбранных агентов в качестве золотого образа** (), после чего подтвердить операцию в открывшемся окне.



Примечание

Любое изменение состава ПО на таких агентах будет отмечено специальным значком (), который означает, что на агенте появились новые программы, не зафиксированные в составе ПО золотого образа. Просмотреть, что именно изменилось, можно после перехода на страницу **Агент** выбранного агента. Агенты с созданным золотым образом, состав ПО которых не менялся, будут отмечены значком  .

Чтобы отменить отслеживание состава ПО на агентах, необходимо отметить их флажками и нажать кнопку **Отключить отслеживание состава ПО выбранных агентов золотому образу** (), после чего подтвердить операцию в открывшемся окне. Информация об изменениях состава ПО для таких агентов перестанет отображаться на сервере управления.

Чтобы включить защиту от удаления для выбранных агентов, необходимо отметить их флажками и нажать кнопку **Включить защиту от удаления для выбранных агентов** (), после чего откроется окно **Включение защиты от удаления агентов**. Далее необходимо задать пароль и нажать кнопку **Отправить**. Удаление агента с компьютера, на котором он установлен, после завершения операции будет возможно только после ввода пароля. Чтобы увидеть и при необходимости скопировать пароль удалени) необходимо перейти на страницу удаляемого агента. Пароль будет показан аналитику при наведении курсора на значок  . Пароль для удаления будет установлен для выбранных агентов вне зависимости от того, устанавливался ли на одном или нескольких агентах пароль ранее, в таком случае пароль будет просто перезаписан.

Чтобы отключить защиту от удаления для выбранных агентов, необходимо отметить их флажками и нажать кнопку **Отключить защиту от удаления для выбранных агентов** (), после чего подтвердить операцию в открывшемся окне. Требование о вводе пароля при удалении агента будет снято.

Изменить критичность на выбранных агентах – чтобы изменить критичность на агентах, необходимо отметить флажком одного или нескольких агентов, после чего нажать кнопку  . Откроется окно **Изменение критичности агентов**, в котором следует выбрать необходимую критичность, после чего нажать кнопку **Применить**. Операция требует подтверждающего действия, для завершения необходимо нажать кнопку **Подтвердить** в открывшемся окне. Критичность влияет на то, как система реагирует при совпадении определенных событий. Например, при выборе критичности агента **Критичная** и обнаружении на агенте трендовой уязвимости (определяется на TI-платформе) происходит создание инцидента уязвимости.

Аналитик может выполнить команды онлайн-терминала на нескольких агентах одновременно, например, чтобы распространить какой-либо скрипт в пределах агентской сети или ее части с помощью команды **put**. Для выполнения команды необходимо отметить флажками агентов, после чего нажать кнопку **Выполнить команду на выбранных агентах** (). В открывшемся окне ввести соответствующую команду и нажать кнопку **Отправить**, после чего подтвердить операцию. Данный функционал является устаревшим и оставлен только для обратной совместимости с более ранними версиями агента. Для выполнения команд и реагирования в текущей версии агента используется кнопка **Реагирование для выбранных агентов** (). Функционал позволяет выполнить или запланировать задачу для выбранных агентов. Подробнее о задачах можно узнать в разделе 11.22.

Чтобы исключить агента из группы, необходимо отметить флажками агентов, состоящих в группе, после чего нажать кнопку **Исключить из группы**. Далее следует подтвердить операцию в открывшемся окне.

В таблице аналитик может выбрать произвольное количество агентов для проведения операций с ними, в том числе всех агентов на странице или всех агентов выборки. Чтобы выбрать всех агентов на странице, аналитику необходимо поставить флаг для кнопки выбора в первом столбце таблицы ().



Совет

Если требуется отметить всех агентов, показанных на всех страницах, то необходимо перевести переключатель **Выбрать все элементы** во включенное положение (). При этом переход на другую страницу переводит переключатель в выключенное положение.

Для удаления агентов необходимо отметить их флажками и нажать кнопку **Удалить выбранные**, после чего подтвердить операцию в открывшемся окне. Удаленные агенты не удаляются из системы полностью, а попадают на повторную верификацию.

Кнопка **Принудительно синхронизировать конфигурацию агента** () дает возможность пользователю синхронизировать конфигурацию профилей и наборов агента с конфигурацией, получаемой агентом с сервера (привязанную к агенту конфигурацию), если произошла какая-то нештатная ситуация и агент получил, например, неполную конфигурацию.

Аналитик может фильтровать информацию на странице **Агенты** по следующим полям фильтрации (рис. 71):

1) Показывать по;
2) Группа;
3) Домен;
4) Изоляция;
5) Активность;
6) Операционная система;
7) Имя компьютера;
8) Защита агента;
9) Агент;
10) Платформа;
11) Сетевой адрес;
12) Защита от удаления;
13) Автоматическое обновление;
14) Золотой образ;
15) Поля для фильтрации;
16) Запрос на языке DSL;

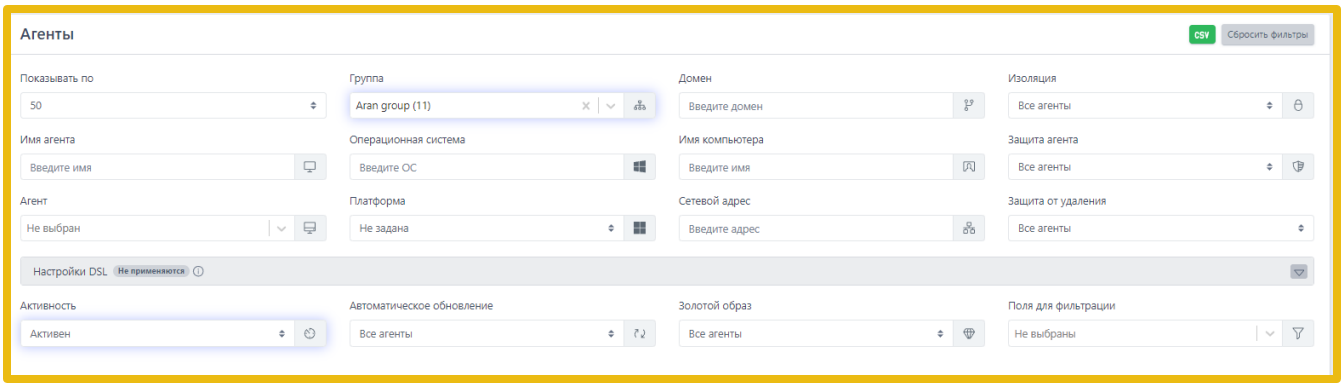


Рисунок 71 – Поля фильтрации в области «Агенты»

Показывать по – фильтр устанавливает количество событий, которые отображаются на странице в таблице. Возможно выбрать отображение по 10, 20, 50 или 100 событий.

Группа – фильтрует агентов по названию группы, к которой они принадлежат.

Домен – фильтрует агентов по имени домена, к которому принадлежат компьютеры, на которых установлены зарегистрированные в Программе агенты.

Изоляция – при выборе одного из значений фильтра (**Все агенты/Изолирован/Не изолирован**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению.

Активность – при выборе одного из значений фильтра (**Все агенты/Активен/Не активен**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению.

Операционная система – фильтрует агентов по установленной на них операционной системе.

Имя компьютера – фильтрует агентов по именам компьютеров, на которых установлены зарегистрированные в Программе агенты.

Защита агента – фильтрует агентов в соответствии с тем, включена на них защита или нет.

Агент – позволяет выбрать одного из представленных в списке агентов.

Платформа – фильтрует агентов в соответствии с выбранной операционной системой: Windows или Linux.

Сетевой адрес – фильтрует агентов по вводимому в поле фильтра сетевому адресу. Можно фильтровать по неполному соответствию.

Защита от удаления – фильтрует агентов по тому, включена ли на них защита от удаления или нет.

Автоматическое обновление – фильтрует агентов по признаку включенного или выключенного автоматического обновления.

Золотой образ – фильтрует агентов по тому, отслеживается ли на них изменения программного обеспечения или нет.

Поля для фильтрации – при выборе значений в фильтре Поля для фильтрации на страницу дополнительно могут быть добавлены следующие фильтры: **Опция /NO_DRIVER**, **Проблемный**, **Часовой пояс**, **Конфигурация**, **Критичность**, **Наличие открытых инцидентов**, **Артефакт**, **Режим работы**, **Наличие блокировок в рамках реагирования**, **Исключения для файлов**, **Исключения для программ**, **Сетевые исключения**, **Индикаторы компрометации**, **Журналы**, **YARA-правила (файлы)**, **YARA-правила (память)**, **Индикаторы атак**, **Исключения индикаторов атак**, **Профили Антишифра**, **Профили безопасности агента**, **Профили контроля USB**.

Опция /NO_DRIVER – позволяет фильтровать агентов в соответствии с тем, включен ли драйвер на агенте или нет (для агента с установленной опцией NO_DRIVER отсутствует возможность переводить машину с агентом в изоляцию, а также отсутствует защита. Защиту агента при выключенном драйвере также, как и изоляцию, невозможно включить.

Проблемный – фильтрует агентов по наличию на них ошибок или их отсутствию. Ошибки могут быть прикладные (в службе агента) или системные (в драйвере агента).

Часовой пояс – фильтрует агентов по определенному часовому поясу в различных форматах часовых поясов: EST, GMT, UTC и др.

Конфигурация – при выборе одного из значений фильтра (**Все агенты/Заданы не все настройки**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению. В случае, если выбрано значение **Заданы не все настройки**, то в таблице отображаются агенты с не полностью настроенными наборами и профилями.

Критичность – фильтрует агентов по их критичности, предусмотрено несколько уровней критичности агента: **Низкая**, **Ниже среднего**, **Средняя**, **Высокая**, **Критичная**.

Наличие открытых инцидентов – фильтрует агентов по наличию или отсутствию на них открытых инцидентов.

Артефакт – фильтрует агентов по типу и значению артефакта, это можеть быть SHA-256, IP-адрес или доменное имя.

Режим работы – фильтрует агентов по режиму работы, всего доступно два режима – режим ядра и eBPF (агент Linux). Агент Windows работает только в режиме ядра.

Наличие блокировок в рамках реагирования – фильтрует агентов по наличию на агенте блокировок запуска процесса по командной строке, блокировок доступа к файлу и блокировок доступа к сетевому эндпойнту. Наличие блокировок показано в таблице с агентами значком в поле **Состояние**. Чтобы снять блокировки с агента, необходимо воспользоваться командой block с соответствующими аргументами (см. пункт 11.2).

Исключения для файлов – фильтрует агентов по названию выбранного в поле фильтра набора исключений для файлов. В таблице будут представлены только агенты, привязанные к этому набору.

Исключения для программ – фильтрует агентов по названию выбранного в поле фильтра набора исключений для программ. В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация об исключениях для программ содержится в пункте 11.11.3.

Сетевые исключения – фильтрует агентов по названию выбранного в поле фильтра набора сетевых исключений. В таблице будут представлены только агенты, привязанные к этому набору.

Индикаторы компрометации – фильтрует агентов по названию выбранного в поле фильтра набора индикаторов компрометации. В таблице будут представлены только агенты, привязанные к этому набору.

Журналы – фильтрует агентов по названию выбранного в поле фильтра набора журналов. В таблице будут представлены только агенты, привязанные к этому набору.

YARA-правила (файлы) – фильтрует агентов по названию выбранного в поле фильтра набора файловых сигнатур, объектом сканирования при этом будут файлы. В таблице будут представлены только агенты, привязанные к этому набору.

YARA-правила (память) – фильтрует агентов по названию выбранного в поле фильтра набора файловых сигнатур, объектом сканирования при этом будет память. В таблице будут представлены только агенты, привязанные к этому набору.

Индикаторы атак – фильтрует агентов по названию выбранного в поле фильтра набора индикаторов атак. В таблице будут представлены только агенты, привязанные к этому набору.

Исключения индикаторов атак – фильтрует агентов по привязанным к ним наборам исключений индикаторов атак.

Профили Антишифра – фильтрует агентов по названию фильтра, выбранного в поле профиля Антишифра. В таблице будут представлены только агенты, привязанные к этому профилю.

Профили безопасности агента – фильтрует агентов по названию выбранного в поле фильтра профиля безопасности агента. В таблице будут представлены только агенты, привязанные к этому профилю.

Запрос на языке DSL представляет собой отдельную область на странице **Агенты**, в которой помимо строки запроса существуют дополнительные строки **Период регистрации**, **Источник события**, **Подтип события**. Подробную информацию о запросах DSL см. в пункте 11.26. На странице **Агенты** DSL-запрос позволяет выделить агентов, на которых происходили события, соответствующие запросу.

11.16 Операции на странице «Агент»

На странице **Агент** аналитик может управлять выбранным агентом и просматривать подробную информацию о его состоянии. Большинство операций, которые аналитик может выполнить для отдельного агента, совпадает с групповыми операциями. Для перехода к странице **Агент** необходимо кликнуть по имени агента в любом разделе Программы, содержащем имена агентов.

На странице **Агент** аналитик может выполнить следующие действия:

– просмотреть информацию о выбранном агенте (версия, часовой пояс, имя и т.д);

– просмотреть информацию о наличии на агенте системных или прикладных ошибок (значок  , в случае появления значка рекомендуется собрать логи агента и отправить их представителям производителя Программы);

– просмотреть количество событий и инцидентов на агенте за последнее время и за все время с момента его верификации;

– снять или установить параметр автоматического обновления агента при обновлении дистрибутива агента;

– удалить агента с сервера управления (в случае, если агент будет удален с сервера, но не будет удален с компьютера, на котором он установлен, агент пройдет автоверификацию и восстановится на сервере управления);

– выполнить операции по реагированию;

– включить/выключить защиту на агенте;

– отправить агенту команду через онлайн-терминал;

– зафиксировать состав ПО агента и отслеживать изменения в составе ПО;

– включить или выключить защиту от удаления агента;

– задать или изменить пароль для удаления агента;

– просмотреть информацию о количестве событий, приходящих с агента в секунду (EPS) на текущий момент и среднее EPS за последнюю неделю;

– просмотреть информацию о системе, в которой установлен агент;

– просмотреть информацию об установленном ПО на машине с агентом;

– просмотреть информацию об установленных драйверах;

– выявить уязвимости установленного ПО;

– назначить или изменить конфигурационные наборы с индикаторами, профилями или исключениями для агента;

– изменить группу, в которую входит агент;

– просмотреть информацию о запусках задач на агенте;

– просмотреть состояние агента (загрузка ЦП агентом и использование памяти);

– просмотреть графики, показывающие статистическую информацию по активности системы за последние 15 минут;

– создать отчет об агенте в формате pdf;

– узнать информацию о пяти последних пользователях, вошедших локально или дистанционно на компьютер с установленным агентом (кроме того, показывается и время входа);

– создать текстовое описание агента;

– просмотреть последние события в журнале агента (провайдера подсистемы ETW).

Значок рядом с индикатором активности агента (KM или eBPF) показывает, какой защитный компонент присутствует на агенте: компонент ядра или eBPF (технология в ядре Linux, позволяющая безопасно запускать программы в привилегированном контексте ядра, не изменяя его исходный код или загружая модули ядра).

Важно

Для агентов, у которых установлена опция с выключением драйвера, будет отсутствовать возможность переводить агента в изоляцию и включать защиту.

У агентов Windows всегда будет активен значок **Компонент ядра** (KM).

Кроме того, в случае наличия блокировок на агенте, в области **Агент** появится значок, предупреждающий о наличии блокировок на агенте (рис. 72). Просмотреть список блокировок можно с помощью команды block list в онлайн-терминале.

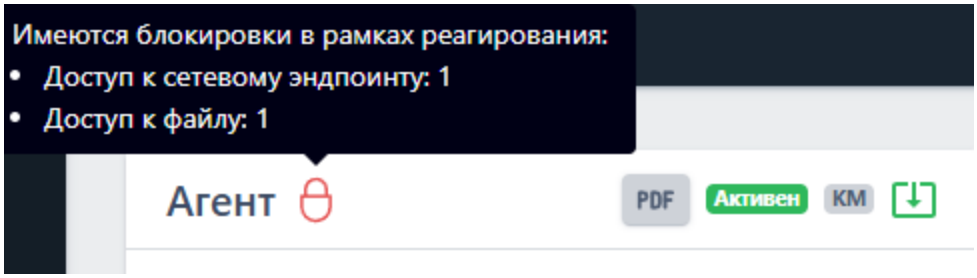


Рисунок 72 – Сообщение о наличии блокировок на агенте

11.16.1. Выполнение операций по реагированию

Операции по реагированию

На странице **Агент** пользователь может выполнить следующие операции по реагированию с помощью кнопки Реагирование :

1) Сетевая изоляция;
2) Отправить сообщение;
3) Блокировка запуска по командной строке;
4) Блокировка доступа к файлу;
5) Блокировка доступа к сетевому эндпойнту;
6) Загрузить файл в Хранилище;
7) Скачать файл из Хранилища;
8) Заблокировать сеанс пользователя;

9) Завершить сеанс пользователя

10) Выключить компьютер;

11) Собрать форензику;

12) Сканировать файловую систему.

13) Удалить файл/каталог.

Сетевая изоляция – операция реагирования позволяет отключить компьютер от сети, чтобы предотвратить распространение вредоносных программ в защищаемой инфраструктуре. Ограничение не распространяется на взаимодействие агента с административным модулем управления, то есть аналитик сможет отправлять команды агенту с помощью онлайн-терминала, планировщика задач или сценариев реагирования. Программа выполняет изоляцию агента в течение 5 секунд после отправки команды, после чего статус агента на странице **Агент** и в поле **Состояние** таблицы на странице **Агенты** поменяется на Изолирован .

На машине агента в этот момент в области уведомлений пользователю придет сообщение о том, что сеть агента изолирована (если соответствующие сообщения включены в Программе).

Отправить сообщение – операция реагирования позволяет отправить на компьютер с установленным агентом сообщение произвольного характера.

Блокировка запуска по командной строке – операция реагирования позволяет заблокировать запуск процесса по его командной строке. Описание командных строк поддерживает wildcard-символы (? и *). Пользователь может установить приоритет блокировки над исключениями, по умолчанию исключения имеют приоритет.

Блокировка доступа к файлу – операция реагирования позволяет заблокировать файл на компьютере с агентом, после чего любые действия с файлом станут недоступны до отмены блокировки. При этом пользователь сервера управления может выполнять любые действия с этим файлом с помощью онлайн-терминала. Пользователь сервера управления также заблаговременно может установить время действия блокировки в минутах, а также определить приоритет блокировки над исключениями, по умолчанию исключения имеют приоритет.

Блокировка доступа к сетевому эндпойнту – операция реагирования позволяет заблокировать на компьютере с агентом доступ к любой сетевой конечной точке (по доменному имени или IP-адресу). Пользователь может дополнительно выбрать порт, по которому будет блокироваться сетевое подключение, или

оставить значение порта по умолчанию (все порты). Также можно установить приоритет над исключениями, по умолчанию исключения имеют приоритет.

Загрузить файл в Хранилище – операция реагирования позволяет загрузить файл с хоста, на котором установлен агент, на сервер управления в раздел **Хранилище**, где файл можно исследовать с помощью программы просмотра или сохранить на компьютер, с которого осуществлен доступ на сервер управления. Загрузка файла объемом более 32 мегабайт требует установки специального флага при отправке команды.

Скачать файл из Хранилища – операция реагирования позволяет отправить на компьютер с агентом файл из раздела **Хранилище** сервера управления с помощью скопированной заранее ссылки на файл.



Важно

В Программе есть два вида ссылок: постоянная и временная. Постоянная ссылка требует указать имя файла, если имя файла не указывать, то его отправка не состоится.

Операция реагирования позволяет выбрать каталог размещения файла на агенте, если каталог не выбран, то файл будет отправлен по пути **C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\downloads**.

Заблокировать учетную запись пользователя – сценарий реагирования отключает учетную запись пользователя и запрещает ему вход в систему, сохраняя при этом все данные пользователя (профиль, файлы).

Заблокировать сеанс пользователя – сценарий реагирования блокирует компьютер с установленным агентом, активируя экран блокировки и требуя повторного ввода пароля для доступа. При блокировании сохраняются все запущенные приложения и открытые файлы. Действие реагирования аналогично нажатию Win+L на компьютере.

Завершить сеанс пользователя – сценарий реагирования находит на компьютере с агентом активную сессию выбранного пользователя и принудительно ее завершает, при этом несохраненные данные будут полностью потеряны и запущенные программы принудительно закрыты.

Выключить компьютер – сценарий реагирования выключает компьютер с агентом. Пользователь может установить время задержки перед выключением. По умолчанию задержки на выключение нет.

Собрать форензику – сценарий реагирования запускает Powershell-скрипт, сохраняющий различную информацию, которая может помочь при расследовании инцидента кибербезопасности. Сценарий сохраняет информацию в архивный файл в разделе **Хранилище**.

Сканировать файловую систему – сценарий реагирования сканирует выбранный каталог с помощью YARA-правил для файла, примененных на агенте.

Удалить файл/каталог – сценарий реагирования удаляет выбранный файл или каталог на компьютере с агентом.

Подробное описание механизма реализации функции сетевой изоляции со стороны агента.

Режим сетевой изоляции включается при получении агентом соответствующей команды от сервера управления EDR. С логической точки зрения сетевая изоляция подразумевает невозможность сетевого обмена с агентом (установку новых входящих/исходящих соединений и прием/передачу данных по установленным соединениям), кроме как со стороны сервера управления EDR с целью предотвращения утечки данных, распространения угрозы, связи с серверами управления злоумышленника, а также предотвращения других подобных проявлений при возникновении признаков потенциальной вредоносной активности на агенте.

С технической точки зрения сетевая изоляция распространяется на сетевые слои, начиная с транспортного и выше (согласно модели OSI), при этом также распространяется на ICMP-трафик (ping и др.) и реализуется драйвером агента за счет следующих мер:

1) Блокировка новых исходящих TCP-подключений (исходящий TCP-пакет SYN не отправляется с агентской машины);

2) Блокировка новых входящих TCP-подключений одним из 3-х методов (определяется настройками сетевого модуля агента):

– входящие TCP-пакеты SYN не доставляются до стека TCP/IP агента;

– в ответ на входящие TCP-пакеты SYN агент безальтернативно отправляет TCP-пакет RST;

– соединение устанавливается до момента первой попытки сетевого обмена, при возникновении которой соединение разрывается;

3) Принудительный разрыв соединения при возникновении попыток сетевого обмена (отправка/прием данных) в рамках уже установленных TCP-соединений соответствующая попытка блокируется (пакет не доставляется);

4) Блокировка входящих и исходящих UDP-пакетов (пакеты не доставляются).

Как следует из логики, описанной выше, если на момент включения режима сетевой изоляции TCP-соединение уже было установлено, но обмен данными по нему не происходил во время действия режима сетевой изоляции, то это соединение останется существовать, и после выхода из режима сетевой изоляции данные по нему снова могут беспрепятственно передаваться.

Кроме того, есть ряд исключений в части сетевого обмена, на которые не распространяется сетевая изоляция.

К ним относятся протоколы:

– NETBIOS;

– DHCP (в т.ч. IPv6-версия);

– LLMNR (определяются по TCP/UDP-порту).



Важно

Взаимодействие по указанным выше протоколам не прекращается даже в режиме сетевой изоляции агента, поскольку это критично для функционирования сетевого стека ОС (в частности, Windows).

11.16.2. Возврат к нормальному режиму работы после установки агента в режиме «no_driver»

Для возврата агента, который был установлен с опцией «no_driver», к нормальному режиму работы требуется выполнить следующие действия:

1) В модуле администрирования перейти в онлайн-терминал;

2) Выбрать агента, которому требуется изменить параметр;

3) Выполнить команду:

– enable;

4) Перейти на страницу агента и убедиться, что опция **Защита агента** включена.

Указанную выше команду можно выполнить для группы агентов на странице **Агенты** с помощью создания и запуска задачи с соответствующей командой ().

11.16.3. Отслеживание изменений состава ПО

Во многих случаях изменение состава ПО на компьютерах защищаемой инфраструктуры может сигнализировать о том, что на рассматриваемую систему выполняется установка нежелательных или вредоносных программ. В RT Protect EDR аналитик может создать золотой образ ПО на выбранном агенте, после чего отслеживать изменения состава ПО и установленных драйверов этого агента. Для этого аналитик может воспользоваться кнопкой **Управление** –  (управление золотым образом) на странице **Агент**.

По умолчанию для любого агента в защищаемой инфраструктуре золотой образ имеет статус **Не отслеживается**. Чтобы у аналитика была возможность отслеживать изменения золотого образа, ему необходимо нажать кнопку  и выбрать операцию **Зафиксировать и включить отслеживание**, после чего подтвердить выбранное действие.

После создания золотого образа в списках, представленных в разделах **Обновления системы**, **Установленное ПО** и **Установленные драйверы**, аналитику будут показаны все установленные программы и драйверы, а также обновления операционной системы, не соответствующие золотому образу. Значок  и зачеркнутое наименование элемента означает, что программа была удалена с компьютера с установленным агентом, но при этом присутствует в золотом образе. Значок  означает, что программа была установлена на компьютер с агентом, но при этом в золотом образе она отсутствует.

11.16.4. Настройка конфигураций с наборами

Для корректной работы конфигурации с исключениями, правилами, или профилями для того или иного агента необходимо назначить для него соответствующую конфигурацию и применить ее после назначения. Аналитические конфигурации могут содержать несколько наборов, например, наборы, получаемые с TI-платформы, и наборы, создаваемые в Программе.

На странице **Агенты** можно назначить конфигурационные наборы или профили для нескольких агентов с помощью кнопки **Применить конфигурацию** (), предварительно отметив агентов флажками.

После нажатия кнопки необходимо выбрать набор(ы) или профиль, после чего в открывшемся окне выбрать название набора(ов) или профиля, которые будут назначены агентам.

На странице **Агент** назначить конфигурационные наборы и профили для агента можно в области **Конфигурации** (рис. 73).

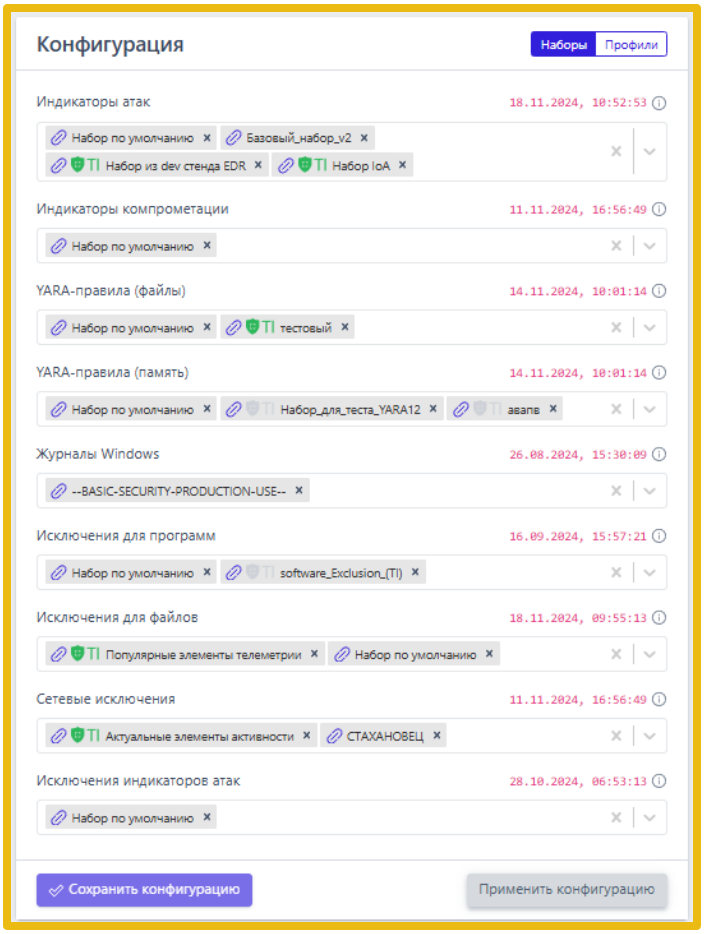


Рисунок 73 – Настройка конфигурации для агента

Конфигурации разделены по двум вкладкам: **Наборы** и **Профили**. Переключаясь между вкладками, можно настроить все необходимые конфигурации правил, исключений и профилей агента. Пустой конфигурация быть не может, в этом случае кнопка **Сохранить конфигурацию** становится неактивной. Помимо этого, на странице есть возможность применить конфигурацию, ранее созданную в разделе **Конфигурации**. Для этого используется кнопка **Применить конфигурацию**, при нажатии которой открывается окно **Применение параметров конфигурации**, где в строке **Шаблон конфигурации** можно выбрать ранее созданный шаблон.

В окне также предусмотрены следующие действия с наборами:

– заменить наборы;

– вставить наборы в начало (выбранные наборы будут поставлены перед ранее привязанными наборами;

– удаление наборов (выбранные наборы будут удалены из списка ранее привязанных к агентам наборов).

11.16.5. Защита на агенте

Еще одной важной операцией, которая доступна аналитику на страницах **Агент** и **Агенты**, является включение или отключение защиты (рис. 74).

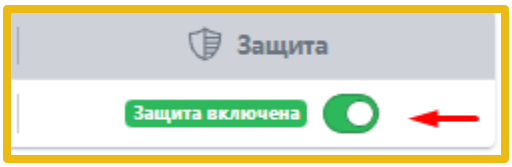


Рисунок 74 – Защита на агенте

Отключение защиты на агенте означает, что будут отключены защитные функции драйвера: не будут работать индикаторы компрометации, индикаторы атак, Антишифр, другие аналитические возможности, не будут присылаться на сервер события сетевой, файловой подсистемы, события модуля контроля USB, события реестра, сведения о процессах и события подсистемы Антишифр.

При этом агент отправляет статистику, события журналов, события сессий, вызовов, а также может принимать конфигурационные наборы и обрабатывать команды терминала, кроме команд **stop** и **memscan**. Программа уведомит о невозможности выполнить команду строчкой текста в терминале (рис. 75).



Рисунок 75 – Сообщение о невозможности выполнить команду в режиме без защиты

Отключение защиты может понадобиться в тех случаях, когда есть подозрения, что агент как-то влияет на работу системы. Чтобы не удалять агента, можно просто отключить его защиту.

Чтобы отключить защиту необходимо перевести ползунок в области **Защита агента** на странице **Агент** или с помощью кнопки  на странице **Агенты**.

11.16.6. Обновление агента

Обновление агента по умолчанию осуществляется в EDR автоматически. Для управления функцией обновления предусмотрена кнопка на странице **Агент** (рис. 76).

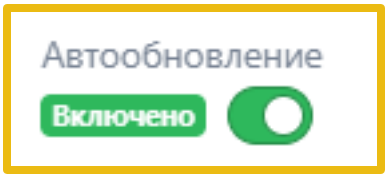


Рисунок 76 – Кнопка обновления агента

Операцию включения/отключения автоматического обновления необходимо подтверждать.

11.16.7. Защита от удаления агента

Режим защиты от удаления агента управляется на странице **Агент** модуля управления EDR. В Программе предусмотрена возможность включения/выключения режима и возможность установки/изменения пароля для удаления агента с конечной точки. После установки пароля удалить агента с помощью стороннего ПО становится невозможно, агент удаляется только с помощью утилиты uninstall.exe из состава дистрибутива агента, при этом какая-либо информация о пароле на машине с установленным агентом отсутствует, ее можно увидеть только на сервере управления EDR.

Защита от удаления агента на странице **Агент** включается ползунком в области **Управление**. Операция требует подтверждения в отдельном окне. Защита от удаления устанавливает на агенте парольную защиту, которая позволит удалить агента только после ввода пароля. Пароль задается аналитиком при включении защиты в отдельном окне, которое появляется после перевода ползунка в состояние **Защита включена**.

В Программе предъявляются следующие требования к паролю защиты от удаления:

1) Пароль не должен совпадать с именем или другой персональной информацией или быть слишком похожим на нее;

2) Пароль должен содержать как минимум 12 символов;

3) Пароль не может быть одним из широко распространённых паролей;

4) Пароль не должен состоять только из цифр.

После установки пароля для защиты от удаления агента в строке с ползунком появятся дополнительные значки управления паролем. Чтобы просмотреть его значение, необходимо навести курсор мыши на значок  . Скопировать пароль для удаления агента можно, нажав значок  . Изменить значение пароля можно, нажав значок  .

При удалении агента, защищенного от удаления паролем, Программа откроет окно, в котором необходимо будет ввести пароль, только после этого агент будет удален с компьютера. Это позволит избежать несанкционированного удаления агента с компьютера пользователем этой машины или злоумышленником.

11.16.8. Создание отчета об агенте в формате pdf

Чтобы создать отчет о функционировании агента, аналитику необходимо нажать кнопку **Скачать отчет в PDF** () в области **Агент**. Отчет сохранится в папку **Загрузки** (в папку, установленную для загрузок в браузере). Отчет может быть представлен в полном или кратком виде.

Отчет содержит различную информацию, связанную с активностью и статистикой работы агента: группа, ОС, версия агента, количество событий на агенте за сутки и за 15 минут, общее количество инцидентов, количество открытых инцидентов, число уязвимых программ на компьютере с установленным агентом и т.д.

11.16.9. Просмотр запусков задач для агента

На странице Агент аналитику доступен просмотр запусков задач агента, для этого необходимо раскрыть строку **Запуски задач агента**. В таблице будут показаны все запуски для агента, которые являются ссылками на страницу **Запуск**, где аналитик может просмотреть информацию о статусе и состоянии запуска, в том числе о запускаемой команде и ее выводе.

11.16.10. Просмотр событий, описывающих состояние агента

На странице **Агент** аналитику доступен просмотр событий, описывающих состояние выбранного агента. Аналитик может просмотреть последние события, для этого ему необходимо раскрыть их список с помощью кнопки **Показать** () в области **Состояние агента**.

Кроме списка событий в области отображаются графики с загрузкой центрального процессора службой и драйвером агента и с использованием памяти агентом. При этом пользователь может видеть нагрузку, которую создает драйвер агента на центральный процессор. Эта нагрузка отображается, как распределенная по подсистемам мониторинга:

1) Монитор процессов;
2) Монитор сети;
3) Монитор файлов;
4) Монитор реестра;
5) Подсистема индикаторов атак.

Также на странице отображается график **Тяжеловесные индикаторы/исключения, bps**, на котором отображается топ-5 индикаторов атак по нагрузке от общей нагрузки на ЦП механизма проверки индикаторов атак/исключений (bps (базисные пункты) – единица измерения доли времени ЦП, которое ИА-подсистема агента потратила на проверку конкретного индикатора атак или исключения, 10000 bps соответствует 100 процентам от нагрузки);



Совет

Если какой-то индикатор атак или исключение набирает несколько тысяч bps – это значит, что ИА или исключение создает значительную долю в общей нагрузке подсистемы на ЦП, и поэтому требует оптимизации.

Также на странице отображаются графики **Динамика подсчета хешей файлов** с количеством захешированных данных (показывает динамику операций хеширования данных, это может быть полезным при поиске аномалий в нагрузке на файловый монитор) и **Динамика сканирования файлов** с количеством просканированных данных (показывает, сколько данных просканировано с помощью глубокого сканирования).

В дополнение к вышеуказанной информации в разделе **Состояние агента** аналитик может просмотреть объем занятого места модулем ремедиации (Мбайт).

Аналитик может искать необходимые ему события в области **Состояние агента** по совпадению в поле **Описание события**, а также фильтровать события по уровням: критическая ошибка, ошибка, предупреждение, информация и подробно.

11.16.11. Просмотр графиков на странице «Агент»

На странице **Агент** возможно просматривать следующие графики, отображающие статистическую информацию об агенте:

– загрузка центрального процессора;

– загрузка памяти;

– количество запущенных процессов;

– количество нитей;

– количество дескрипторов;

– загрузка диска (на чтение);

– загрузка диска (на запись);

– загрузка сети (на передачу);

– загрузка сети (на прием);

– количество сетевых соединений.

11.17 Группы

Группировка агентов по определенным признакам, например, по домену, позволит выполнять групповые операции с агентами, для чего нужно будет просто отфильтровать их на странице **Агенты** по определенной группе.

В разделе **Группы** на странице **Группы агентов** можно выполнить следующие операции:

– просмотреть список групп агентов;

– создать новую группу агентов;

– редактировать название группы;

– удалить выбранные группы агентов.

Чтобы создать группу агентов на странице **Группы агентов**, необходимо ввести название в поле **Название группы**, после чего нажать кнопку **Создать группу**.

Для редактирования имени группы можно воспользоваться кнопкой **Редактировать группу** ( ). Откроется окно, в котором можно изменить название, после чего нажать кнопку **Сохранить изменения**.

Чтобы удалить группу или группы из модуля администрирования, необходимо отметить флажками соответствующие кнопки выбора и нажать кнопку **Удалить выбранные**. После подтверждения операции выбранные группы будут удалены.

При клике по имени группы произойдет переход на страницу **Агенты** с соответствующим предустановленным фильтром по имени группы, то есть в списке будут отображаться все агенты этой группы. На странице **Агенты** аналитик также сможет добавить агентов в группу или исключить агентов из нее (подробнее см. пункт 11.15).

11.18 Конфигурации

Раздел **Конфигурации** содержит редактируемые настройки наборов и профилей для агентов Windows и Linux, которые агенты получают в момент верификации. Можно настраивать несколько наборов в одной конфигурации. Кроме того, аналитик может настраивать собственные удаляемые и редактируемые конфигурации, которые могут использоваться в качестве шаблонов, распространяемых на агентов на странице **Агенты**.

Для новых агентов автоматически назначаются конфигурации с наборами по умолчанию. Такие конфигурации выделены желтым цветом на странице **Конфигурации** (для Windows и Linux).

Чтобы создать новую конфигурацию, необходимо нажать кнопку **Создать конфигурацию**. Откроется окно **Создание конфигурации**, в котором необходимо задать имя конфигурации и выбрать наборы и профили, после чего нажать кнопку **Создать**. Кнопка будет активна только в том случае, если будут назначены все наборы и профили конфигурации. При создании конфигурации можно выбрать ранее созданный шаблон для дальнейшего изменения конфигурации.

Важно

Порядок следования наборов имеет значение, потому что срабатывает первый обнаруженный анализатором агента элемент. Например, это важно в исключениях, когда один и тот же элемент добавлен в разные наборы с разным действием (блокировать и разрешить).

Конфигурации можно редактировать и удалять, при этом удалить используемые при верификации конфигурации по умолчанию для Windows и Linux нельзя. Чтобы редактировать конфигурацию, необходимо нажать кнопку . Чтобы удалить конфигурацию, необходимо нажать кнопку .

Администратор может работать со списком конфигураций с помощью фильтра по имени. Конфигурации сортируются на странице по алфавиту или по числовым и символьным значениям.

11.19 Комбинации наборов созданных правил аналитики, исключений и профилей

На страницах наборов элементов аналитики, исключений и профилей имеется иконка , с помощью которой можно перейти на страницу **Комбинации наборов**.

Указав в фильтре тип конфигурации (исключения для файлов, исключения для программ, и прочее), можно просмотреть комбинации созданных наборов данного типа.

Информация на странице представлена в виде таблицы со следующими полями:

– Иконка, раскрывающая дополнительную информацию ( );

– Комбинация;

– Файлы (указывается сколько вариантов комбинаций наборов имеется для данного типа конфигурации);

– Тип конфигурации.

При нажатии по иконке напротив каждой комбинации наборов открывается всплывающее окно, по примеру того, которое представлено на рисунке 77.

Код	Размер	SHA1	Дата создания
26	0 B	da39a3ee5e6b4b0d3255bfef95601890afd80709	25.07.2025, 11:42:39
25	48 B	9f783337b843cb5d7b59b041cbebb13d7d1fb2c1	25.07.2025, 11:42:39
24	46 B	210b85a1515f16972b4658c1d446b76cba8a9be6	25.07.2025, 11:42:39
23	149 B	35c3b13a35902ce4a9d83bdd274c7b8d80f3b90e	25.07.2025, 11:42:39
19	1.11 KB	2eaff1e72a78068cb27466fd4ab4c991541df28c	25.07.2025, 11:42:39

Рисунок 77 – Файлы комбинации наборов

В таблице выше в поле **Код** указывается код типа конфигурации, размер файла с набором в байтах с возможностью скачать файл, нажав по иконке , контрольная сумма файла с набором конфигурации и дата создания набора.

11.20 Уязвимости

Уязвимость – это недостаток программы, используя который, можно нарушить ее целостность и вызвать неправильную работу программы.

Просмотр результатов сканирования защищаемой инфраструктуры на наличие в ней уязвимостей осуществляется в разделе **Уязвимости**.

Сканирование уязвимостей осуществляется TI-платформой и позволяет проверить программное обеспечение на конечных точках с установленными агентами и выявить программы, защита которых ослаблена наличием известных и эксплуатируемых уязвимостей.

Примечание

Запрос на сканирование программы на наличие уязвимостей отправляется TI-платформе в случае обнаружения в RT Protect EDR нового ПО.

Сканер способен обнаруживать уязвимости из базы NIST (National Institute of Standarts and Technology), а также из базы данных угроз ФСТЭК (БДУ ФСТЭК).

Информация об установленном ПО на агенте обновляется при каждом запуске агента (старт компьютера, установка или обновление агента), но не реже одного раза в сутки в автоматическом режиме или принудительно по запросу, путем отправки агенту команды **inventory**.

Примечание

Информация о «железе» обновляется также при каждом запуске агента. Если меняется конфигурация сетевых интерфейсов или накопителей, то эта информация обновляется автоматически непосредственно в момент такого изменения.

Для специалиста, работающего с уязвимостями, важно обращать внимание на инциденты модуля уязвимости и критичность агента.

Под инцидентами подразумеваются сущности, возникающие в случае совпадения двух событий: на агенте присутствует программа, в которой есть «трендовая» уязвимость, а также критичность агента имеет значение «Критичная».

Трендовые уязвимости определяются аналитиками TI-платформы, а критичность агента устанавливается аналитиками RT Protect EDR. Критичным может быть агент, развернутый на важном хосте: контроллер домена, сервер с важной базой данных и т.д. Трендовая уязвимость в Программе помечается соответствующим значком ( ). Обычно под трендовыми подразумеваются такие уязвимости, которые активно используются злоумышленниками в данный момент времени и поэтому требуют особого внимания к себе со стороны сотрудников информационной безопасности.

Страница **Уязвимости** содержит диаграммы, на которых можно видеть результаты сканирования обнаруженных в защищаемой инфраструктуре программ, количество выявленных уязвимостей с разбивкой по критичности, а также покрытие агентов по наличию на них уязвимостей. Записи диаграмм **Программы** и **Уязвимости** кликабельны и позволяют перейти во вкладку **Программы** с соответствующей настройкой фильтрации полей.

Информация во вкладке **Инциденты** представлена в таблице, которая содержит следующие поля:

1) Инцидент (содержит название инцидента и CVE-идентификатор уязвимости);

2) Агент (показывает имя критичного агента, на котором содержится программа с трендовой уязвимостью);

3) Статус инцидента (активен, завершен автоматически или завершен вручную);

4) Программное обеспечение (название программы, в которой обнаружена трендовая уязвимость);

5) Время обнаружения;

6) Действия (содержит кнопку **Закрыть инцидент**  , для закрытых вручную инцидентов появляется кнопка **Переоткрыть инцидент** ).

Инциденты можно искать с помощью фильтров: **Статус**, **Агенты**, **Группы**, **CVE**. Настройки фильтра сбрасываются с помощью кнопки **Сбросить фильтры**. Клик по имени инцидента приводит к переходу на страницу, содержащую сведения об инциденте, сведения о программе, в которой найдена трендовая уязвимость, и сведения об этой уязвимости. В области **Сведения об инциденте** содержится кнопка **Закрыть инцидент** (). При закрытии инцидента необходимо указывать причину его закрытия, это может быть изменение критичности агента, обновление программы, закрывающее уязвимость или снятие с уязвимости аналитиком TI-платформы статуса трендовой.

Информация во вкладке **Программы** представлена в таблице, которая содержит следующие поля:

1) Имя;

2) Издатель;

3) Версия;

4) Агенты;

5) Уязвимости.

Программы в таблице можно фильтровать с помощью следующих фильтров:

1) Статус;

2) Агенты;

3) Группы;

4) Имя;

5) Издатель;

6) Критичность агентов;

7) Платформа (Windows или Linux);

8) Тип ПО, на котором выявлена уязвимость (это может быть Прикладное ПО или операционная система);

9) Критичность уязвимости (от низкой до критичной);

10) Признак трендовой уязвимости (трендовая или обычная);

11) Значение CVE.

12) Оценка CVSS V2 (не менее);

13) Оценка CVSS V3 (не менее);

14) Оценка CVSS V3.1 (не менее);

15) Оценка CVSS V4 (не менее).



Примечание

Для всех CVSS допускается значение от 0 до 10.

Настройки фильтров сбрасываются с помощью кнопки **Сбросить фильтры**.

Клик по имени программы в таблице вкладки **Программы** приводит к переходу на страницу, содержащую сведения о программе, в том числе об агентах, на которых эта программа присутствует, а также сведения обо всех обнаруженных в программе уязвимостях. Уязвимости отмечаются значками, показывающими степень критичности (– критичная, – высокая, – средняя, – ниже среднего, – низкая).

Клик по идентификатору CVE-уязвимости в таблице вкладки **Программы** позволяет посмотреть описание уязвимости и другую дополнительную информацию для перехода на страницу, содержащую сведения об уязвимости, в том числе список относящихся к ней CWE и количество программ, в которых уязвимость присутствует, необходимо нажать кнопку **Перейти к уязвимости**.



Примечание

В отличие от CVE, идентификатор CWE указывает не на конкретную уязвимость, а на общую проблему или недочет в программном обеспечении.

Кроме сведений об уязвимости страница содержит критерии соответствия уязвимости, ее описание, рекомендации по устранению, список агентов, на которых эта уязвимость обнаружена, а также список найденных в защищаемой инфраструктуре программ с этой уязвимостью.

Во вкладке **Уязвимости** одноименной страницы отображены все найденные уязвимости в защищаемой инфраструктуре. Информация представлена в таблице со следующими полями:

1) CVE;
2) Описание;
3) Агенты;
4) Инциденты;
5) Количество программ с выбранной уязвимостью (**Кол-во ПО**);
6) Создана (когда уязвимость была зарегистрирована).

Уязвимости можно фильтровать с помощью следующих фильтров:

1) Показывать по;
2) Критичность;
3) Агенты;
4) Группы;
5) Признак трендовой уязвимости;
6) Критичности агентов;
7) CVE;
8) Оценка по CVSS V2 (не менее);
9) Оценка по CVSS V3 (не менее);
10) Оценка по CVSS V3.1 (не менее);
11) Оценка по CVSS V4 (не менее).

Для сброса всех установленных фильтров необходимо нажать кнопку **Сбросить фильтры**.

11.20.1. Формирование отчетности на странице с уязвимостями

Аналитик может сформировать отчет о найденных на агентах уязвимостях и сохранить этот отчет на компьютер, с которого осуществляется доступ к серверу управления. Отчет формируется на странице **Управление уязвимостями** во вкладке **Программы**. Чтобы сохранить отчет в формате csv, необходимо нажать кнопку  , после чего отчет будет доступен в папке **Загрузки** или в другой папке, указанной в настройках браузера.

В отчете отображается полный список ПО на просканированных агентах, в котором присутствуют программы с найденными уязвимостями. Отчет формируется с учетом применяемых на странице фильтров.

11.20.2. Распространенность программы с уязвимостью в защищаемой инфраструктуре

Чтобы получить информацию о распространении программы с уязвимостью в защищаемой EDR инфраструктуре, аналитику необходимо перейти в раздел **Программы** страницы **Управление уязвимостями**, после чего кликнуть по имени программы. Откроется страница с разделом **Сведения о программе**, в котором в поле **Агенты с уязвимостью** можно просмотреть все хосты с установленными агентами, на которых обнаружена программа.

11.20.3. Изучение сведений об уязвимости

С помощью модуля сканирования уязвимостей аналитик может изучить подробную информацию о найденной уязвимости и определить способы нейтрализации этой уязвимости.

Для этого на странице **Сведения об уязвимости** публикуется ее описание на английском языке, а также описание на русском языке, если указанная уязвимость присутствует в БДУ ФСТЭК. Кроме того, на странице публикуется информация о базовых метриках, описанных по стандартам CVSS 4.0, CVSS 3.x и CVSS 2.0.

CVSS – это общая система оценки уязвимостей, которая позволяет сравнивать уязвимости программного обеспечения с точки зрения их опасности.

Базовые метрики описывают характеристики уязвимости, не меняющиеся с течением времени и не зависящие от контекста, то есть среды исполнения (например, вид операционной системы, в которой исполняется программа).

В зависимости от времени публикации информация по той или иной версии CVSS в сведениях об уязвимости может отсутствовать.

Базовые метрики, отображаемые на странице **Сведения об уязвимости** и их возможные значения представлены в таблице 56.

Таблица 56 –Базовые метрики уязвимостей

Стандарт	Метрики	Описание	Значения метрики
CVSS 4.0	Вектор атаки (AV)	Показывает удаленность потенциального атакующего от уязвимого объекта. Предполагается, что число потенциальных злоумышленников при доступе через сеть, больше, чем число потенциальных злоумышленников, которые могут использовать уязвимость, требующую физического доступа к устройству, и поэтому сетевой вектор требует более внимательного подхода	Сетевой (N)
			Смежная сеть (A)
			Локальный (L) (атакующему требуется локальная сессия)
			Физический (P) (атакующему требуется физический доступ к уязвимой системе)
	Сложность атаки (AC)	Эта метрика фиксирует измеримые действия, которые должен предпринять злоумышленник, чтобы активно обойти существующие встроенные механизмы повышения безопасности, чтобы получить рабочий эксплойт.	Высокая (H)
			Низкая (L)
	Требования к атаке (AT)	Эта метрика фиксирует предварительные условия развертывания и выполнения или переменные уязвимой системы, которые делают возможной атаку. Они отличаются от методов/технологий повышения безопасности (см. Сложность атаки), поскольку основная цель этих условий не в том, чтобы явно смягчать атаки, а, скорее, возникать естественным образом как следствие развертывания и работы уязвимой системы.	Отсутствуют (N)
			Присутствуют (P)
	Уровень привилегий (PR)	Эта метрика описывает уровень привилегий, которыми должен обладать злоумышленник для успешного использования уязвимости. Метод, с помощью которого злоумышленник получает привилегированные учетные данные для атаки (например, учетные записи с бесплатной пробной версией), выходит за рамки этой метрики.	Без привилегий (N)
			Низкий (L)
			Высокий (H)
	Взаимодействие с пользователем (UI)	Эта метрика фиксирует требование к пользователю, помимо злоумышленника, участвовать в успешной компрометации уязвимой системы. Эта метрика определяет, может ли уязвимость быть использована исключительно по воле злоумышленника или должен ли отдельный пользователь (или инициированный пользователем процесс) участвовать каким-либо образом. Результирующий балл наибольший, когда взаимодействие с пользователем не требуется	Не требуется (N)
			Пассивное (P)
			Активное (A)
	Конфиденциальность (VC/SC)		Высокий уровень воздействия (H)
			Низкий уровень воздействия (L)

Стандарт	Метрики	Описание	Значения метрики
		Конфиденциальность относится к ограничению доступа к информации и ее раскрытию только для авторизованных пользователей, а также к предотвращению доступа или раскрытия информации неавторизованным лицам. Результирующий балл наибольший, когда потери для системы наиболее высоки.	Воздействие отсутствует (N)
	Целостность (VI/SI)	Метрика измеряет то, как успешно реализованная уязвимость влияет на уровень целостности. Целостность системы нарушается, когда злоумышленник вызывает несанкционированное изменение системных данных. Целостность также нарушается, когда пользователь системы может отказаться от критических действий, предпринятых в контексте системы (например, из-за недостаточного ведения журнала). Результирующий балл наибольший, когда последствия для системы наиболее высоки.	Высокий уровень воздействия (H)
			Низкий уровень воздействия (L)
			Воздействие отсутствует (N)
	Доступность (VA/SA)	Эта метрика измеряет влияние на доступность пораженной системы в результате успешно использованной уязвимости. В то время как метрики влияния на конфиденциальность и целостность применяются к потере конфиденциальности или целостности данных (например, информации, файлов), используемых системой, эта метрика относится к потере доступности самой пораженной системы. Результирующий балл наибольший, когда последствия для системы наиболее высоки.	Высокий уровень воздействия (H)
			Низкий уровень воздействия (L)
			Воздействие отсутствует (N)
CVSS 3.x	Вектор атаки (AV)	Показывает удаленность потенциального атакующего от уязвимого объекта	Сетевой (N)
			Смежная сеть (A)
			Локальный (L) (атакующему требуется локальная сессия)
			Физический (P) (атакующему требуется физический доступ к уязвимой системе)
	Сложность атаки (AC)	В зависимости от количества условий для проведения атаки, ее сложность увеличивается (чем больше условий, тем выше сложность)	Высокая (H)
			Низкая (L)
			Высокий (H)

Стандарт	Метрики	Описание	Значения метрики
	Уровень привилегий (PR)	Показывает, требуется ли аутентификация для атаки, и если требуется, то какая	Низкий (L)
			Не требуется (N)
	Взаимодействие с пользователем (UI)	Требуются ли действия со стороны пользователей атакуемой системы	Требуется (R)
			Не требуется (N)
	Влияние на другие компоненты системы (S)	Оказывает ли влияние атакуемая подсистема на другие компоненты	Не оказывает (U)
			Оказывает (C)
	Влияние на конфиденциальность (C)		Не оказывает (N)
			Низкое (L)
			Высокое (H)
	Влияние на целостность (I)	Влияние на надежность и гарантированную правдивость информации	Не оказывает (N)
			Низкое (L)
			Высокое (H)
	Влияние на доступность (A)	Имеется в виду влияние на легкость доступа к информационным ресурсам	Не оказывает (N)
			Низкое (L)
			Высокое (H)
CVSS 2.0	Способ получения доступа (AV)	Удаленность атакующего от уязвимого объекта	Сетевой (N)
			Смежная сеть (A)
			Локальный (L) (любые действия, не затрагивающие сеть)
	Сложность получения доступа (AC)	Метрика показывает сложность атаки, которая позволяет эксплуатировать уязвимость при получении доступа к атакуемой системе	Высокая (H)
			Средняя (M)
			Низкая (L)
	Аутентификация (Au)	Метрика показывает количество раз, которое злоумышленник должен аутентифицироваться, чтобы эксплуатировать уязвимость	Множественная (M)
			Единственная (S)
			Не требуется (N)
	Влияние на конфиденциальность (C)		Не оказывает (N)
			Частичное (P)
			Полное (C)
	Влияние на целостность (I)	Влияние на надежность и гарантированную правдивость информации	Не оказывает (N)
			Частичное (P)
			Полное (C)
	Влияние на доступность (A)	Имеется в виду влияние на легкость доступа к информационным ресурсам	Не оказывает (N)
			Частичное (P)
			Полное (C)

Для уточнения значения метрик дополнительно можно использовать временные и контекстные метрики, которые позволяют учитывать отличные от базовых факторы.

Для подобной работы можно использовать калькулятор БДУ ФСТЭК, ссылка на который содержится на странице с уязвимостью (кнопка в строке **Вектор атаки**).

11.21 Работа с терминалом (устаревший функционал, оставлен для совместимости с агентами более ранних версий)

11.21.1. Общая информация

Терминал является консолью управления, предназначенной для задания команд определенному агенту. Оболочка командной строки доступна аналитику со страницы **Терминал**.

Примечание

Формат команд аналогичен формату команд средства автоматизации PowerShell для агентов, установленных в ОС Windows, и командного процессора BASH для агентов, установленных в ОС Linux.

В области **Выбор Агента** необходимо выбрать из всплывающего списка агента, для которого будут вводиться команды в терминале. Чтобы оставить в списке только активных в данный момент агентов, следует установить флажок Только активные . Если флажок не устанавливать, то для выбора будут доступны все агенты, но отправлять команды в терминале можно будет только активным, для неактивных агентов доступен только просмотр истории команд терминала.

После выбора активного агента появится окно **Терминал**, разделённое на две части:

1) Область просмотра истории работы с терминалом;

2) Область ввода команд.

Если в списке выбрать неактивного в данный момент агента, то область ввода команд будет выделена для такого агента заливкой серого цвета, обозначающей, что ввод команд невозможен, кнопки Прервать Отправить также будут неактивны, как и область ввода **Тайм-аут (сек)**. По умолчанию тайм-аут составляет 300 секунд.

Для некоторых пользователей доступ к терминалу может быть запрещен, в этом случае страница **Терминал** будет отсутствовать для такого пользователя, а также станут неактивными кнопки **Выполнить команду на выбранных агентах** на странице **Агенты** и **Открыть** на странице **Агент**.

11.21.2. Отправка команд управления на странице «Терминал»

Для управления агентом с помощью командной строки аналитику следует прописать в области ввода **Введите команду (Enter – отправить, Ctrl-C – прервать, макс. длина 32768 символов)** необходимую команду и нажать клавишу **Enter** или кнопку Отправить. В области просмотра истории терминала отображаются ранее введённые команды и показывается текущий статус выполнения команды. Предусмотрены следующие статусы: Отправлена / Получена / Выполнена (код 0)

Для просмотра основных доступных команд и описаний к ним необходимо ввести в окне терминала команду **help** (рис. 78).

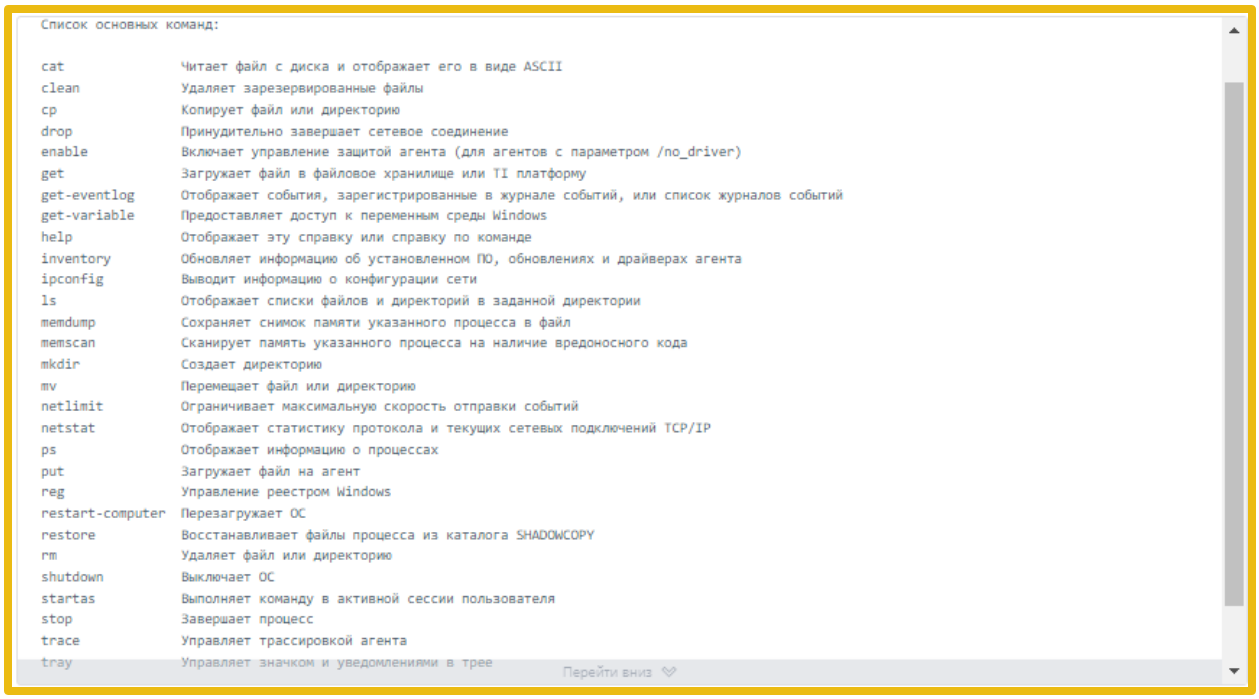


Рисунок 78 – Список основных команд терминала

Если требуется справка о команде из представленного списка, необходимо ввести команду с одним из аргументов: /h, /help, -h, --help, /?. Примеры команд:

```
restore /?
```

restore --help

Снизу от области просмотра истории терминала находится кнопка перехода к результату последнего ввода команды Перейти вниз .

В нижней части области **Терминал** содержится кнопка Прервать, ее действие дублируется с помощью нажатия сочетания клавиш Ctrl+C во время выполнения команды в терминале. С помощью кнопки или сочетания клавиш можно прервать выполнение команды. Статус команды поменяется на Прервана (Ctrl-C) , а через единицу времени, указанную в поле **Тайм-аут (сек)** статус поменяется на прервана по тайм-ауту.

Для установки времени ожидания ответа от агента при отправке команд в поле **Тайм-аут (сек)** необходимо указать нужный интервал времени в секундах. По умолчанию время ожидания составляет 300 секунд.

Для изменения агента в области **Выбор Агента** нужно нажать кнопку ✕ в строке с названием текущего агента, после чего из выпадающего списка выбрать нового агента.

11.21.3. Описание команд терминала, реализованных в службе агента

Перечень команд, реализованных в службе агента:

– admin_msg

– clean;

– drop;

– get;

– put;

– inventory;

– restore;

– startas;

– stop;

– tray;

– enable;

– команды перезапуска службы агента;

– trace;

– memdump;

– memscan;

– net_contain;

– netlimit;

– reset-errors;

– get-log.

Все команды доступны также и в онлайн-терминале.

Команда **admin_msg** – отправляет сообщение на компьютер с агентом. Команда выполняется согласно синтаксису admin_msg <Сообщение> [-b64] [-i=<Тип значка>] [-t=<Заголовок>], где:

<Сообщение> – текст сообщения;

<Тип значка> – тип значка сообщения (0 – нет значка, 1 – информация, 2 – предупреждение, 3 – ошибка, по умолчанию используется тип значка информация);

<Заголовок> – заголовок сообщения (по умолчанию содержит название Программы);

-b64 – указывается, если сообщение закодировано в формате base64.

Примеры написания команды:

admin_msg "Сетевой доступ будет заблокирован на время проведения расследования" – отправка сообщения, заданного в текстовом виде;

admin_msg 0JzQvdC+0LPQvtGB0YLRgNC+0YfQvdC+0LU0YHQvtC+0LHRidC10L3QuNC1 -b64 – отправка UTF-сообщения, заданного в формате base-64 (удобно ипользовать, если сообщение содержит переносы строк и другие служебные символы);

admin_msg "Компьютер будет заблокирован через 1 минуту" -i=2 -t="Предупреждение" – отправка сообщения с заголовком и предупреждающим типом значка.

Команда **clean** – удаляет зарезервированные файлы. Команда выполняется согласно синтаксису **clean** [<Максимальный возраст файлов>]. Максимальный возраст файлов (допустимые суффиксы: d – дни, h – часы, m – минуты). По умолчанию используется значение из профиля Антишифра (10 дней).

Примеры написания команды **clean**:

clean 10h – удаляет зарезервированные файлы старше десяти часов;

clean 2d – удаляет зарезервированные файлы старше двух дней.

Команда **drop** – принудительно завершает сетевое соединение.

Команда выполняется согласно синтаксису drop [-id] <fluuid или flow> [-w admin|ti], где

– id – fluuid или flow сетевого соединения;

– w – кто завершил сетевое соединение: admin – администратор, ti – TI платформа (по умолчанию: admin).

Примеры написания команды **drop**:

drop -id c24bba95-9d6b-01da-2d12-000000000000 – завершает сетевое соединение с уникальным идентификатором (поле fluuid в событии) c24bba95-9d6b-01da-2d12-000000000000;

drop -id 2096738 – завершает сетевое соединение с идентификатором (поле flow в событии) 2096738.

Команда **get** – загружает файл в файловое хранилище EDR.

Команда выполняется согласно синтаксису get [-f] <Полный путь до файла> [-t <ti или cloud>] [-r] [-xl], где:

-f –путь до файла;

-t – тип хранилища для загрузки файла (ti – ti-платформа, cloud – хранилище EDR, по умолчанию берется тип хранилища cloud);

-r – параметр удаляет файл на агенте после успешной загрузки (по умолчанию файл не удаляется);

-xl – параметр разрешает загрузку файла больше 32 МБ (по умолчанию ограничение на макс. размер загружаемого файла составляет 32 МБ).

Пример написания команды:

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" (загрузка файла в хранилище EDR);

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" -t cloud (загрузка файла в хранилище EDR);

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" -t ti (загрузка файла на ti-платформу).

Команда **memdump** – сохраняет снимок памяти указанного процесса в файл. Файл сохраняется в директорию dumps (в ProgramData\<директория агента>). Команда выполняется согласно синтаксису: memdump {[-id] <UUID процесса> | <PID>}.

Пример написания команды:

memdump 2260

memdump -id 2260

memdump {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

memdump -id {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

В результате выполнения команды в директории **C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\dumps** будет создан файл с дампом процесса.

Команда **memscan** – сканирует память указанного процесса на наличие вредоносного кода. Команда выполняется согласно синтаксису: memscan {[-id] <UUID процесса> | <PID>}, где:

pid – это идентификатор процесса (вместо PID процесса можно указать его уникальный идентификатор в RT Protect EDR).

Пример написания команды:

memscan 1080

memscan -id 1080

memscan {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

memscan -id {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

Команда **inventory** – обновляет информацию об установленном ПО, обновлениях и драйверах агентов.

Команда **put** – загружает файл с сервера EDR на машину с установленным агентом. Команда выполняется согласно синтаксису put [-u] <Ссылка для загрузки> [-w <Расположение файла на агенте>] [-y] [-n <Новое имя файла>], где:

-u – это ссылка для загрузки;

-w – расположение файла на агенте (директория, в которую загружается файл; если директория не существует, то она создается, по умолчанию C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\download\);

-y – перезапись существующего файла (по умолчанию перезаписи нет);

-n – новое имя файла (по умолчанию имя берется из ссылки для загрузки).

Примеры написания команды:

1) Команда загрузки файла на машину с агентом по пути C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\download\first_aid_kit.exe:

put https://<адрес_сервера>/api/storage/user/object/<UUID-объекта>/first_aid_kit.exe;

2) Команда загрузки файла на машину с агентом по пути C:\Tools\file_ver_1.exe:

put https://<адрес_сервера>/api/storage/user/object/<UUID-объекта>/first_aid_kit.exe -w C:\Tools -n file_ver_1.exe.

Команда **restore** – восстанавливает зарезервированные файлы. Команда выполняется согласно синтаксису restore [-id] <UUID-процесса> [-c], где:

-id – это UUID процесса;

-c – аргумент для удаления созданных файлов.

Пример написания команды:

restore -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}.

Команда **startas** – запускает процесс под определенным пользователем. Команда выполняется согласно синтаксису startas [-cmd] <Командная строка> [-u <Имя пользователя>] [-ws {normal | hidden | minimized | maximized}], где:

-cmd – это командная строка для запуска;

-u – имя пользователя с активной сессией (по умолчанию используется активная сессия пользователя);

-ws – стиль окна запускаемого процесса: normal (по умолчанию), hidden, minimized, maximized.

Пример написания команды:

startas calc.

Команда **stop** – завершает процесс. Команда выполняется согласно синтаксису stop [-id] <UUID процесса [-c <Статус завершения процесса>] [-w admin|ti] [-t <Тип сообщения>], где:

-id – это UUID процесса;

-c – статус завершения процесса (по умолчанию 0);

-w – кто завершил процесс: admin – администратор, ti – ti-платформа (по умолчанию admin);

-t – тип сообщения, определяет уровень уведомления о завершении процесса: info, warning, error (по умолчанию: если параметр -w установлен как admin, то -t принимает значение info, если параметр -w установлен как ti, то -t принимает значение error).

Примеры написания команды:

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4};

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti;

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w admin -t error.

Формат команды для кнопки **Завершить процесс**: stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}

Формат команды для завершения процесса по требованию TI-платформы: stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti

Команда **tray** – управляет значком и уведомлениями в трее.

Команда выполняется согласно синтаксису tray [<Уровень>], где:

[<Уровень>] 0 – нет значка в трее, уведомления не выводятся;

[<Уровень>] 1 – есть значок, уведомления не выводятся;

[<Уровень>] 2 – есть значок, показывать только критические уведомления;

[<Уровень>] 3 – есть значок, показывать все уведомления.

Пример написания команды:

tray (выводит информацию о текущем состоянии значка трея);

tray 2 (переводит значок трея в режим показа только критических уведомлений).

Команда **enable** – включает управление защитой агента, установленного с параметром /no_driver.

– Пример: enable.

Команды перезапуска службы агента – для перезапуска службы агента необходимо выполнить последовательно следующие команды в терминале агента:

New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpsvc -Name AllowStop -PropertyType DWord -Force -Value 1

sc.exe control vrpsvc 128

restart-service vrpsvc



Совет

Локально перезапуск службы можно осуществить с помощью команды Setup /noUI /update, запущенной из каталога, в котором находится установочный файл текущего агента.

Команда **trace** управляет трассировкой агента. Команда выполняется согласно синтаксису trace <-start или -stop> <-svc или -drv> [маска логируемых подсистем (по умолчанию трассируются все подсистемы: 0xFFFFFFFF)][уровень логирования (по умолчанию: 0xFF)][-s], где:

-start – запускает трассировку;

-stop – останавливает трассировку;

-svc – управление трассировкой службы;

-drv – управление трассировкой драйвера;

-usb – управление трассировкой USB-драйвера;

– [маска логируемых подсистем] – маска трассируемых подсистем службы или драйвера (используется в команде -start);

– [уровень логирования] – 0x5 (Verbose), 0x4 (Informational), 0x3 (Warning), 0x2 (Error), 0x1 (Critical), (используется в команде -start) (по умолчанию уровень логирования определяется как **Verbose**);

– -s – аргумент, позволяющий не удалять файл трассировки после остановки (по умолчанию файл будет удален после удачной отправки на сервер), (используется в команде -stop).

– Маски логируемых подсистем и наименования этих подсистем приведены в таблице 57.

Таблица 57 – Маски логируемых подсистем

Подсистемы	Маски
Маски логируемых подсистем для службы агента	
TRACE_SERVICE_ENGINE	0x00000001
TRACE_EVENTS	0x00000002
TRACE_METADATA_ENGINE	0x00000004
TRACE_AGENT_UPDATE	0x00000008
TRACE_FILE_SCANNER	0x00000010
TRACE_NETWORK_CONTAINMENT	0x00000020
TRACE_SESSION_MONITOR	0x00000040
TRACE_ETW_CONSUMER	0x00000080
TRACE_ETW_DOTNET_LOAD_IMAGE_MONITOR	0x00000100
TRACE_ETW_RPC_MONITOR	0x00000200
TRACE_ETW_KERBEROS_ATTACK_MONITOR	0x00000400
TRACE_ETW_SYSTEMTIME_CHANGED_MONITOR	0x00000800
TRACE_ETW_WMI_ACTIVITY_MONITOR	0x00001000
TRACE_ETW_MONITORS	0x00002000
TRACE_TERMINAL	0x00004000

Подсистемы	Маски
TRACE_WMI_MONITOR	0x00008000
TRACE_SYSTRAY	0x00010000
TRACE_MS_GROUP_POLICY	0x00020000
TRACE_YARA	0x00040000
TRACE_ML	0x00080000
Маски логируемых подсистем для драйвера агента	
TRACE_REGISTRY_MONITOR	0x00000001
TRACE_REGISTRY_MATCHER	0x00000002
TRACE_REGISTRY_CONFIG_PARSER	0x00000004
TRACE_RESERVED1	0x00000008
TRACE_FS_MONITOR	0x00000010
TRACE_FS_MONITOR_SIGN	0x00000020
TRACE_FS_MONITOR_RULES	0x00000040
TRACE_FS_MONITOR_HASHES	0x00000080
TRACE_FS_MONITOR_SCAN	0x00000100
TRACE_FS_MONITOR_DEF_SCAN	0x00000200
TRACE_RESERVED2	0x00000400
TRACE_RESERVED3	0x00000800
TRACE_ARW	0x00001000
TRACE_ARW_BLOCK_OPERATION	0x00002000
TRACE_ARW_RESERVED1	0x00004000
TRACE_ARW_RESERVED2	0x00008000
TRACE_PATH_CLASSIFY	0x00010000
Маски логируемых подсистем для USB-драйвера	
TRACE_BASE	0x00000001
TRACE_PNP	0x00000002
TRACE_AGENT_INTERACTION	0x00000004

Примеры написания команды:

1) Трассировка всех подсистем службы с уровнем логирования Verbose (если не указывается конкретный уровень логирования, то применяется уровень логирования по умолчанию):

```
trace -start –svc
```

2) Трассировка подсистем службы: TRACE_SESSION_MONITOR и TRACE_WMI_MONITOR, с уровнем логирования Warning:

```
trace -start -svc 0x8040 0x3
```

3) Остановка трассировки службы:

trace -stop -svc

4) Трассировка всех подсистем драйвера с уровнем логирования Verbose:

trace -start -drv

5) Трассировка подсистем драйвера TRACE_REGISTRY_MONITOR, TRACE_REGISTRY_MATCHER, TRACE_REGISTRY_CONFIG_PARSER с уровнем логирования Error:

trace -start -drv 0x7 0x2

6) Остановка трассировки драйвера:

trace -stop -drv

7) Трассировка всех подсистем USB-драйвера с уровнем логирования Verbose:

trace -start -usb

8) Остановка трассировки USB-драйвера:

trace -stop -usb

Команда **net_contain** – управляет сетевой изоляцией агента. Команда выполняется согласно синтаксису net_contain [0|off|false|1|on|true], где значение 0, off и false означают, что изоляция агента будет выключена, а 1, on и true, что изоляция будет включена. **Net_contain** без аргументов показывает текущее состояние изоляции агента.

Примеры написания команды:

net_contain 0 – изоляция сети выключена;

net_contain 1 – изоляция сети включена;

net_contain false – изоляция сети выключена;

Команда **netlimit** – ограничивает максимальную скорость отправки событий. Команда выполняется согласно синтаксису: netlimit [<Макс. скорость>], где:

<Макс. скорость> – Максимальная скорость отправки (Кбит\с) (значение 0: без ограничений).

Пример написания команды:

1) Вывод текущего ограничения максимальной скорости отправки:

netlimit

2) Установка ограничения максимальной скорости отправки 5 Кбит\с:

```
netlimit 5
```

3) Снятие ограничения на максимальную скорость:

```
netlimit 0
```

Команда **reset-errors** – сбрасывает счетчики прикладных и системных ошибок на агенте, команда выполняется согласно синтаксису reset-errors [all | app | sys], где:

all – сброс всех счетчиков ошибок (выполняется по умолчанию);

app – сброс счетчика прикладных ошибок;

sys – сброс счетчика системных ошибок.

Примеры выполнения команд:

Сброс счетчиков системных и прикладных ошибок:

```
reset-errors
```

Сброс счетчика прикладных ошибок:

```
reset-errors app
```

Сброс счетчика системных ошибок:

```
reset-errors sys
```

Команда **get-log** – загружает логи агента в файловое хранилище, команда выполняется согласно синтаксису get-log <Наименование лога>, где наименование лога агента принимает следующие значения:

driver – лог драйвера;

usb – лог usb-драйвера;

service – лог службы.

После выполнения команды логи можно забрать в разделе **Хранилище**.

Логи драйвера на хосте можно также собрать в папке C:\Windows\VrpntMetadata, логи USB-драйвера в папке C:\Windows\VrpusbcMetadata, а логи службы в папке C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR.

11.21.4. Информация в области «Выбор Агента»

В области **Выбор агента** аналитик может выбрать агента, которому необходимо отправить команду. Для большего удобства в строке выбора можно оставить только активных агентов, поставив флажок **Только активные**. В области **Выбор агента** пользователю доступна следующая информация об агенте:

1) Имя компьютера;
2) Версия ОС;
3) Время загрузки системы;
4) Процессор;
5) Оперативная память;
6) Сетевые адреса.

Имя компьютера – в поле отображается имя компьютера, на котором установлен агент.

Версия ОС – в поле отображается название ОС, установленной на компьютере, на котором работает агент.

Время загрузки системы – в поле отображается информация о дате и времени последней загрузки операционной системы, под управлением которой действует агент.

Процессор – в поле отображается наименование и тактовая частота процессора компьютера, на котором установлен агент.

Оперативная память – в поле отображается объем оперативной памяти компьютера, на котором установлен агент. Объем указан в мегабайтах.

Сетевые адреса – в поле отображаются IP-адреса, назначенные для всех сетевых интерфейсов компьютера, на котором установлен агент.

В нижней части области **Выбор Агента** отображается состояние агента – 

.

11.22 Управление задачами

Планировщик задач – это инструмент, позволяющий аналитику управлять задачами, назначаемыми агентам и операционной системе, на которой установлен агент. Планировщик позволяет автоматизировать выполнение задач и выполнять их периодическое планирование. Через планировщик, аналитик может одним действием запустить сбор артефактов на сотне хостов, регулярно выполнять диагностический скрипт на

критичных серверах или настроить автоматическую остановку процесса при срабатывании правила. Примери применения планировщика задач:

– ручное реагирование на инцидент (остановить процесс, изолировать хост, собрать дамп);

– плановая диагностика и инвентаризация (проверка версий ПО, сбор журналов);

– автоматизация ответных действий при появлении вредоносного вердикта TI;

– массовая ремедиация по итогам расследования.

Создание, редактирование и удаление задач осуществляется в разделе **Планировщик задач**. Задача может состоять из одной или нескольких команд или скрипта/скриптов, отправляемых агенту и выполняющихся по определенному триггеру.

На данный момент в Программе задаются четыре триггера – это запуск задачи по требованию, запуск по расписанию, триггер по вердикту от TI-платформы (если TI отвечает, что артефакт вредоносный, то сервер формирует сценарий запуска задачи), а также триггер по инциденту.

По требованию может быть запущена любая задача, даже та, у которой настроено расписание. В случае с запуском по расписанию доступно создание расписания посредством файлов crontab или с помощью предусмотренного Программой конструктора, а также запуск задачи по временному шаблону, то есть выбор расписания из заданного в Программе списка.

Каждая задача в Программе является контейнером для сценария. Сценарий представляет собой команду, скрипт или набор команд/скриптов, задаваемых аналитиком во вкладке **Сценарии** раздела **Планировщик задач**.

Аналитик может редактировать, удалять, включать и отключать как задачи, так и сценарии. Отключать или включать задачи можно только в том случае, если это задачи с триггером запуска **По расписанию** и сценарий задачи не выключен. Отключение сценария приведет к тому, что не будут выполняться все задачи, связанные с этим сценарием.

Кратко информация об основных сущностях планировщика задач представлена в таблице 58.

Таблица 58 – Сущности планировщика задач

Сущность	Назначение
Сценарий	Многоразовый сценарий: заголовок, описание, набор действий. В скрипте описано, что делать
Задача	Расписание запуска сценария на выбранных агентах с таймаутом, cron-выражением и контекстом подстановки. В задаче описывается, когда и где это делать, плюс возможно добавить параметры выполнения сценария.

Сущность	Назначение
Запуск	Конкретный запуск сценария с конкретными результатами. Появляется либо при разовом запуске, либо по расписанию задачи, либо по сценарию реагирования.

11.22.1. Создание сценария

Сценарий – это набор действий, выполняемых на агенте, в том числе это могут быть цепочки последовательных действий (всего в сценарии может быть последовательно выполнено 100 команд или скриптов). У каждого действия есть интерпретатор и сама команда. Из сценариев формируются задачи. Сценарий может быть один для нескольких разных задач.

Чтобы создать сценарий необходимо выполнить следующие шаги:

1) Нажать кнопку **Добавить сценарий** на странице **Сценарии**;

2) В открывшемся окне **Добавить сценарий** ввести название сценария;

3) Добавить одно или несколько действий, предварительно выбрав вариант исполнения скрипта или команды, то есть выбрав, будет ли это встроенная команда или исполнение в одном из представленных в списке интерпретаторов (Powershell, CMD, BASH или SH); список встроенных команд представлен в подпункте 11.21.3 (добавление действия также является обязательным при создании сценария), порядок действий имеет значение, можно менять действия местами, перетаскивая их, аналитик может задать не более ста действий.;



Примечание

Перед тем, как текст скрипта или команды попадает в интерпретатор, он обрабатывается шаблонизатором jinja2. Шаблонизатор – это инструмент, который позволяет отделить структуру (шаблон) от данных, автоматически подставляя значения в нужные места. Например, мы можем написать отдельный скрипт для каждого сервера (Remove-AnyFile -Path "C:\Server1\Logs\app.log", Remove-AnyFile -Path "C:\Server2\Logs\app.log", Remove-AnyFile -Path "C:\Server3\Logs\app.log"), а можем записать шаблон Remove-AnyFile -Path "{{ server_path }}", где server_path заменяется на любое значение пути (которое в нашем случае будет определено в параметре, задаваемом при формировании задачи).

4) Ввести описание сценария, пункт является опциональным.

5) Установить флаг **Включить сценарий**, чтобы сценарий стал активным (в дальнейшем сценарий можно отключить, выключенный сценарий не будет исполняться);

6) Нажать кнопку **Добавить**, после чего сценарий будет добавлен на страницу **Сценарии** и доступен для создания задачи во вкладке **Задачи**.

Powershell — это кроссплатформенный фреймворк автоматизации и управления конфигурацией от Microsoft, сочетающий в себе командную оболочку и язык сценариев.

CMD – стандартный интерпретатор командной строки в операционных системах Windows, позволяющий быстро выполнять простые команды, работать с устаревшими приложениями (например, DOS-программы) и выполнять простую автоматизацию.

BASH – современная командная оболочка UNIX-подобных операционных систем, основная область применения которой это системное администрирование (управление серверами и службами, автоматизация развертывания и обслуживания, мониторинг системных ресурсов и т.д.).

SH – оригинальная командная оболочка для UNIX-подобных систем, отличается от BASH минимальным набором функций, поддержкой только базовых команд, по сути являясь фундаментом, на котором построены все современные командные оболочки в Linux.

Важно

При создании сценария необходимо обращать внимание на ОС агента и соответствие интерпретатора этой системе. Например, если выбран агент Windows, а в качестве интерпретатора выбраны BASH или SH, то такой сценарий не будет выполнен.

Сценарии можно фильтровать по следующим фильтрам:

– по количеству сценариев на странице;

– по названию (для поиска по вхождению строки можно использовать символ *);

– по описанию (для поиска по вхождению строки можно испольэловать символ *);

– по логину создателя сценария;

– по времени создания.

Сценарии управляются с помощью кнопок в поле **Управление** на вкладке **Сценарии** страницы **Планировщик задач**. Чтобы отключить/включить сценарий, необходимо нажать кнопку / и подтвердить действие в открывшемся окне. Для редактирования сценария следует нажать кнопку , внести необходимые изменения и нажать кнопку **Сохранить**. Кнопка удаляет сценарий, действие требует подтверждения. Любой сценарий можно закрепить за типовым сценарием реагирования с помощью кнопки **Закрепить за сценарием реагирования** ( ), это позволит заменить дефолтные действия сценария реагирования на действия соответствующего сценария.

Сценарии можно экспортировать и импортировать (в JSON-формате). Чтобы экспортировать сценарии, выберите нужные и нажмите кнопку  снизу таблицы со сценариями. Чтобы импортировать сценарии на сервер управления, нажмите кнопку  .

Переход на страницу сценария осуществляется кликом по названию сценария. На странице **Сценарий** пользователь может выполнять те же самые операции, что и во вкладке **Сценарии** (включение/выключение сценария, редактирование, удаление, и закрепление за сценарием реагирования). Здесь же пользователь может просмотреть набор действий, которые будут выполнены при активации сценария, отследить статус сценария (включен или отключен), узнать автора сценария, идентификатор сценария, время, когда сценарий был изменен в последний раз, а также название и описание сценария.

Кроме того, на странице **Сценарий** доступен просмотр задач, которые задействуют сценарий, а также доступен функционал добавления задачи для этого сценария по кнопке **Добавить задачу**.

11.22.2. Создание задачи

Как уже упоминалось выше, задачи – это элементы Программы, которые являются контейнерами для сценариев, по сути, задача – это сценарий плюс параметры планирования, то есть каждой задаче соответствует определенный сценарий.

Чтобы создать задачу необходимо выполнить следующие шаги:

1) Ввести название задачи в строке **Название** (это условие является обязательным для создания задачи);

2) Определить агентов, на которых будет исполняться задача (условие является обязательным для создания задачи);

3) Выбрать сценарий для задачи (условие является обязательным);

4) Выбрать расписание, по которому задача будет исполняться, для дальнейшего запуска задачи по требованию необходимо выбрать исполнение задачи без расписания. Расписание задачи можно задать тремя способами:

– с помощью crontab;

– с помощью конструктора, который повторяет синтаксис crontab, но позволяет создавать расписание более наглядно для аналитиков, незнакомых с синтаксисом crontab;

– с помощью шаблонов расписания;

5) Установить тайм-аут в секундах в строке **Тайм-аут;**



Примечание

Тайм-аут показывает, по истечении какого временного периода задача будет отменена, если агент не принял задачу на исполнение, по умолчанию устанавливается значение 1200 секунд.

6) Выбрать временной период распределения задачи по агентской сети, период назначается в минутах;

7) Ввести описание (пункт является опциональным);

8) Установить флаг **Включить задачу**, чтобы задача стала активной (в дальнейшем задачу можно отключить, выключенная задача не будет исполняться);

9) Если необходимо сразу перейти к задаче после ее создания, то установить флаг **Перейти к задаче**;

10) Если требуется, то добавить параметры задачи (параметры задачи определяются с помощью шаблонизатора jinja2 на этапе создания сценария, то есть аналитик может сам решить, какие параметры, каким переменным будут соответствовать).

Примечание

Разберем на примере сценария реагирования **Отправить сообщение**: `admin_msg {{ msg | b64encode }} -b64 {% if title is defined and title %} -t="{{ title }}"{% endif %} {{ add_params | default }}`

Здесь **admin_msg** – это встроенная команда, отправляющая сообщение.

`{{ msg | b64encode }}` — параметр msg (шаблон для сообщения) передается через фильтр b64encode, который кодирует его содержимое в Base64. Это делается, чтобы безопасно передавать данные, содержащие спецсимволы, пробелы или многострочный текст.

-b64 — флаг, указывающий, что данные закодированы в Base64 (программа будет их декодировать перед обработкой).

`{% if title is defined and title %} -t="{{ title }}"{% endif %}` — условная конструкция: если шаблон title существует и не пустой, то добавляется параметр -t со значением title в кавычках. Это позволяет сделать параметр -t опциональным.

`{{ add_params | default }}` — добавляются дополнительные параметры add_params, если они есть (фильтр default выводит значение переменной или пустую строку, если переменная не определена).

Подробная информация о шаблонах jinja содержится в документации разработчика.

11) Нажать кнопку **Добавить**, после чего задача появится в таблице со списком задач.

Crontab в планировщике задач – это таблица расписаний выполнения задачи, одна строка, состоящая из полей времени (см. таблицу 59).

Таблица 59 – Описание полей времени

Поле	Диапазон	Описание
Минуты	0-59	Минута запуска команды
Часы	0-23	Час запуска
День месяца	1-31	Число (день) запуска
Месяц	1-12	Месяц запуска
День недели	0-6	День недели (0 - воскресенье)

Для гибкой настройки расписания необходимо использовать специальные символы:

1) * (звездочка): любое допустимое значение.

2) , (запятая): перечисление значений (например, 1,3,5).

3) - (дефис): диапазон значений (например, 9-17).

4) */n (слеш): шаг значений (например, */10 в поле **Минуты** означает «каждые 10 минут»).

Примеры заданий для crontab:

1) Каждый день в 14:30 – 30 14 * * *

2) Каждый понедельник в 9:00 утра – 0 9 * * 1

3) Каждые 10 минут – */10 * * * *

4) Каждый день в 0:30 и 12:30 – 30 0,12 * * *

Планирование задач осуществляется на сервере. Если задача не будет выполнена на агенте за установленное в тайм-ауте время, ее выполнение завершится без результата. Это может быть, например, если агент выключен или потерял связь с сервером на длительное время, большее, чем время тайм-аута, установленное в задаче.



Примечание

Если сценарий задачи состоит из нескольких шагов или задача применяется на большое количество агентов и успевает отработать за время тайм-аута только часть из этих шагов или только на части агентов, то по истечении тайм-аута задача прервется, а в ее запуске отобразятся частичные результаты выполнения задачи. Время отсчета тайм-аута начинается с момента запуска задачи.

Указав значение тайм-аута 0, аналитик может создать задачу с бесконечным лимитом времени выполнения. Такой функционал поддерживается EDR, но не рекомендуется в качестве общего подхода к работе с задачами. Прервать выполнение такой задачи можно будет только вручную.

Список задач можно фильтровать по следующим фильтрам:

– по количеству задач на странице;

– по названию (для поиска по вхождению строки можно использовать символ *);

– по описанию (для поиска по вхождению строки можно использовать символ *);

– по логину создателя задачи;

– по агенту;

– по названию сценария;

– по времени создания;

– по значению действия в сценарии.

Для управления задачами используются кнопки в поле **Управление** на вкладке **Задачи** страницы **Планировщик задач** (включение/отключение задачи (/), запуск задачи ( ), редактировать задачу ( ) и удалить ( )).

Клик по имени задачи перенаправляет на страницу с основными характеристиками этой задачи (название, время тайм-аута, статус задачи, описание и т.д.) и ее запусками. На странице аналитик может управлять задачей: запускать ее, в том числе, запускать задачу с параметрами ( ), включать/выключать задачу (если триггер запуска по расписанию), редактировать и удалять.

11.22.3. Запуск задачи

Запуск задачи – это инструмент, позволяющий отследить, как задача и сценарий с его шагами выполнялись на конкретном агенте или агентах.

Запуск задачи по требованию осуществляется во вкладке **Задачи** раздела **Планировщик задач** и со страницы **Агенты**. Со страницы **Планировщик задач** во вкладке **Задачи** можно запустить как отдельную задачу, так и несколько задач одновременно. Для того, чтобы запустить отдельную задачу, необходимо нажать кнопку **Запустить задачу** ( ) в строке с задачей в поле **Управление**. Задачу можно запускать как с параметрами, так и без них. Чтобы выполнить действие, необходимо его подтвердить.

Чтобы запустить несколько задач одновременно, необходимо выбрать требуемые задачи ( ) и нажать кнопку **Запустить выбранные задачи** ( ) в нижней части страницы **Планировщик задач** на вкладке **Задачи**. Операция требует подтверждения.

Со страницы **Агенты** в рамках реагирования запуск задач осуществляется следующим образом:

1) Выделить агента или группу агентов, для которых будет выполняться задача ( );

2) Нажать кнопку **Реагирование для выбранных агентов** ( ), на данный момент реагирование подразумевает выполнение команд по требованию и по расписанию;

3) Выбрать пункт **Выполнить задачу** (здесь же можно создать задачу по расписанию – пункт **Запланировать задачу**);

4) В открывшемся окне **Выполнить задачу** ввести название задачи в строке **Название**;

5) Установить тайм-аут для задачи (по умолчанию 300 секунд);

6) Выбрать тип действия (Powershell, CMD, SH, BASH или встроенная команда);

7) В поле **Команда** ввести значение команды;

8) Нажать кнопку **Добавить.**

Все запуски задач можно отслеживать во вкладке **Запуски** страницы **Планировщик задач** и, соответственно, можно отслеживать статус задачи – на каком этапе выполнения находится задача. У задачи могут быть следующие статусы:

1) Завершено;

2) Тайм-аут;

3) Отменено;

4) Ошибка;

5) В процессе;

6) Ожидание.

Важно

На агенте количество одновременно выполняемых задач не может превышать двух.

На любом этапе выполнения задачи ее можно остановить с помощью кнопки **Завершить выполнение** ( ).

Информацию во вкладке **Запуски** можно фильтровать с помощью следующих фильтров:

1) Статус запуска;
2) Триггер, по которому выполняется запуск;
3) Агент, на котором выполняется запуск;
4) Инициатор (пользователь, осуществивший запуск);
5) Сценарий (фильтрует запуски по имени сценария);
6) Задача (фильтрует запуски по имени задачи);
7) Время создания запуска.

Страница открывается с предустановленными настройками фильтра **Статусы** (отображаются запуски со статусами **Создан**, **Подтвержден** и **В процессе**).

На странице **Запуск**, которая открывается, если кликнуть по имени запуска, аналитик может просмотреть ход выполнения задачи на агентах, триггер, по которому задача была запущена, время запуска, действия, которые запланированы к выполнению в ходе запуска, агенты, на которых выполняется задача, и т.д. Кроме того, в отдельной круговой диаграмме показано распределение агентов (рис. 79) по статусам выполнения действий на них (агенты с завершенной успешно задачей, агенты с отмененными действиями, агенты, находящиеся в процессе выполнения задачи, агенты, находящиеся в ожидании выполнения задачи, агенты, действия на которых были завершены по тайм-ауту или завершены с ошибкой, а также агенты, действия на которых пропущены программой).

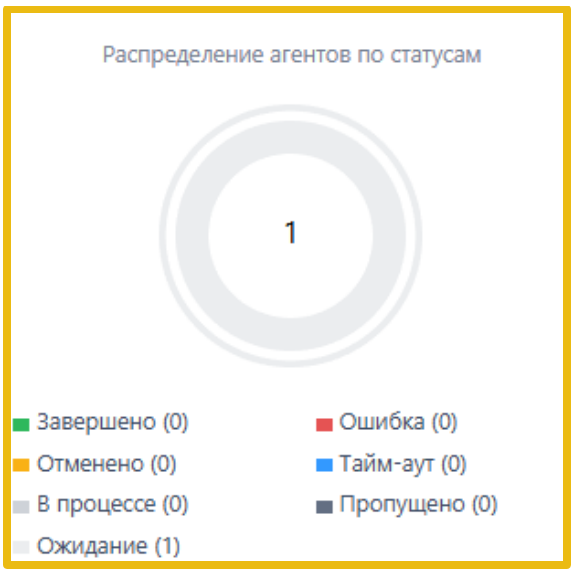


Рисунок 79 – Распределение агентов по статусам

В поле **Состояние** в области **Статусы агентов** отображаются иконки состояния каждого шага сценария: зеленые, если действие на агенте было завершено успешно (код завершения 0), оранжевые, если действие завершилось с ошибкой (любой код завершения, отличный от 0). Если выполнение задачи будет остановлено по тайм-ауту, то в поле **Состояние** отобразится иконка серого цвета для текущего этапа сценария, также если статус агента будет **Пропущено**, то иконка состояния будет серого цвета. В поле **Параметры** для запусков по инциденту отображается событие, которое привело к возникновению инцидента и сам инцидент. Также поле **Параметры** доступно для запусков по вердикту TI для файлов.

В поле **Действия** отображается последовательность команд, которые выполняются в сценарии запуска.

Чтобы просмотреть итоги выполнения команд, необходимо нажать кнопку › в области **Статусы агентов** (рис. 80).

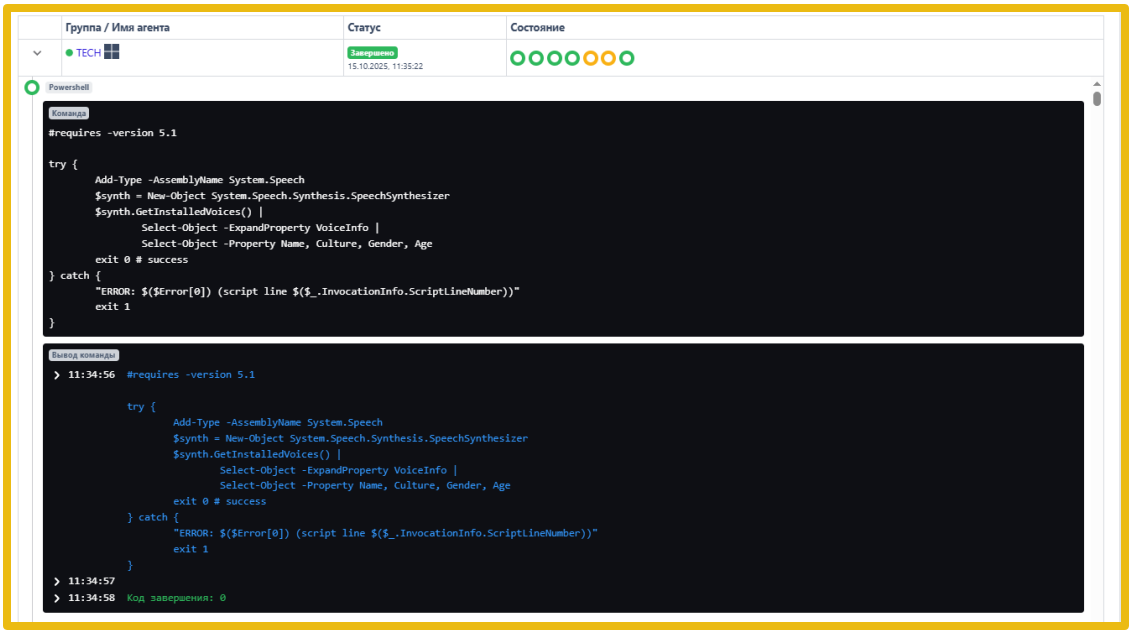


Рисунок 80 – Вывод команды

Запуски задач по требованию (в том числе запуски сценариев реагирования) можно повторять. Для выполнения действия необходимо нажать кнопку **Повторить запуск** ( ).

Документ с информацией о запуске имеет лимит в 20 000 символов, в случае его превышения пользователю будет показан значок в строке с запуском.

11.23 Реагирование

Реагирование в EDR — это комплекс действий, направленных на устранение киберугрозы, которая была обнаружена на конечной точке (компьютере, сервере).

Ключевые цели реагирования:

1) Остановить атаку — немедленно прервать деятельность злоумышленника.

2) Минимизировать ущерб — не дать угрозе распространиться на другие системы.

3) Вернуть систему в безопасное состояние — удалить вредоносные объекты и восстановить нормальную работу.

4) Собрать доказательства — сохранить данные об атаке для последующего анализа (форензики).

Основные инструменты реагирования в RT Protect EDR можно разделить на три вида:

1) **Онлайн-терминал**. Это прямое подключение к командной оболочке на подозрительной конечной точке. Аналитик получает возможность в реальном времени исследовать систему и выполнять команды, как если бы работал с ней напрямую.

2) **Планировщик задач**. Инструмент для отложенного или массового выполнения действий. Позволяет создать задание, которое запустит необходимую команду или скрипт в определенное время на одном или множестве агентов. Поддерживаются все основные оболочки:

– CMD и PowerShell (для Windows);

– Bash и SH (для Linux).

Планировщик задач хорошо подходит для запуска сложных скриптов, сбора артефактов или выполнения стандартных процедур очистки.

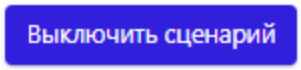
3) **Сценарии реагирования**. Заранее созданные в EDR сценарии реагирования – это эффективный механизм устранения последствий атаки. По сути, это «быстрые кнопки», которые позволяют парой кликов запустить на агенте предписанное действие или целый набор действий.

11.23.1. Сценарии реагирования

Сценарии реагирования – кастомизируемые наборы действий по реагированию, заданные в Программе по умолчанию. Сценарии реагирования подразумевают выполнение определенных команд или скриптов, но аналитики могут по своему желанию их изменять и дополнять.

Подробный список сценариев реагирования, представленных в Программе, содержится в разделе **Планировщик задач** во вкладке **Сценарии**. Также сценарии можно выполнить на различных страницах модуля администрирования: странице **Агенты, Активность, Процесс**. Можно сказать, что сценарии реагирования разбросаны по модулю администрирования, чтобы аналитик мог легко и быстро выполнить команды тогда, когда это подсказывает логика, например, сценарий реагирования **Загрузить файл в Хранилище** в файловом событии.

Сценарии реагирования могут быть изменены аналитиком. Нажатие ЛКМ на имя сценария открывает страницу **Сценарий**, на которой аналитик может его отредактировать, добавив новые действия или изменив дефолтные действия.

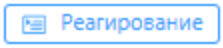
Изменения в сценарии реагирования можно откатить до дефолтных значений, для этого следует использовать кнопку **Восстановить действия сценария реагирования по умолчанию** () на странице сценария реагирования (открывается при клике по имени сценария). Также аналитик может отключить сценарий, сделав его неактивным с помощью кнопки 

, что будет подтверждено надписью 

в строке **Статус** на странице сценария реагирования.

Загрузить файл в Хранилище

Сценарий позволяет выбрать файл на компьютере с агентом и поместить выбранный файл в Хранилище EDR для последующего анализа. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию 

. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. На странице **Активность** кнопки загрузки файла в **Хранилище** отображаются в соответствующих тому или иному файлу полях или в поле **Информация** страницы **Активность**. Здесь можно загрузить файл по полному имени исполняемого файла процесса (**app**), полному имени файла (**name**), полному имени исполняемого модуля инициатора операции (**who**).

После открытия окна **Загрузить файл в Хранилище** в строке **Имя файла** необходимо написать полное имя файла, после чего нажать кнопку **Отправить**.

В случае с загрузкой со страницы **Активность** строка **Имя файла** заполняется автоматически. Если размер загружаемого файла превышает 32 Мб, то предварительно следует установить флаг **Файл более 32 Мб**. Для автоматического перехода к запуску сценария в Планировщике задач необходимо установить флаг **Перейти к запуску** (рис. 81). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

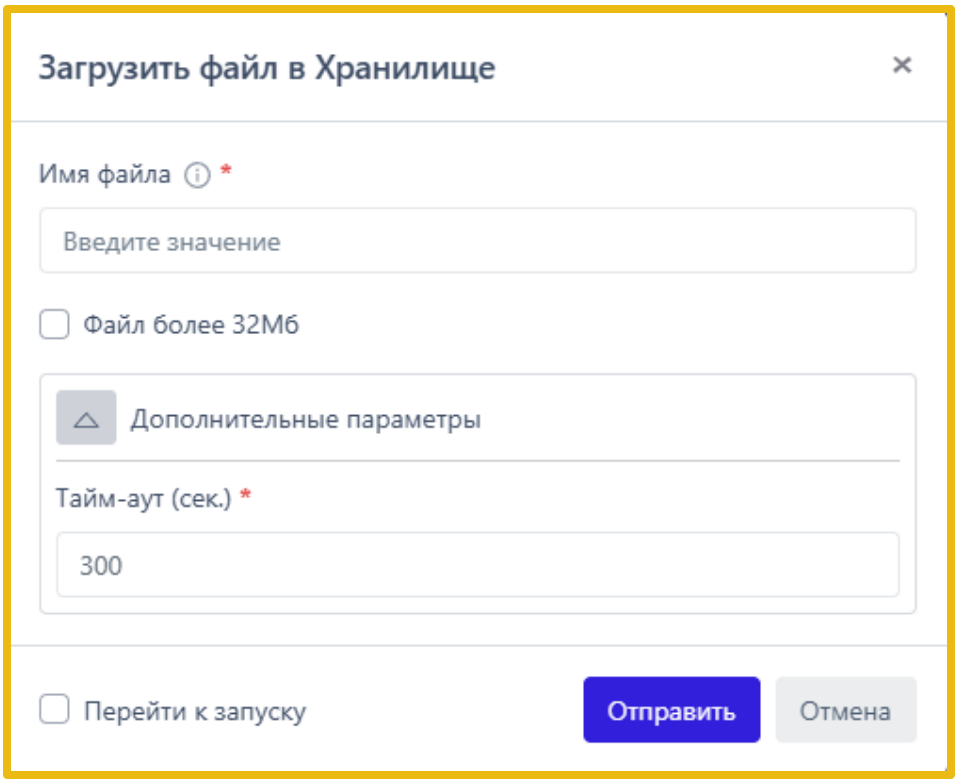


Рисунок 81 – Сценарий загрузки файла в Хранилище

Сетевая изоляция

Блокирование сетевого трафика компьютера, на котором установлен агент, кроме связи с EDR-консолью. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** ( ), после чего выбрать операцию Сетевая изоляция . На странице **Агент** список

сценариев открывается в области **Реагирование** по кнопке Реагирование (здесь мы изолируем одного выбранного агента).

В открывшемся окне **Сетевая изоляция** будет автоматически выбрана опция **Включить сетевую изоляцию** (чтобы снять изоляцию на изолированном ранее агенте, необходимо перевести переключатель в состояние **Выключить сетевую изоляцию**). Для завершения операции необходимо нажать кнопку **Отправить**.

Примечание

Сетевая изоляция компьютера с установленным агентом происходит в течение 5 секунд после отправки команды.

Необходимо также помнить, что в случае изоляции агента, подключенного через VPN, рекомендуется заблаговременно добавить IP-адрес VPN-шлюза в сетевые исключения с флагом **Разрешить (всегда)**, иначе снять изоляцию такого агента не получится. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 82). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

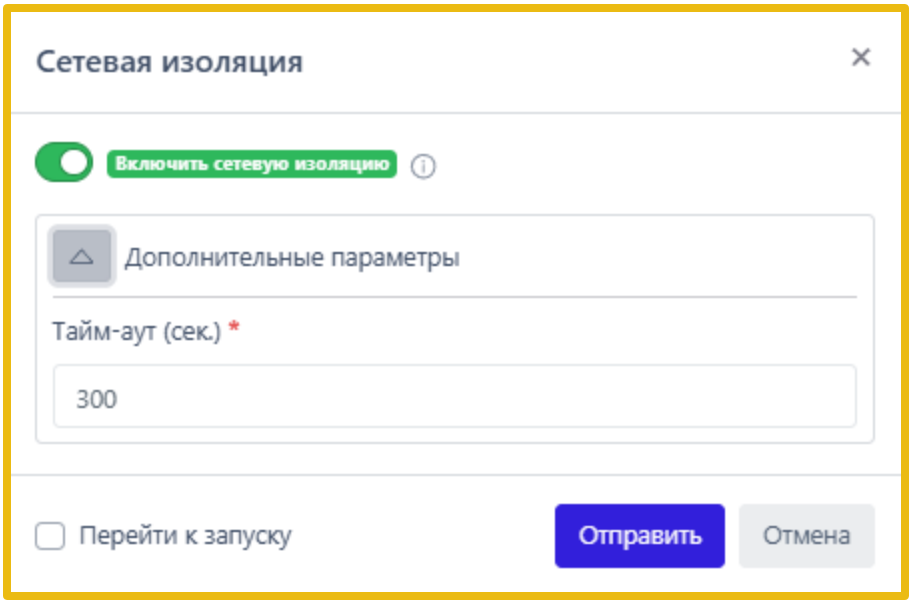


Рисунок 82 – Сценарий сетевой изоляции агента

Изолированные агенты помечаются надписью Изолирован на странице **Агенты** в столбце **Состояние**, а также на странице **Агент**.

Отправить сообщение

Действие реагирования выполняет отправку сообщения на компьютер с агентом для пользователя этого компьютера, например, сообщая о том, что компьютер пользователя будет выключен через определенное время. Аналитик может указать заголовок сообщения, а также выбрать иконку сообщения. Сообщение не будет выведено, если сообщения запрещены текущим уровнем трея (команда **tray**). Тайм-аут на выполнение сценария по умолчанию равен 300 секундам.

Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию Отправить сообщение. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки Реагирование. В открывшемся окне в поле **Сообщение** следует ввести сообщение для пользователя и нажать кнопку **Отправить**. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 83). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

Примечание

Сценарий реагирования не работает на агентах LInux.

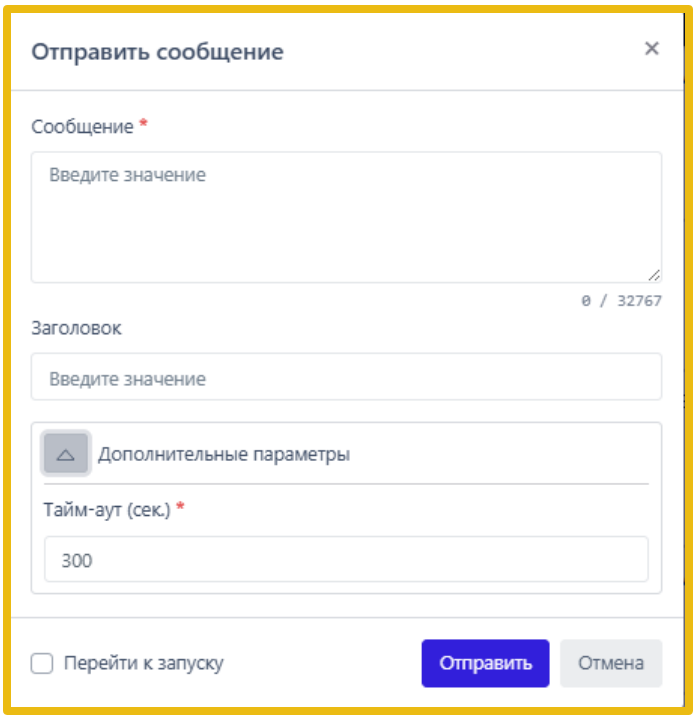


Рисунок 83 – Сценарий отправки сообщения

Блокировка запуска по командной строке

Действие реагирования блокирует запуск процесса по командным строкам (процесса, процесса-родителя и процесса-прародителя). При блокировке можно указать время, в течение которого процесс будет заблокирован.

Примечание

Блокировки (в том числе блокировки файлов и сетевых эндпойнтов) можно просмотреть на агенте с помощью онлайн-терминала (команда block list) и принудительно удалить с помощью параметров нативной команды block. Список агентов с блокировками можно сформировать на странице **Агенты**.

При написании командных строк можно использовать wildcard-символы * и ?. По умолчанию время блокировки устанавливается в значение 0, то есть без ограничений по времени. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Сценарий выполняется на странице **Процесс**. После открытия окна **Блокировка**

запуска процесса по командной строке поля ввода для командной строки процесса, его родителя и прародителя будут автоматически предзаполнены (если у процесса определены родитель и прародитель), исходя из выбора процесса на странице **Процесс**. Для пользователя останется только определить срок действия блокировки в минутах. По умолчанию время действия блокировки устанавливается на 60 минут. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску**. Чтобы у блокировки запуска по командной строке был приоритет над исключениями для программ, необходимо установить флаг **Приоритет над исключениями** (рис. 84). Для исполнения сценария реагирования следует нажать кнопку **Отправить**. Для снятия блокировки необходимо использовать команду **block clear** в онлайн-терминале.

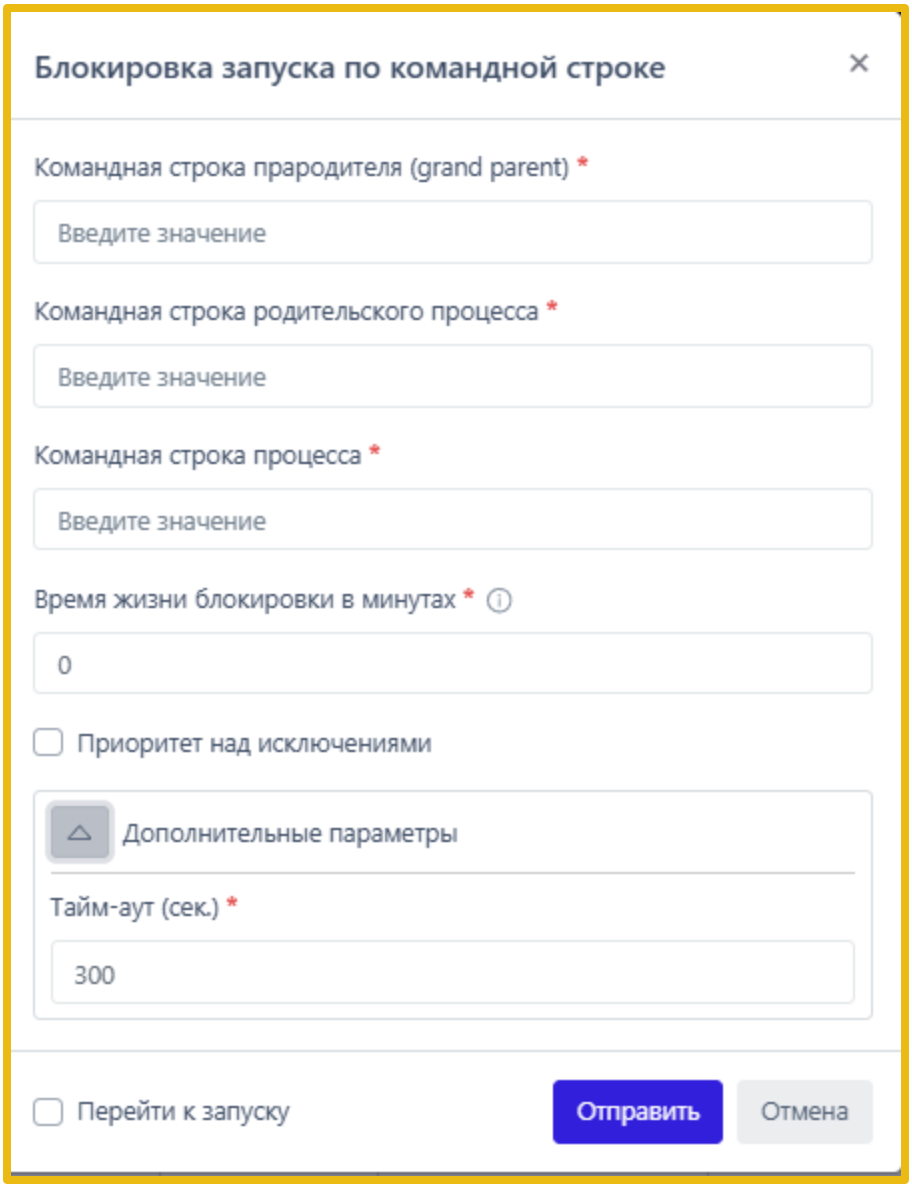
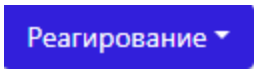


Рисунок 84 – Сценарий блокировки запуска по командной строки

Блокировка доступа к файлу

Действие реагирования блокирует доступ к файлу по хешу SHA-256 или имени файла (под именем файла подразумевается абсолютное имя файла, базовое имя или имя файла, написанное с помощью регулярного выражения, например, *file.txt). При блокировке файла можно указать время, в течение которого файл будет заблокирован, то есть подразумевается, что с файлом ничего нельзя будет сделать. По умолчанию время блокировки устанавливается в значении 60 минут. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Выполнение сценария осуществляется на страницах **Процесс** и **Активность** с помощью кнопок реагирования ( и 

).

В окне **Блокировка доступа к файлу** будет автоматически указано имя файла. Для большей точности можно вместо имени указать хеш-сумму SHA-256 блокируемого файла. Далее необходимо установить время блокировки этого файла. Чтобы снять блокировку необходимо воспользоваться командой **block clear** в онлайн-терминале. Чтобы блокировка доступа к файлу имела приоритет над исключениями для файлов необходимо установить флаг **Приоритет над исключениями**. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 85). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

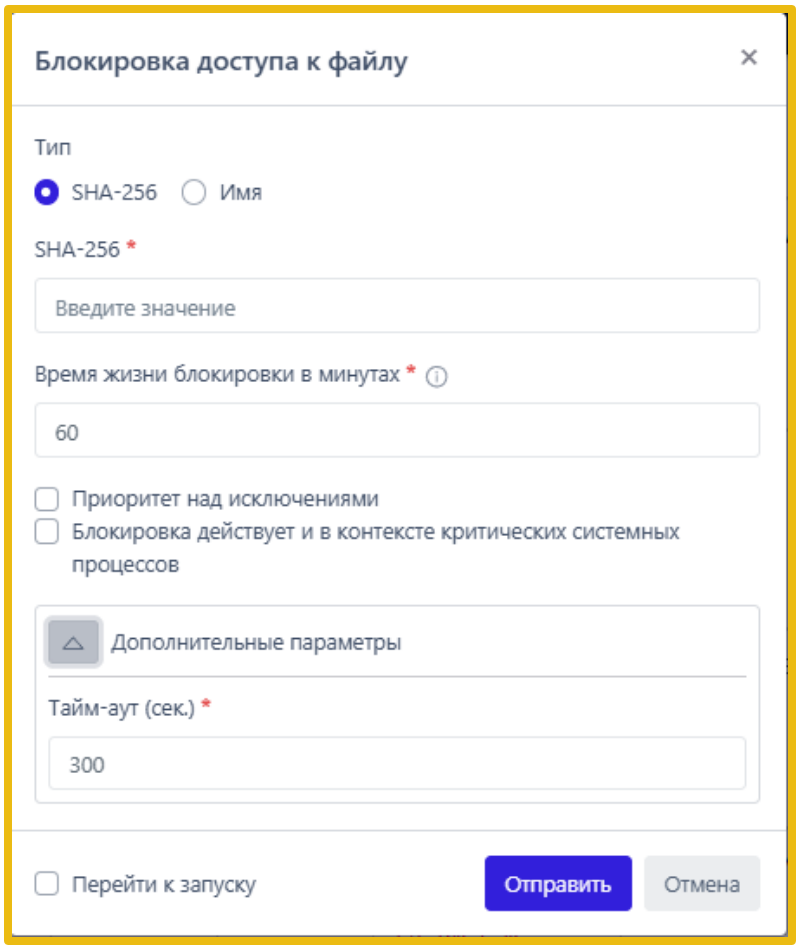


Рисунок 85 – Сценарий блокировки доступа к файлу

Блокировка доступа к сетевому эндпойнту

Действие реагирования позволяет блокировать доступ к определенной конечной точке по доменному имени или IP-адресу сетевой конечной точки (в том числе по локальному имени или адресу). Аналитик может также определить номер порта, по которому будет блокирован доступ к сетевому эндпойнту, и время блокировки этого эндпойнта.

По умолчанию время блокировки устанавливается равным 60 минутам. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Активность** в сетевых событиях нажать кнопку реагирования ( ) и выбрать соответствующую операцию. В открывшемся окне **Блокировка доступа к сетевому эндпойнту** автоматически заполнится IP-адрес удаленного хоста и удаленный порт. Аналитик может поменять значение IP-адреса на доменное имя. Для снятия блокировки следует воспользоваться командой **block clear** в онлайн-терминале. Чтобы блокировка доступа к сетевому эндпойнту

имела приоритет над сетевыми исключениями необходимо установить флаг **Приоритет над исключениями**. Для автоматического перехода к запуску сценария в Планировщике задач необходимо установить флаг **Перейти к запуску** (рис. 86). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

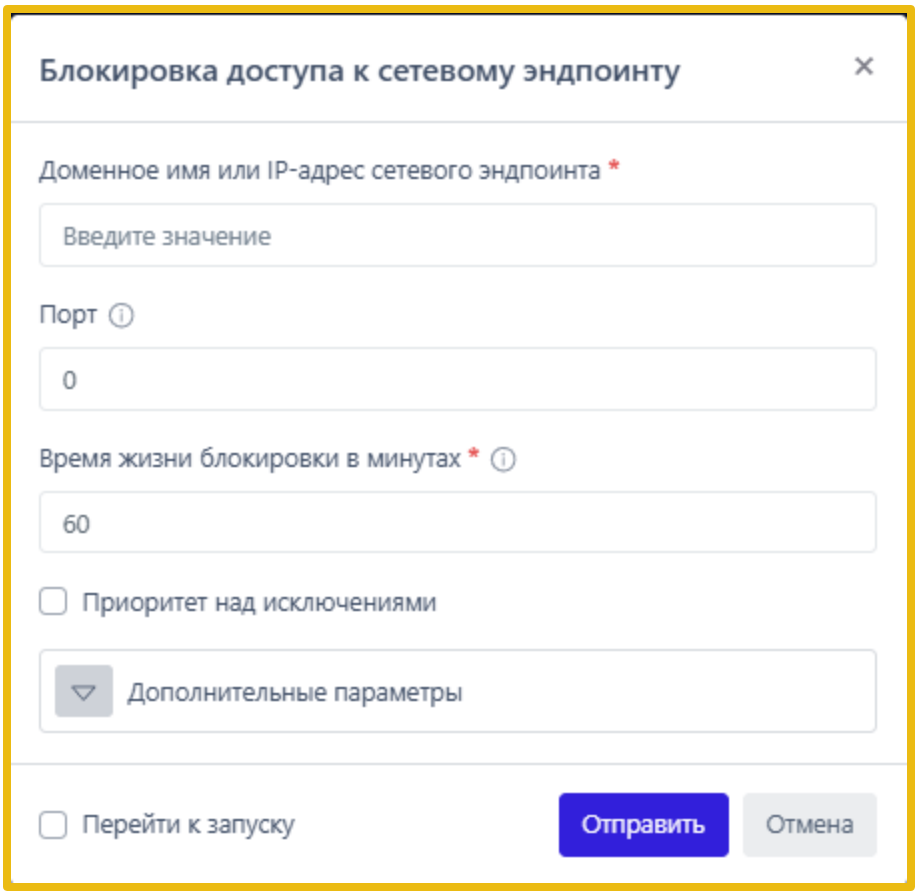


Рисунок 86 – Сценарий блокировки доступа к сетевому эндпоинту

Завершить сетевое соединение

Действие реагирования завершает сетевое взаимодействие по идентификатору сетевого потока (**fluuid** или **flow** в модели данных RT Protect EDR для агентов Windows).

Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Сценарий выполняется на странице **Активность** для сетевых событий. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 87). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

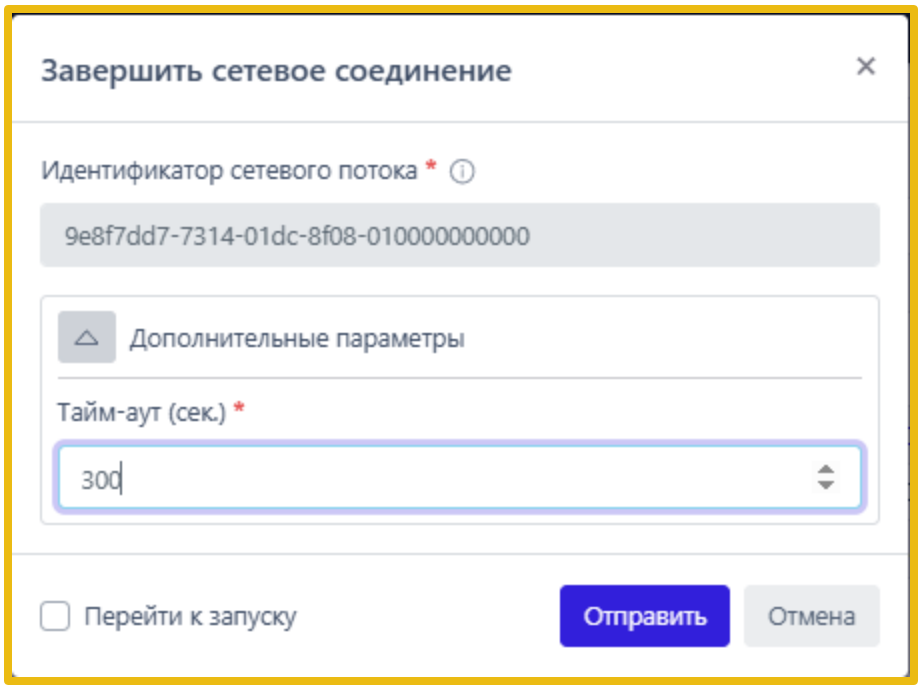


Рисунок 87 – Сценарий завершения сетевого соединения

Завершить процесс

Действие реагирования выполняется на странице **Процесс**. Сценарий завершает выбранный процесс (**uuid** или **pid** в модели данных RT Protect EDR), соответственно, если процесс завершился до вмешательства аналитика, то сценарий становится недоступным для выполнения. При открытии окна **Завершить процесс** будет автоматически заполнено поле **Уникальный идентификатор процесса**. Аналитику только остается установить Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 88). Для выполнения сценария реагирования следует нажать кнопку **Отправить**.

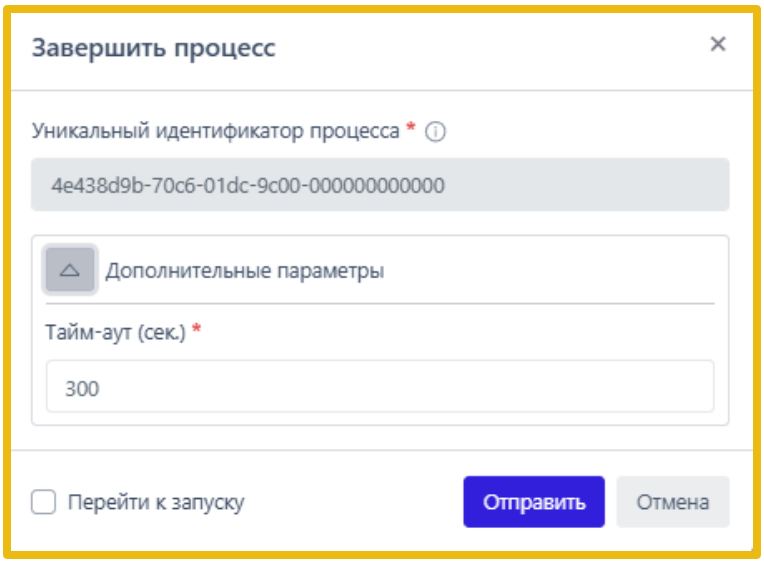


Рисунок 88 – Сценарий завершения процесса

Скачать файл из Хранилища

Действие реагирования выполняет скачивание файла из **Хранилища** и помещает этот файл на компьютер с агентом. Для выполнения действия необходимо получить ссылку на файл на странице **Хранилище** во вкладке **Загрузка файлов** ( ). Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** ( ), после чего выбрать операцию Скачать файл из Хранилища . На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки Реагирование . В открывшемся окне вставить ссылку на файл и ввести значение каталога размещения файла на агенте (по умолчанию файл будет размещен по пути: C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\downloads).

Примечание

При использовании постоянной ссылки на файл в строке **Имя файла** необходимо явно указать имя файла со страницы **Загрузка файлов** раздела **Хранилище**.

Для перезаписи файла на компьютере с агентом следует установить флаг **Перезаписать файл**. Для автоматического перехода к запуску сценария в Планировщике задач необходимо установить флаг **Перейти к запуску** (рис. 89). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

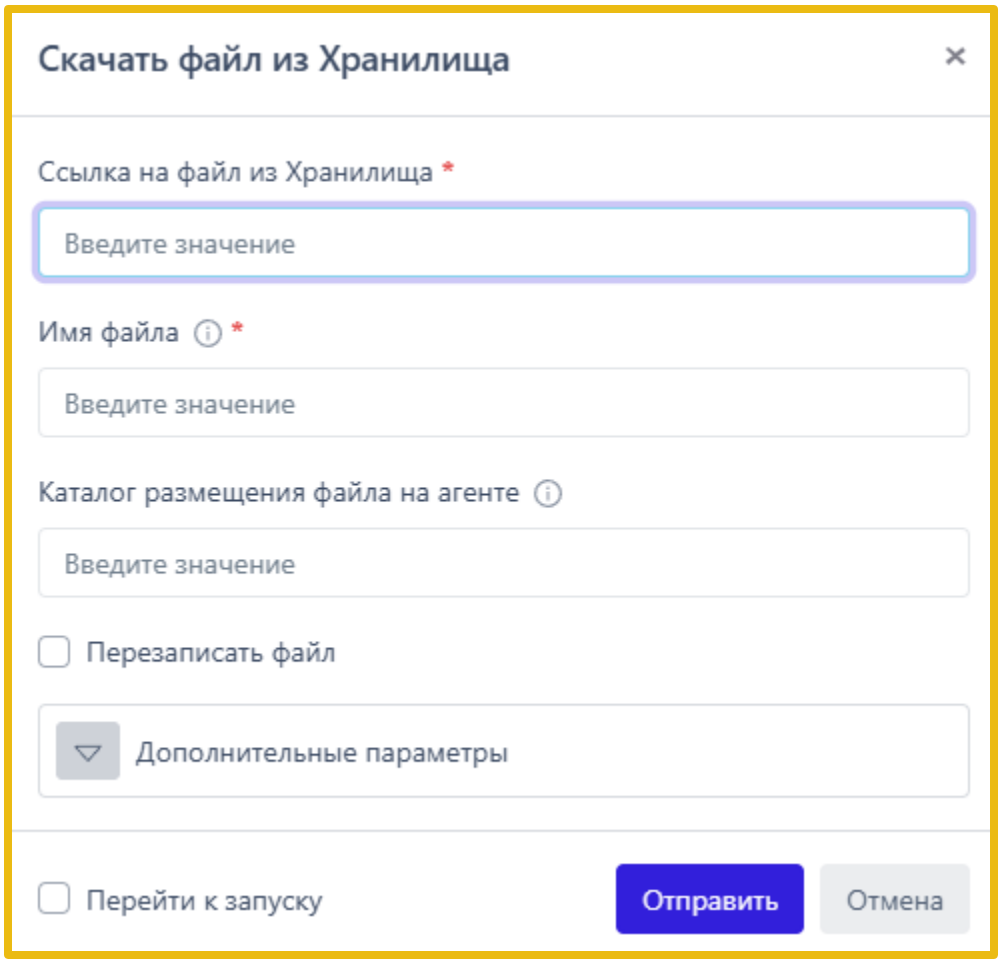


Рисунок 89 – Сценарий загрузки файла из Хранилища

Завершить группу процессов

Действие реагирования завершает выбранную группу процессов. Действие реагирования запускается со страницы **Процесс**. Для выполнения действия автоматически подставляется уникальный идентификатор группы процессов (**hid** в модели данных RT Protect EDR). Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Сценарий запускается со страницы **Процесс**. В открывшемся окне ввести уникальный идентификатор группы процессов.

Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску**). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

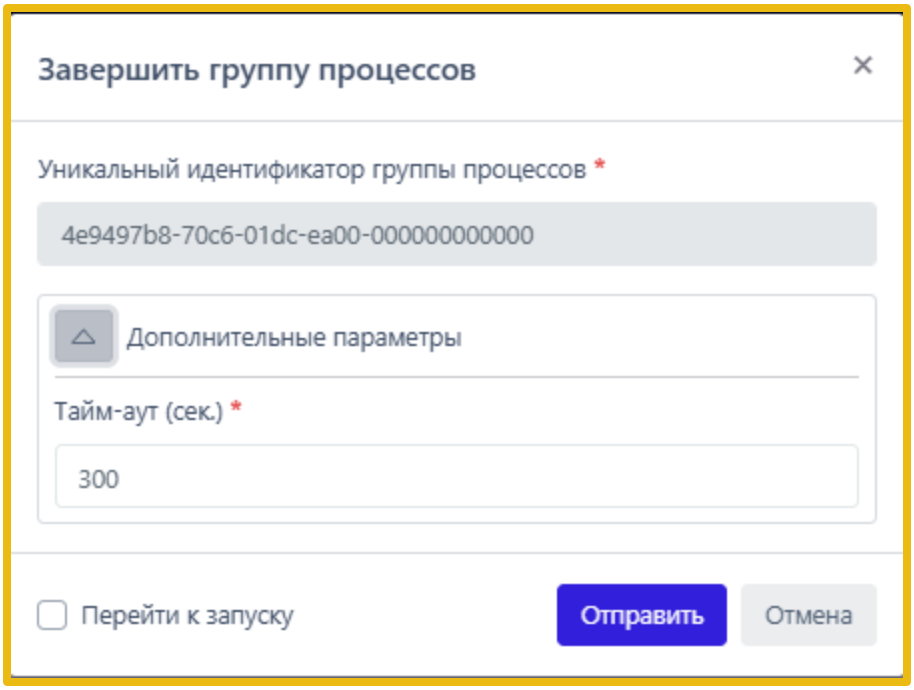
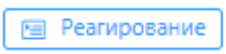


Рисунок 90 – Сценарий завершения группы процессов

Заблокировать учетную запись пользователя

Действие реагирования отключает учетную запись выбранного пользователя и запрещает ему вход в систему, сохраняя при этом все данные пользователя (профиль, файлы). Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию 

. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. Также сценарий можно выполнить на странице **Активность**. После открытия окна **Заблокировать учетную запись пользователя** следует ввести имя пользователя, учетная запись которого будет заблокирована (разблокировать учетную запись можно с помощью онлайн-терминала, команда net user Имя_пользователя /active:yes). В случае с запуском сценария реагирования на странице **Активность**, имя пользователя будет подставляться автоматически.

Для перехода к запуску сценария в Планировщике задач необходимо установить флаг **Перейти к запуску** (рис. 91). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

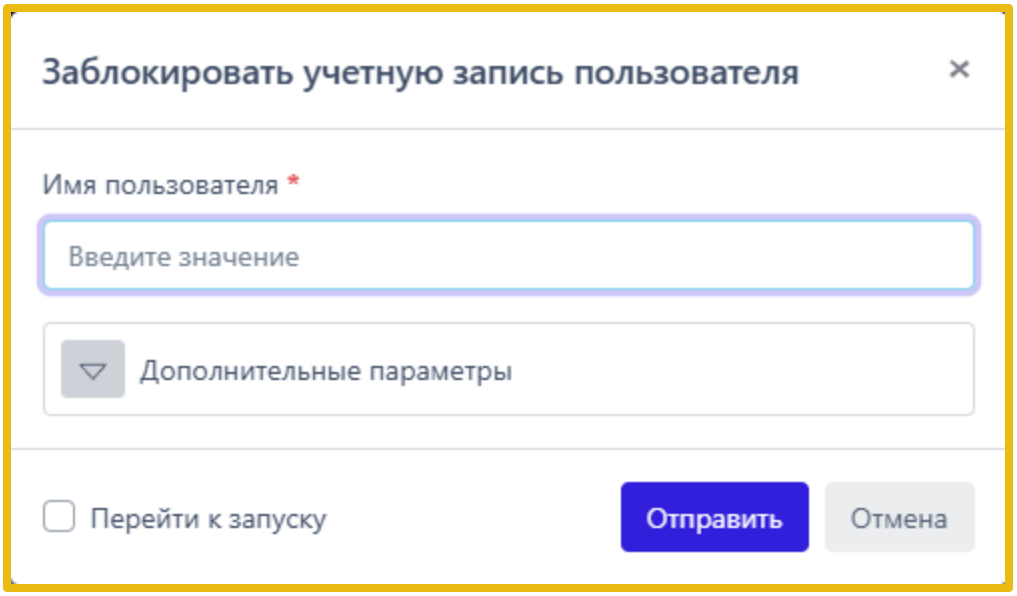
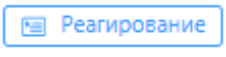


Рисунок 91 – Сценарий блокировки учетной записи пользователя

Завершить сеанс пользователя

Действие реагирования принудительно завершает активную сессию пользователя, при этом несохраненные данные будут полностью потеряны и запущенные программы принудительно закрыты. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию 

. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. Также сценарий можно выполнить на странице **Активность**. После открытия окна **Завершить сеанс пользователя** следует ввести имя пользователя, сеанс которого необходимо завершить. Для сценария, выполняемого на странице **Активность** имя пользователя устанавливается автоматически. Для перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 92). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

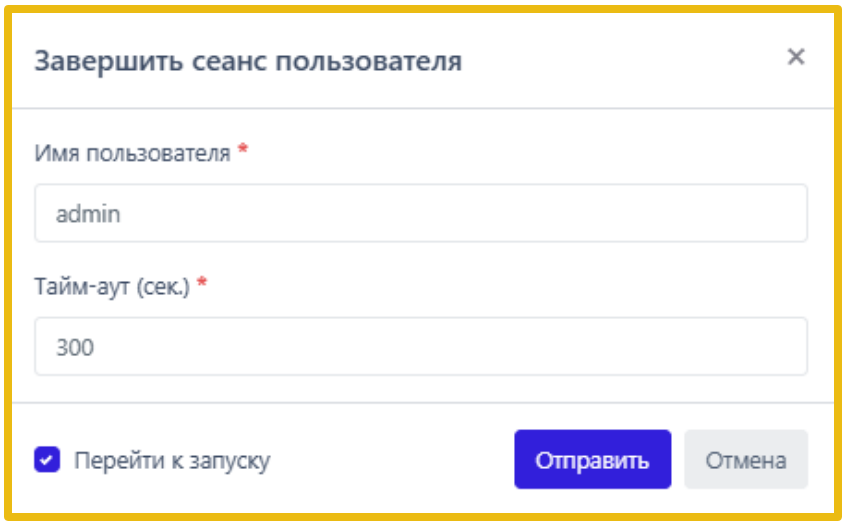
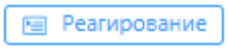


Рисунок 92 – Сценарий завершения сеанса пользователя

Заблокировать сеанс пользователя

Действие реагирования блокирует компьютер с установленным агентом, активируя экран блокировки Windows и требуя повторного ввода пароля для доступа. При блокировании сохраняются все запущенные приложения и открытые файлы. Действие реагирования аналогично нажатию Win+L на компьютере. Тайм-аут на выполнение команды по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию 

. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 93). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

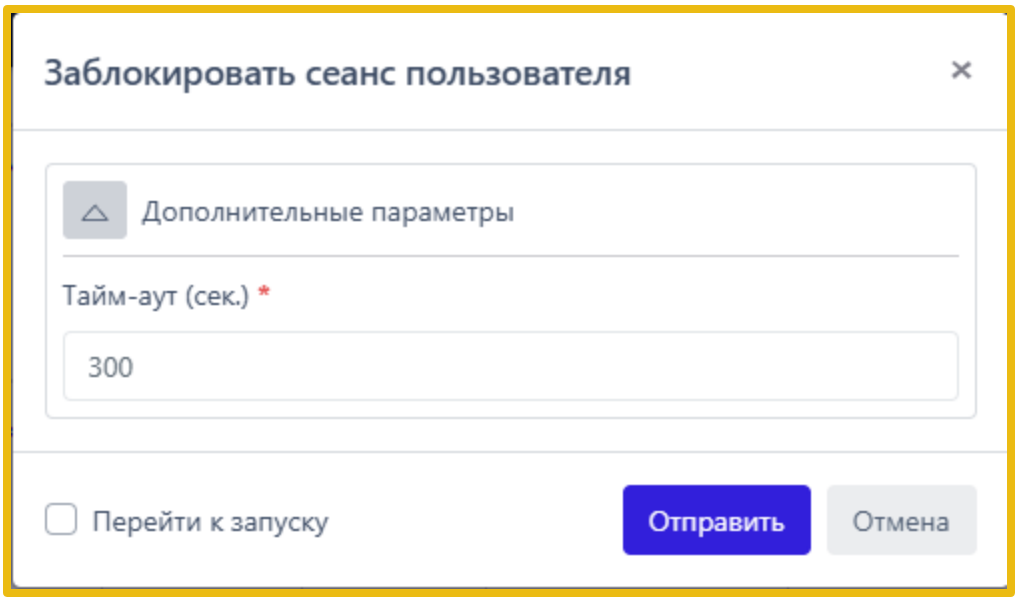
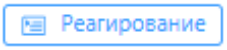


Рисунок 93 – Сценарий блокировки сеанса пользователя

Выключить компьютер

Действие реагирования позволяет выключить компьютер с установленным на нем агентом. Аналитик может выполнить действие с задержкой выключения, устанавливаемой в секундах (по умолчанию выключение выполняется без задержки). Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию 

. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. В открывшемся окне необходимо ввести количество секунд задержки перед выключением (по умолчанию выключение производится без задержек). Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 94). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

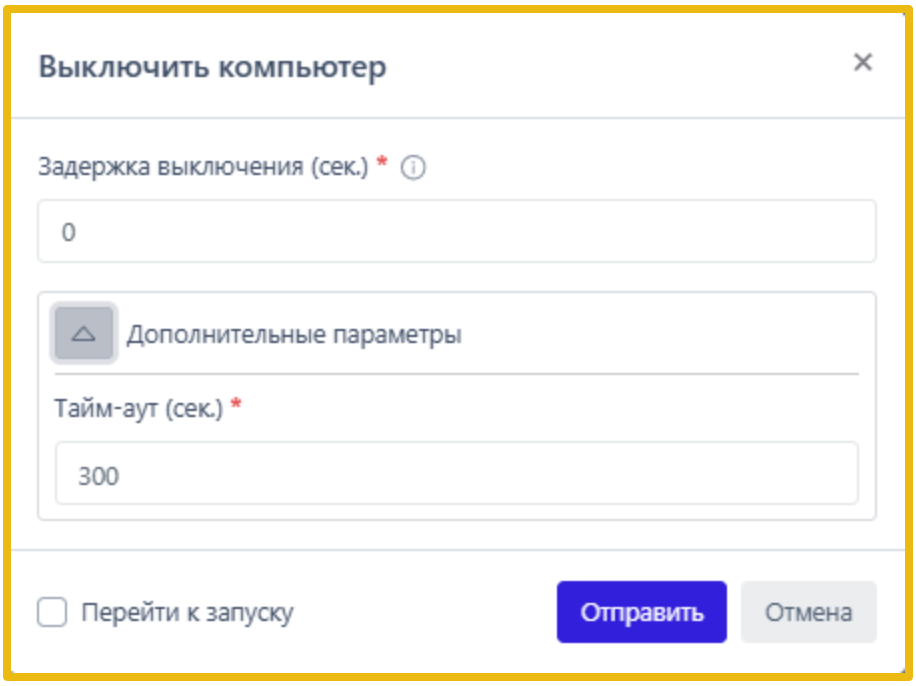


Рисунок 94 – Сценарий выключения компьютера

Собрать цифровые улики

Действие реагирования запускает Poweshell-скрипт, который собирает на компьютере с установленным агентом следующую информацию и помещает ее в zip-архив в раздел **Хранилище**:

1) Системная информация:

– IP-конфигурация и сетевые интерфейсы;

– информация о хосте и ОС;

– теневые копии (Shadow Copies);

– подключенные устройства;

2) Сетевые данные:

– установленные TCP-соединения;

– кеш DNS;

– сетевые шары (SMB);

– RDP-сессии;

– удаленно открытые файлы;

3) Пользовательские данные:

– активные и локальные пользователи;

– история PowerShell (текущий пользователь + все пользователи);

– автозагрузка и точки закрепления;

– запущенные процессы (с хешами SHA256);

4) Активность системы:

– запущенные сервисы;

– запланированные задачи;

– установленные драйверы;

– недавно установленное ПО;

5) Безопасность:

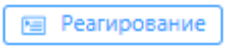
– события безопасности за указанный период;

– файлы Event Viewer (.evtx);

– исключения Защитника Windows;

– логи Microsoft Defender (MPLogs);

6) Браузеры и т.д.

Скрипт позволяет настраивать период поиска, по умолчанию задается период равный двум дням. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию **Собрать цифровые улики**. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. После открытия окна **Собрать цифровые улики** необходимо ввести имя результирующего архива. Для перезаписи архива в Хранилище необходимо выбрать флаг **Перезаписать файл**. Для автоматического перехода к запуску сценария в Планировщике задач необходимо установить флаг **Перейти к запуску** (рис. 95). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

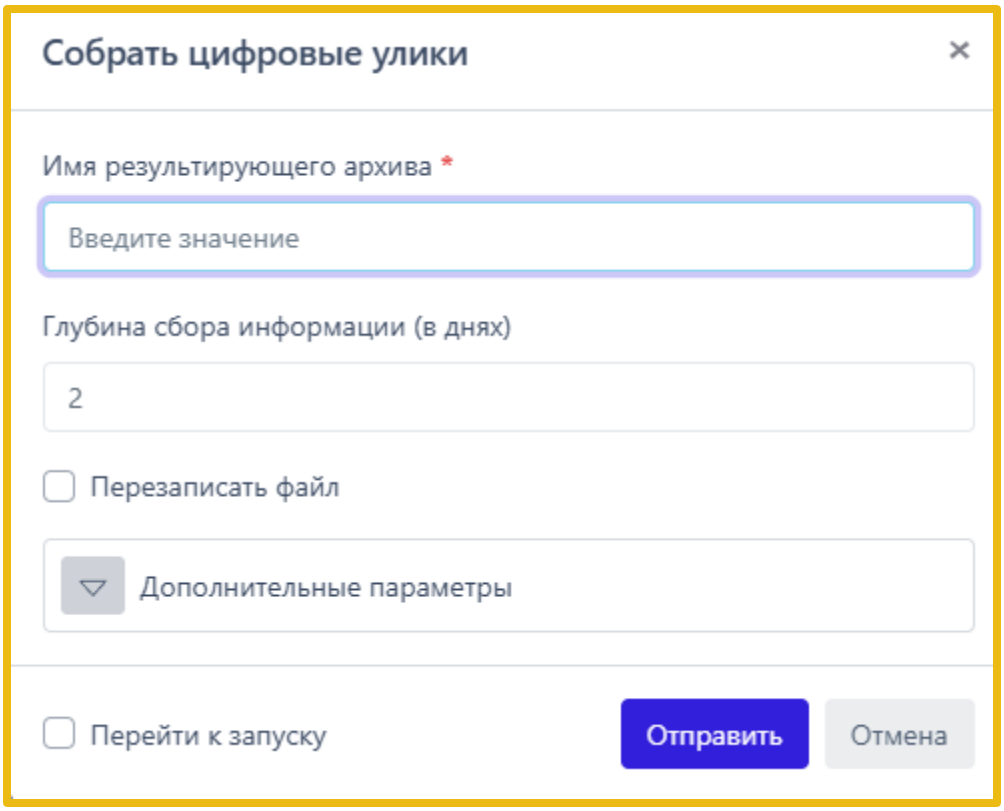


Рисунок 95 – Сценарий сбора форензики

Ремедиация

Операция реагирования, которая откатывает действия, выполняемые выбранной группой процессов (**hid** в модели данных RT Protect EDR). На странице **Процесс** группы процессов помечаются синим значком ( ). Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Операция реагирования доступна на странице **Процесс** по кнопке **Реагирование**. После выбора операции **Ремедиация** для идентификатора группы процессов открывается одноименное окно **Ремедиация**, в котором необходимо указать временной диапазон, на значение которого необходимо откатить изменения в файловой или реестровой системе (для чего в окне есть соответствующие чекбоксы).



Примечание

Максимальный срок отката файловой и реестровой системы составляет 72 часа.

Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 96). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

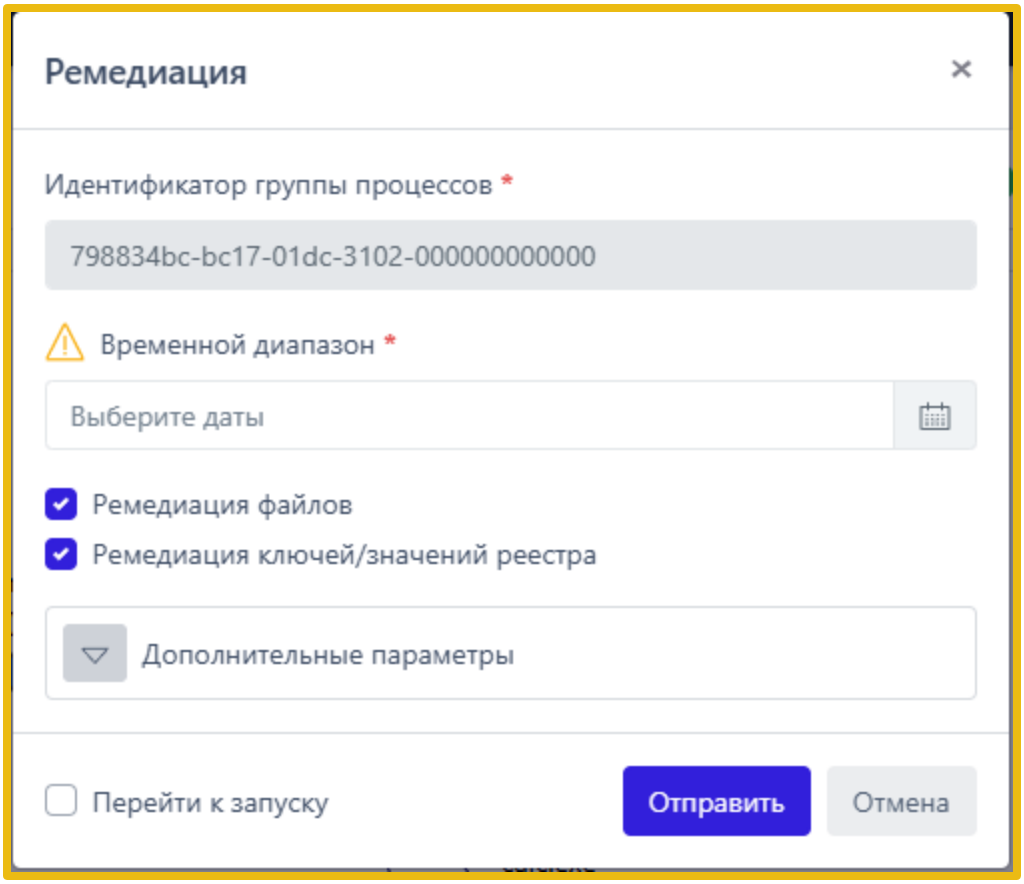


Рисунок 96 – Сценарий ремедиации

Примечание

Ремедиация не поддерживается агентом Linux.

Реакция на вердикт TI для файлов

Операция реагирования, которая определяет реакцию на вердикт TI для файловых артефактов. Является внутренним сценарием реагирования, активируется при обнаружении хеша вредоносного файла алгоритмом TI-платформы. Условия и набор действий можно изменить или дополнить, например, сетевой изоляцией или сбором форензики). Сценарий отправляет команду stop в рамках реагирования (завершает процесс при запуске процесса либо при срабатывании скриптового движка во время доступа к файлу).

Реакция на вердикт TI для сети

Операция реагирования, сетевой аналог файлового сценария, которая определяет реакцию на вердикт TI для сетевых артефактов, по умолчанию прерывает сетевое соединение по идентификатору сетевого соединения для сетевых артефактов (IP-адрес или домен), имеющих вердикт вредоносный. Является внутренним сценарием реагирования, активируется при обнаружении вредоносного IP-адреса/домена.

Сценарий реагирует на сетевые индикаторы компрометации: фоновый процесс TI-менеджера сети опрашивает сетевые события агентов, запрашивает по ним вердикты TI и при «вредоносном» вердикте ставит Планировщику задач одноразовую задачу по этому сценарию, передавая в контекст всё событие. В результате срабатывания сценария выполняется разрыв активного соединения для сетевых событий определённых подтипов (исходящее и входящее соединение и SSL HELLO) уже установленное вредоносное соединение немедленно разрывается по идентификатору потока.

Сделать дамп памяти процесса

Сценарий реагирования делает дамп памяти процесса по его идентификатору (**pid** или **uuid** в модели данных RT Protect EDR). Дамп в агентах Windows сохраняется по пути **C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\dumps**. На агентах Linux дамп сохраняется по пути **/opt/avd/dumps**. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Операция выполняется на странице **Процесс** с помощью кнопки **Реагирование**. При нажатии кнопки и выборе соответствующей операции открывается окно **Сделать дамп памяти процесса**, в котором автоматически проставляется идентификатор выбранного процесса. Для перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 97). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

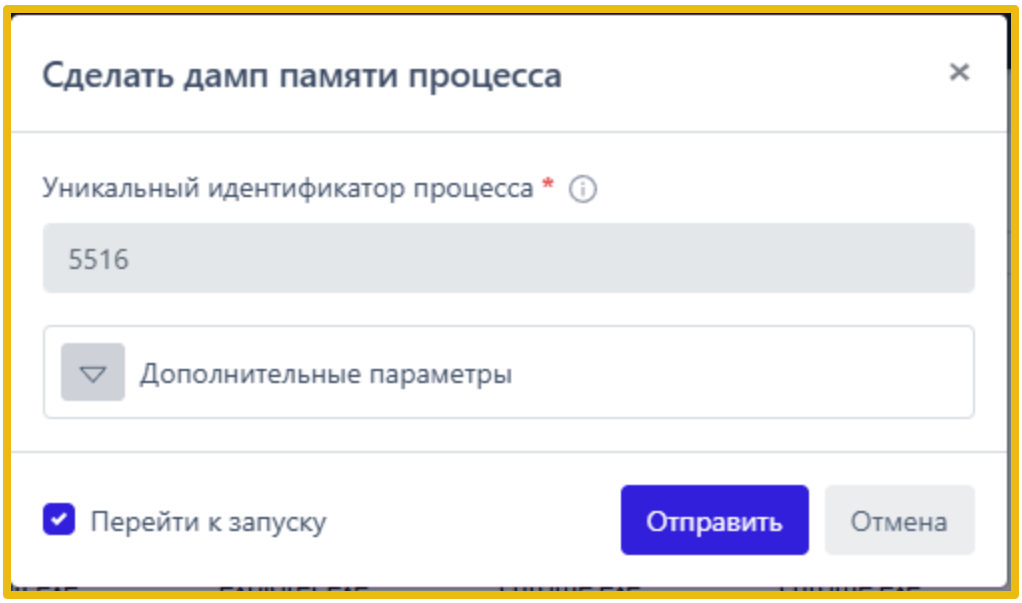


Рисунок 97 – Сценарий создания дампа памяти процесса

Сканировать память процесса

Сценарий реагирования выполняет сканирование памяти процесса по его идентификатору (**uuid** или **pid** в модели данных RT Protect EDR) с помощью YARA-правил (память).

Примечание

В случае срабатывания правила будет сформировано обнаружение, которое в зависимости от критичности может привести к созданию в Программе инцидента (реализовано на текущий момент в Windows-агентах). Критичность устанавливается при создании YARA-правила для памяти в секции **meta**.

Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Сценарий выполняется на странице **Процесс** с помощью кнопки **Реагирование**. Идентификатор процесса вводится в окне **Сканировать память процесса** Программой автоматически при выборе процесса. Для перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 98). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

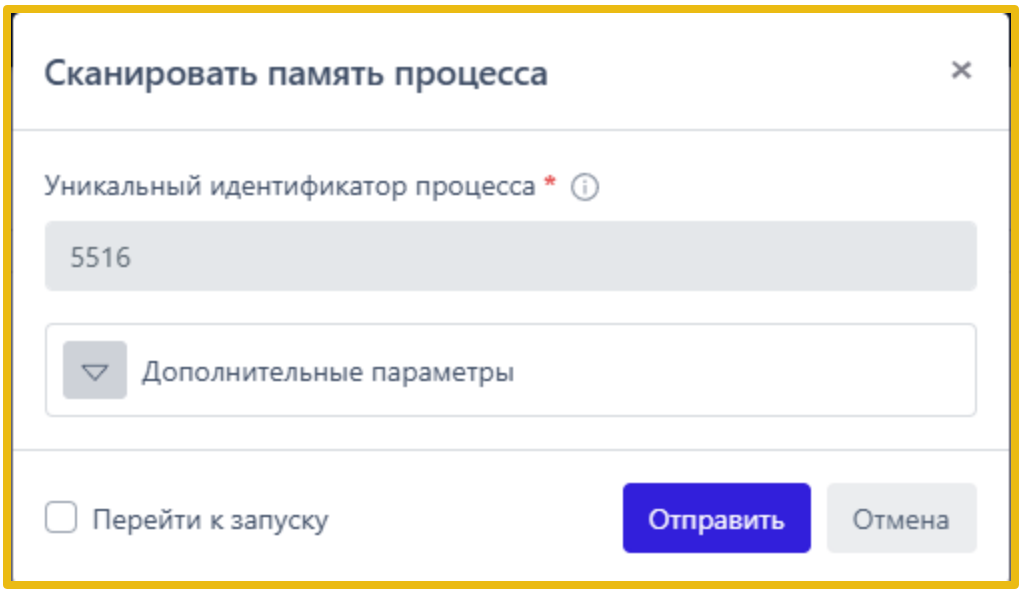
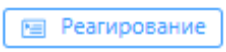


Рисунок 98 – Сценарий сканирования памяти процесса

Сканировать файловую систему

Действие реагирования выполняет команду **fsscan**, которая сканирует файловую систему по правилам YARA для файлов. При выполнении действия реагирования необходимо определить каталог, который будет просканирован. Можно выполнять сканирование не только по правилам, прикрепленным к агенту, но и по файлу на агенте со скомпилированными YARA-правилами (yarc). Для этого в сценарии вводится опциональный параметр **rules_path**. После завершения сканирования отчет о сканировании будет сохранен по пути, указанному пользователем при заполнении сценария сканирования. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам.

Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач**. Для выполнения сценария необходимо на странице **Агенты** выделить требуемое число агентов и нажать кнопку **Реагирование для выбранных агентов** (), после чего выбрать операцию 

. На странице **Агент** список сценариев открывается в области **Реагирование** с помощью кнопки 

. В открывшемся окне ввести имя каталога, сканирование которого необходимо произвести. Для автоматического перехода к запуску сценария необходимо установить флаг **Перейти к запуску** (рис. 99). Для исполнения сценария реагирования следует нажать кнопку **Отправить**.

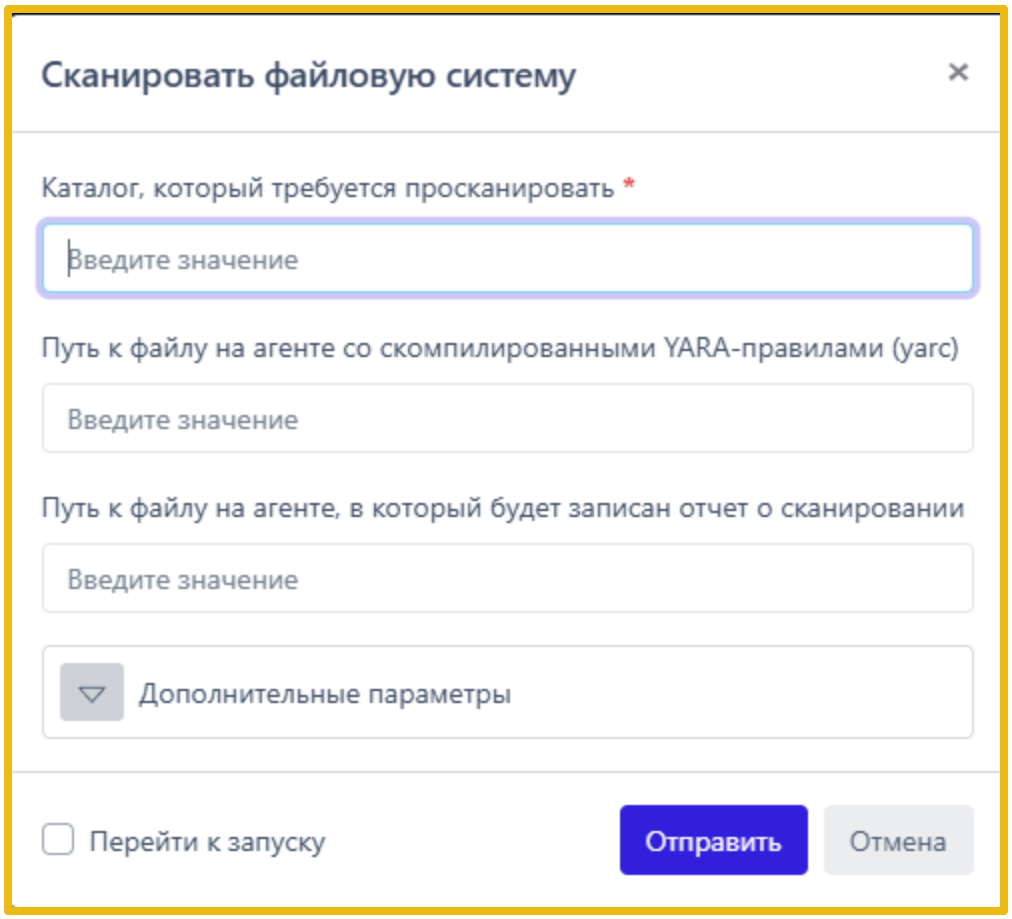


Рисунок 99 – Сценарий сканирования файловой системы

При выполнении сценария будут создаваться обнаружения в случае срабатывания YARA-правил для файлов (в агенте Windows). Для агентов Linux будет сформирован отчет, в котором будут отображаться все срабатывания. Отчет формируется по пути **/opt/avd/reports**.

Реакция на инцидент

По умолчанию сценарий отправляет агенту пустую команду. Является внутренним сценарием реагирования. Можно произвольно менять сценарий реагирования, чтобы при создании инцидентов выполнялись действия, определенные уполномоченными пользователями, например, отправка команды на автоматическую изоляцию агента. В этом случае на изоляцию будет отправлен компьютер с агентом, на котором инцидент был создан (на котором было обнаружено событие, приведшее к созданию инцидента).

Удалить файл/каталог

Сценарий реагирования выполняет удаление указанного файла или каталога. Тайм-аут на выполнение сценария по умолчанию равен 300 секундам. Выполнение сценария реагирования отслеживается на странице **Запуски** в **Планировщике задач** или на странице соответствующего агента в области **Запуски Агента**. Сценарий выполняется на страницах **Активность**, **Агенты** и **Процесс**. На страницах **Активность** и **Процесс** имя каталога, удаление которого необходимо произвести, автоматически подставляется в соответствующее поле. Для перехода к запуску сценария в Планировщике задач необходимо установить флаг **Перейти к запуску** . Для исполнения сценария реагирования следует нажать кнопку **Отправить** (рис. 100).

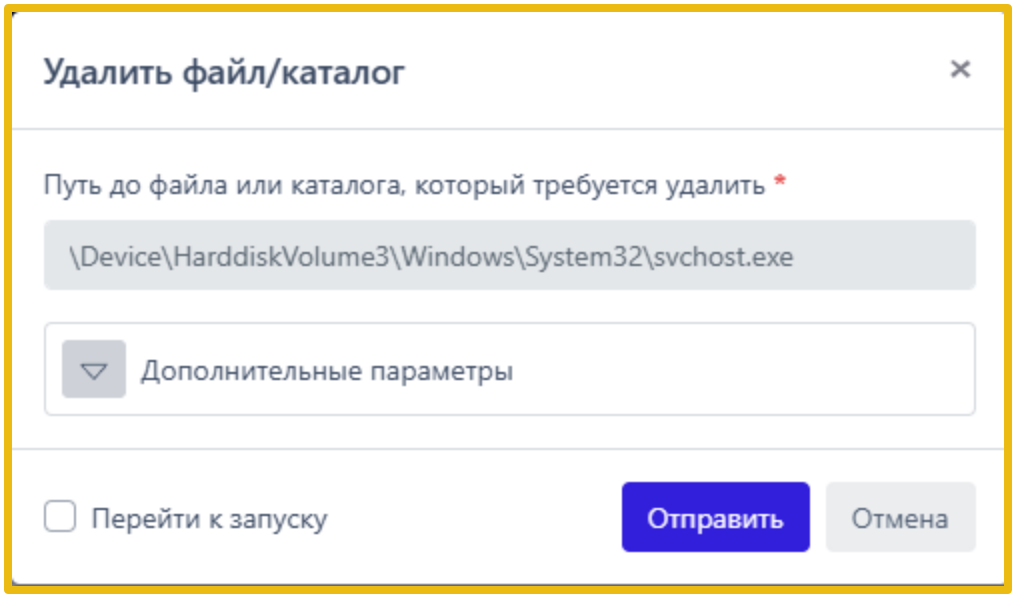


Рисунок 100 – Сценарий удаления файла, каталога

Отправить файл на анализ в TI

Сценарий реагирования, который ставит агенту задачу выгрузить указанный файл и передать его на проверку во встроенную среду анализа TI (локальную среду проверки файлов). Сценарий доступен на странице **Процессы**, **Активность** и **Агенты**. При выборе действия открывается окно **Отправить файл на анализ в TI**, в котором необходимо указать имя отправляемого на анализ файла. В случае с отправкой со страниц **Процессы** и **Активность** имя файла будет определено автоматически. Далее следует установить или снять флажки **Файл более 32 Мб** и **Перейти к запуску**, после чего определить тайм-аут (по умолчанию он составляет 300 секунд). Для исполнения сценария реагирования необходимо нажать кнопку **Отправить** (рис. 101).

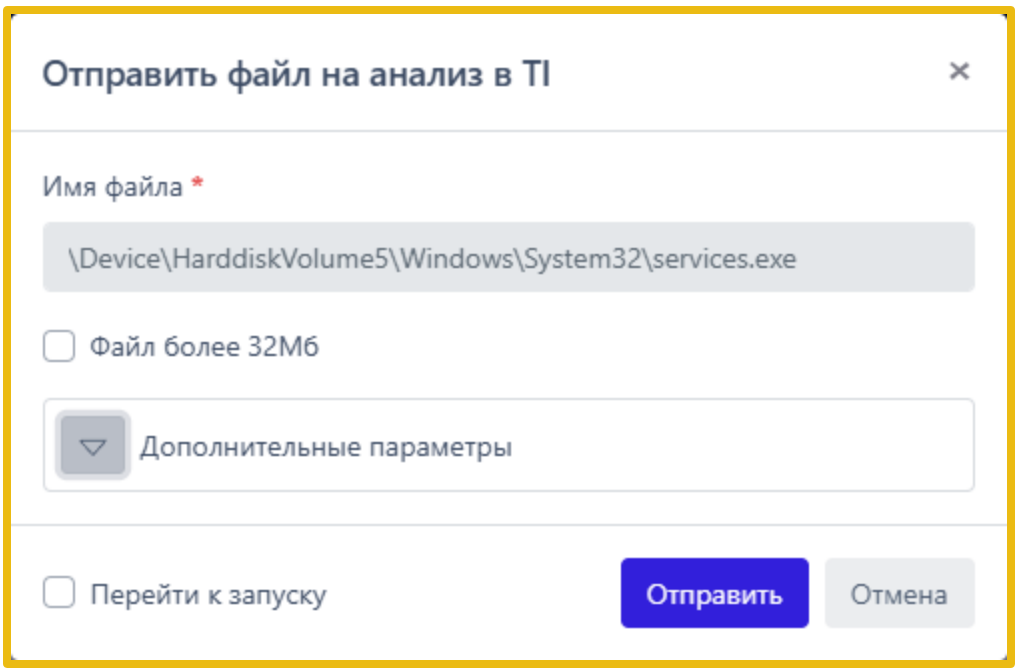


Рисунок 101 – Сценарий отправки файла на анализ в TI

Сделать дамп физической памяти

Сценарий реагирования, который создает дамп физической памяти выбранного агента. Сценарий доступен на странице **Агенты**. При выборе действия открывается окно **Сделать дамп физической памяти**, в котором пользователь может указать имя файла дампа (необязательное условие). Далее можно установить флажки **Перезаписать файл** и **Перейти к запуску**, если это необходимо. и установить время тайм-аута. Для исполнения сценария реагирования необходимо нажать кнопку **Отправить** (рис. 102).

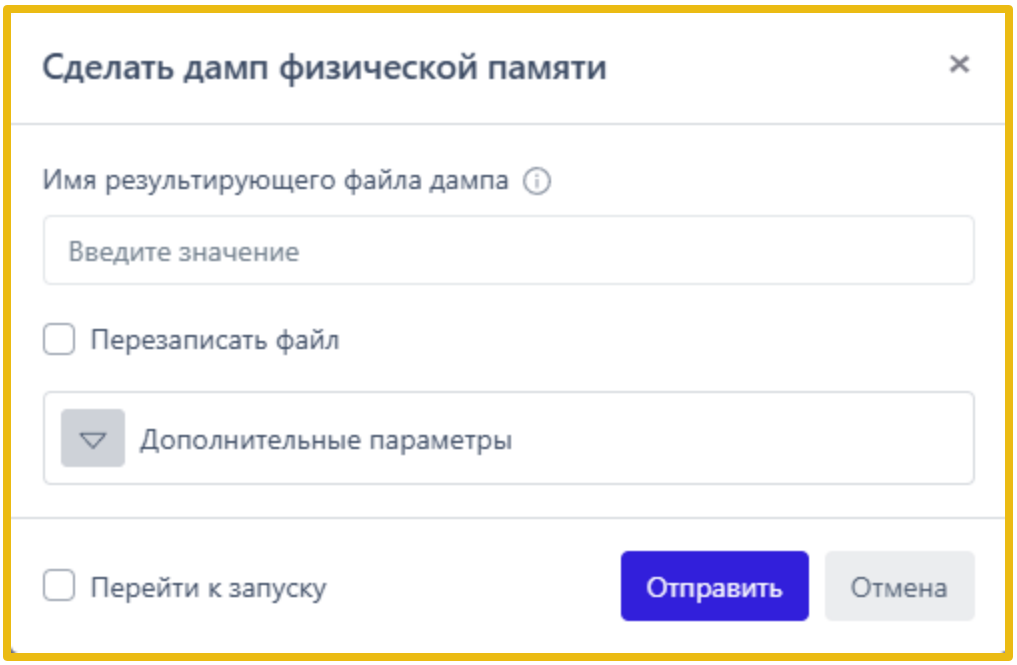


Рисунок 102 – Сценарий создания дампа физической памяти

11.23.2. Параметры сценариев реагирования

Сценарии реагирования могут быть написаны с определенными параметрами. Список параметров и опций в сценариях реагирования приведен в таблице 60.

Таблица 60 – Параметры и опции в сценариях реагирования

Сценарии	Параметры	Описание
Загрузить файл в Хранилище	filename	Имя файла (можно указывать имя файла с буквой или \device\hardiskvolume)
	-xl	Опция позволяет загрузить в Хранилище файл размером более 32 МБ
	-y	Опция для перезаписи существующего файла
Сетевая изоляция	on_off	On, 1 или true – параметр для включения изоляции; Off, 0 или false – параметр для выключения изоляции
Отправить сообщение	-b64	Опция, которая позволяет Отправляет сообщение в кодировке base64
	-t=<Заголовок>	Параметр для написания текста заголовка
	-i=<Иконка сообщения>	Параметр для определения иконки сообщения (число от 0 до 3 (0 – нет иконки, 1 – информация, 2 – предупреждение, 3 – ошибка))
Блокировка запуска процесса по командной строке	cmdlg	Командная строка прародителя (можно использовать wildcard-символы * и ?)

Сценарии	Параметры	Описание
	cmdlp	Командная строка родителя (можно использовать wildcard-символы * и ?)
	cmdl	Командная строка процесса (можно использовать wildcard-символы * и ?)
	-b64	Опция, которая устанавливает, что командные строки имеют кодировку base64
	-ttl	Опция, устанавливающая время жизни блокировки в минутах (0 - без ограничений); по умолчанию 60
Блокировка доступа к файлу	sha256	Хеш SHA-256 файла
	name	Имя файла (можно указывать имя файла с буквой или \device\hardiskvolume)
	overrideExclusions	True, если выбрана опция **Приоритет над исключениями** (-force), иначе false
	-ttl	Опция, устанавливающая время жизни блокировки в минутах (0 - без ограничений); по умолчанию 0
	add_params	Дополнительные параметры
Блокировка доступа к сетевому эндпойнту	host	доменное имя или IP-адрес сетевого эндпоинта
	port	номер порта (0 означает "любой порт") сетевого эндпоинта
	-ttl	Опция, устанавливающая время жизни блокировки в минутах (0 - без ограничений); по умолчанию 0
	overrideExclusions	True, если выбрана опция **Приоритет над исключениями** (-force), иначе false
	add_params	Дополнительные параметры
Завершить сетевое соединение	fluuid	уникальный идентификатор сетевого потока
	add_params	Дополнительные параметры
Завершить процесс	uuid	Уникальный идентификатор процесса
	add_params	Дополнительные параметры
Скачать файл из Хранилища	-y	Опция для перезаписи существующего файла
	downLink	Постоянная ссылка на файл из Хранилища
	filename	Имя файла на агенте
	agentTargetDir	Каталог размещения файла на агенте (если не указан, то файл будет размещен в каталог C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\downloads
	add_params	Дополнительные параметры

Сценарии	Параметры	Описание
	overwriteIfExists	True, если указана опция **Перезаписать файл, если он существует**, иначе false (скачать файл из Хранилища на агент можно только по постоянной ссылке)
Завершить группу процессов	hid	Уникальный идентификатор группы процессов
	add_params	Дополнительные параметры
Заблокировать учетную запись пользователя	usr	Имя пользователя
Завершить сеанс пользователя		
Выключить компьютер	timeout	Задержка выключения (в минутах; по умолчанию 0, т.е. без задержки)
Ремедиация	id	ID группы процессов (hid)
	range	Диапазон времени (UTC)
	-files	Опция ремедиации файлов
	restoreFiles	True, если выбрана опция Ремедиация файлов; иначе false (как минимум один из параметров: restoreFiles, restoreRegistry должен быть задан в true)
	-registry	Опция ремедиации реестра
	restoreRegistry	True, если выбрана опция Ремедиация реестра; иначе false
	add_params	Дополнительные параметры
Сделать дамп памяти процесса; Сканировать память процесса	uuid	Уникальный идентификатор процесса
	add_params	Дополнительные параметры
Сканировать файловую систему	scan_path	Каталог, который требуется просканировать
	add_params	Дополнительные параметры
	rules_path	Путь к файлу на агенте со скомпилированными YARA-правилами (yarc)
	out_path	Путь к файлу на агенте, в который будет записан отчет о сканировании
Удалить файл/каталог	path	Путь до файла или каталога, который требуется удалить
Отправить файл на анализ в TI	filename	Имя файла (можно указывать имя файла с буквой или \device\hardiskvolume)
	allowLargeFiles	True, если выбрана опция **Файл более 32 Мб**, иначе false
	add_params	Дополнительные параметры
Сделать дамп физической памяти	filename	Имя результирующего файла дампа; если не задано, то генерируется автоматически
	overwrite	True, если указана опция **Перезаписать файл**, если он существует; иначе false
	add_params	Дополнительные параметры

11.24 Просмотр графиков

Раздел **Графики** — это рабочее пространство для визуального анализа производительности и состояния защищаемых хостов. Он позволяет в реальном времени отслеживать метрики выбранных агентов, сравнивать поведение нескольких машин на одном экране и быстро переходить от аномалии на графике к породившим её событиям.

Экран состоит из двух частей:

1) Панель управления — добавление новых графиков и общие настройки отображения.

2) Область графиков — набор карточек, каждая из которых отображает одну метрику одного агента.

В шапке панели расположены кнопки выбора **Ширина графиков** — переключатель 50%/100%. В режиме 50% карточки выстраиваются по две в ряд (компактный обзор), в режиме 100% — на всю ширину с увеличенной высотой графика (детальный просмотр). Также в шапке панели расположена кнопка **Удалить все графики**, которая очищает рабочее пространство одним действием.

Ниже находится форма добавления графика:

– **Агент** — выбор хоста с поиском. Рядом с полем выбора агента находится фильтр выбора агента по группе (), в списке агентов отображаются только 20 случайно выбранных агентов, поэтому для поиска конкретного агента необходимо воспользоваться строкой ввода имени агента, агента можно искать по неполному соответствию;

– **Выбор метрики** — выпадающий список, сгруппированный по двум категориям: **Состояние агента** и **Состояние ПК агента**;

– **Выбор интервала** — преднастроенные диапазоны (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца) либо произвольный период по датам;

– Кнопка  добавляет график с выбранными параметрами в рабочее пространство (доступна только после выбора агента).

Доступные метрики:

1) Состояние агента — потребление ресурсов самим средством защиты:

– Загрузка ЦП и памяти службой и драйвером агента;

– Загрузка ЦП мониторами процессов, сетевых соединений, файловых операций, реестра и модулем ИА (механизмом проверки индикаторов атак);

– Динамика подсчёта хешей и сканирования файлов (Кб/с).

2) Состояние ПК агента — общесистемные показатели хоста:

– Загрузка ЦП и памяти (%);

– Процессы, нити, дескрипторы;

– Загрузка диска на чтение/запись (Кб/с);

– Загрузка сети на приём/передачу (Кбит/с);

– Количество сетевых соединений.

11.24.1. Работа с карточкой графика

Каждая карточка автономна и предоставляет следующие возможности:

– Просмотр заголовока — имя агента со ссылкой на его карточку и бейдж активности (активен/не активен);

– Смена агента, метрики и интервала «на лету» — параметры можно менять прямо в карточке, не пересоздавая её;

– Агрегирующая функция — переключатель **Среднее/Минимум/Максимум**, определяющий, какое значение из точки данных выводится на график;

– Подсказка при наведении курсора мыши — точное значение и время;

– Закрытие графика — значок в правом верхнем углу ( ).

Графики счётных метрик (процессы, нити, дескрипторы, соединения) строятся ступенчатой линией, остальные — сглаженной кривой.

11.24.2. Ключевые возможности

Переход к событиям по интервалу – для перехода к событиям на странице **Активность** необходимо выделить на графике интересующий участок времени. Появится кнопка **Перейти к событиям на выбранном интервале** ( ), которая открывает раздел событий, уже отфильтрованный по выбранному агенту и

диапазону дат. Это связывает количественную аномалию (всплеск нагрузки, например) с конкретными событиями безопасности.

Перемещение карточек – карточки можно менять местами перетаскиванием, выстраивая удобную для анализа компоновку.

Сравнительный анализ – поскольку на экран можно добавить произвольное число графиков, раздел удобен для сопоставления одной метрики на разных хостах или разных метрик одного хоста.

11.24.3. Типичные сценарии

Расследование жалоб на медленную работу хоста — анализ загрузки ЦП, памяти и диска.

Контроль потребления ресурсов EDR — мониторинг потребления ресурсов службой и драйвером агента.

Выявление подозрительной сетевой активности — динамика соединений и сетевого трафика с последующим переходом к событиям.

11.25 Просмотр файла в разделе Хранилище

Любой исполняемый файл может быть загружен в файловое хранилище со страниц **Активность**, **Инцидент** и **Процесс** с помощью кнопки (**Загрузить файл в файловое хранилище**). После скачивания в хранилище файл будет доступен аналитику для просмотра и дальнейшего скачивания на компьютер, с которого осуществляется доступ к модулю администрирования (кнопка во вкладке **Файлы с агентов** или **Загрузка файлов**). Аналитик также может загружать файлы в хранилище со своего компьютера, перейдя на вкладку **Загрузка файлов** (кнопка **Загрузить файл**) или использовать ссылку на скачивание ( ) для того, чтобы вставить ее в команду агента **put** для размещения файла на компьютере с агентом (то же самое можно сделать на вкладке **Файлы с агентов**).

Кроме того, на вкладке **Загрузка файлов** аналитик может скачать постоянную ссылку для загрузки файла на компьютер с агентом с помощью кнопки **Скопировать ссылку на файл**), а также отключить или включить скачивание файла агентами с помощью кнопок / .

Файл на странице **Хранилище** можно проанализировать с помощью программы просмотра файлов.

Для просмотра загруженного файла необходимо кликнуть по соответствующей ему кнопке **Просмотреть файл** ( ), после чего откроется окно **Просмотр файла** (рис. 103).



Рисунок 103 – Окно «Просмотр файла»

Файл можно просмотреть в различных кодировках или в бинарном представлении. Если размер файла превысит 1 мегабайт, то файл будет загружен только частично. В таких случаях для загрузки оставшейся части файла необходимо нажать кнопку (**Загрузить ещё 1 Мб содержимого файла**). После просмотра файла его можно удалить, воспользовавшись кнопкой **Удалить файл** ( ).

Загруженные файлы могут быть проверены с помощью TI-платформы, для этого на вкладке **Файлы с агентов** необходимо нажать кнопку **Загрузить файл на сервис RT Protect TI** ( ) и загрузить файл на TI-платформу.

11.25.1. Создание задач по загрузке архивов

Чтобы создать задачу по загрузке архива, аналитику необходимо выбрать один или несколько файлов на вкладке **Файлы с агентов** и нажать кнопку **Создать задачу загрузки архива**. После этого в открывшемся окне **Подтверждение действия** ввести имя архива и нажать кнопку **Подтвердить**. Далее наш архив появится во вкладке **Задачи по загрузке архивов**, где его можно скачать на компьютер, с которого осуществлен доступ к серверу управления, с помощью кнопки **Скачать архив** ( ).

При необходимости архив может быть удален с помощью кнопок **Удалить архив** ( ) и **Удалить выбранные** (после установки флажка для одного или нескольких архивов).

Также задача по загрузке архива может быть отменена, для этого используется кнопка **Отменить выбранные** (после выбора одного или нескольких архивов).

11.26 Проактивный поиск угроз

11.26.1. Проведение расследований на странице «Активность»

Расследование – это определение и изучение аналитиком событий, связанных с возможной или уже существующей нелегитимной активностью внутри защищаемого периметра.

Современные APT-атаки могут проводиться таким образом, что явных инцидентов, указывающих на вредоносную активность на конечных точках, возникать не будет.

Зачастую такие атаки скрываются под легитимными процессами, используют легитимное ПО, которое является нативным для ОС Windows, например, PowerShell или rundll32.

Активный поиск угроз позволяет на ранней стадии выявлять новые и сложные угрозы и рассматривается как дополнение к имеющейся защите информационных систем организации, а не как ее замена. От традиционных методов защиты threat hunting отличает именно проактивность. Активный поиск угроз (охота на угрозы, threat hunting) – это процесс проактивного (упреждающего) обнаружения вредоносной деятельности в компьютерных сетях. Поскольку проникновение в систему может произойти в любой момент, охота на угрозы – это непрерывный процесс, который можно разбить на 3 шага:

1) Формулирование гипотезы. На этом этапе специалисты строят предположения о том, где следует искать угрозы. Источником информации для выдвижения гипотезы могут служить как внутренние данные компании (сведения о состоянии IT-инфраструктуры, результаты тестов на проникновение и так далее), так и внешние (тактики и техники Mitre Att&ck, отчеты разведки киберугроз, новости безопасности и так далее). Например, если в свежем отчете приводится анализ ранее неизвестного вредоносного ПО, можно предположить, что этот зловред мог проникнуть в инфраструктуру компании;

2) Проверка гипотезы посредством поиска угроз. После формулирования гипотезы ее тестируют. Например, анализируют данные с конечных точек на предмет наличия индикаторов компрометации, связанных с новым вредоносным ПО.

3) Улучшение автоматического анализа. Для этого могут использоваться индикаторы компрометации или индикаторы атак. Успешная охота должна завершаться обогащением возможностей автоматического обнаружения. Если в процессе охоты обнаруживается индикатор или паттерн, который может циркулировать в системе, необходимо автоматизировать его обнаружение, чтобы можно было сосредоточиться на поиске новых угроз.



Совет

Чтобы предотвратить целенаправленные атаки, необходимо искать аномалии в работе защищаемой инфраструктуры. Для этого аналитик должен определить, какая активность будет нормой для защищаемых конечных точек или инфраструктуры в целом. Определив нормальное состояние, аналитик сможет начать искать отклонения от нормы, чтобы выяснить, являются ли эти отклонения следствием вредоносной активности или нет.

Если обнаруженная аномальная активность не укажет на APT-атаку, результаты поиска все равно могут быть полезны. Положительным эффектом выявления аномалий может стать определение слабых мест защищаемой инфраструктуры или возможностей для улучшения ее защиты. Чем больше аналитик будет знать о защищаемой системе, тем лучше он сможет ее оборонять от возможных атак и проникновений злоумышленников. Страница **Активность** позволяет аналитику проводить проактивные расследования и выявлять отклонения от нормы в событиях, поступающих от конечных точек.

Кроме большого количества фильтров, позволяющих сортировать телеметрические события по множеству различных параметров, страница **Активность** предоставляет возможность аналитику использовать строку DSL-запросов на языке Elasticsearch Query DSL (рис. 104).

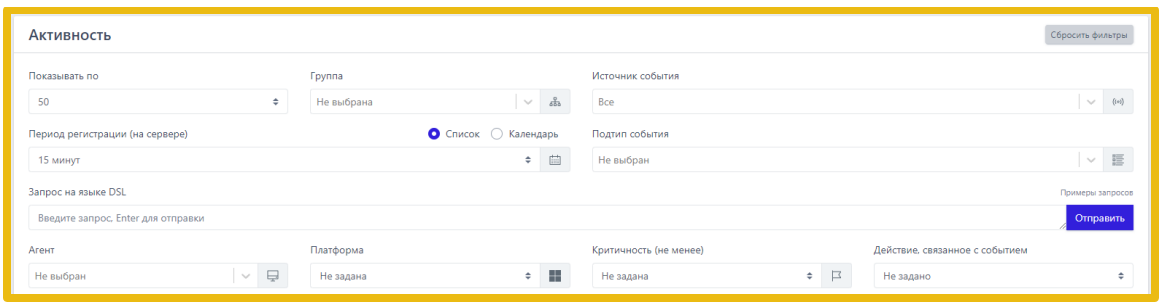


Рисунок 104 – Фильтры на странице «Активность»

Для написания запросов необходимо знать и структуру событий, отправляемых агентами на сервер, и сам язык запросов. Полное описание полей всех событий расположено в разделе 9. Описание языка запросов представлено на официальном сайте elasticsearch (https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html). Далее приведено собственное описание языка запросов с примерами.

Примечание

В общем виде запрос представляет собой поиск событий некоторого заданного значения в БД по определенному временному срезу. Поддерживается как поиск значения вне зависимости от его семантики (принадлежности определенному полю), так и поиск значений среди заданных полей.

Пример первого варианта представлен на рисунке 105.

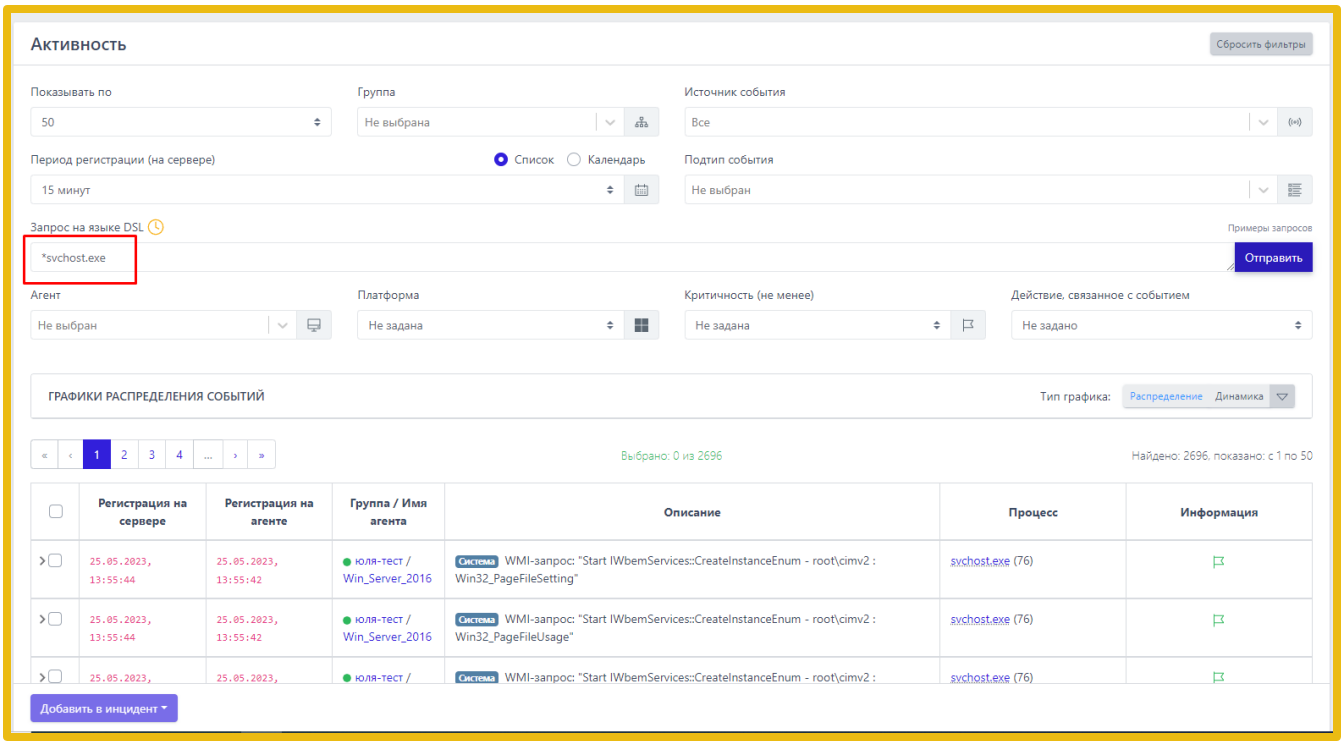


Рисунок 105 – Запрос вне семантики

Результатом строки запроса ***svchost.exe** являются все события, в которых есть поля, значения которых оканчиваются на подстроку **svchost.exe**. Это может быть имя исполняемого файла при запуске нового процесса, так и имя файла в событии создания нового файла и др. При этом в работе с большими временными периодами необходимо учитывать, что такой запрос не будет оптимальным с точки зрения производительности системы.

Примечание

Если DSL-запрос не является оптимальным с точки зрения нагрузки на поисковую систему базы данных, то сверху строки с запросом появляется значок . Если навести на него курсор мыши, то пользователю будет показана информация о том, что запрос желательно изменить с примером того, как это можно сделать.

Если же требуются именно события процессов с исполняемым файлом **svchost.exe**, в запросе необходимо указать имя поля, для которого будет выполнен поиск. Пример такого запроса представлен на рисунке 106.

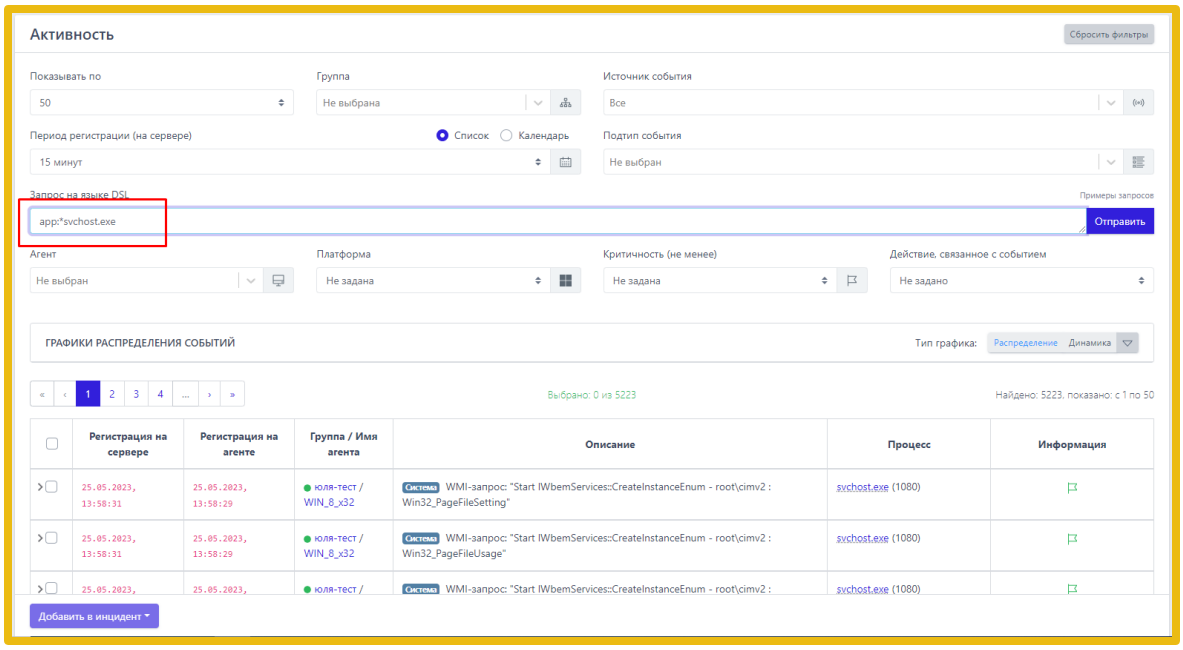


Рисунок 106 – Поиск по заданному полю

Совет

Svchost.exe и другие хост-процессы, например, rundll32.exe скрывают действующий процесс в событии, для того чтобы понять реального актора, необходимо обращать внимание на область **Инициатор** в карточке события на странице **Активность**, а конкретнее, нам нужна строка **Полное имя исполняемого модуля-инициатора операции** (who).

Формат запроса с учетом семантики значения имеет вид: **<имя_поля>:<искомое_значение>**. В случае, если искомое значение представляет собой некоторую подстроку, необходимо использовать регулярные выражения.

На рисунке, приведенном выше, результатом запроса будут все события, в которых есть поле **app**, и значение этого поля оканчивается на **svchost.exe** (при этом возможно, что значение поля будет в точности равно искомому выражению). Поиск значения ведется с учётом регистра символов. Для того, чтобы регистр не учитывался, к имени поля необходимо указать спецификатор **lower**.

Пример запроса без учета регистра приведен на рисунке 107.

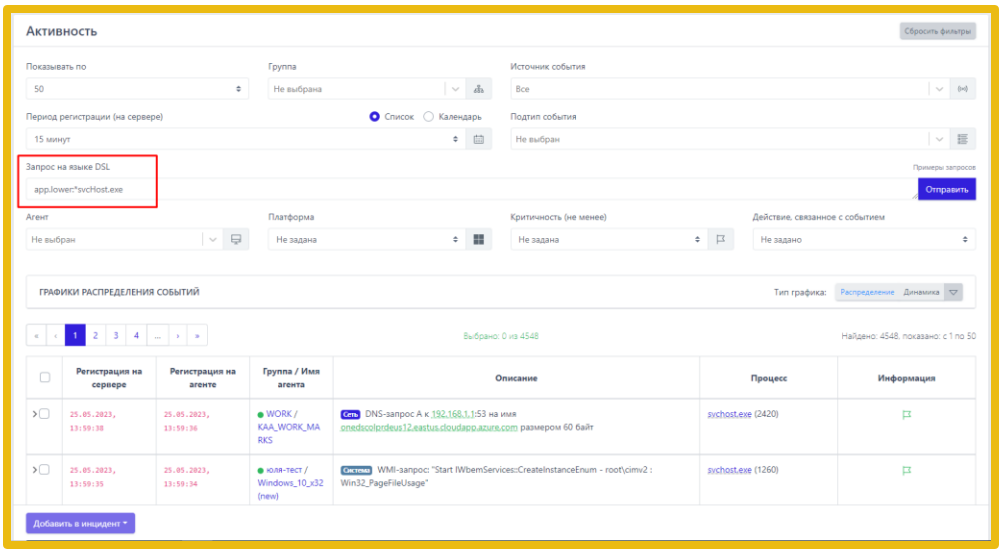


Рисунок 107 – Запрос без учета регистра

Имя поля всегда указывается с учетом регистра. В Программе принято соглашение, что названия полей содержат только строчные буквы, поэтому имена полей в запросе должны состоять только из строчных букв.

Язык Elasticsearch Query DSL позволяет осуществлять сложные запросы, состоящие из объединения простых запросов, рассмотренных ранее, с помощью логических операторов: И, ИЛИ, НЕ. Логические операторы задаются с помощью ключевых слов: AND, OR, NOT. Ключевые слова записываются с учетом регистра символов, т.е. And, and не являются логическими операторами. Для группировки результатов выполнения подзапросов используются круглые скобки. Пример сложного запроса представлен на рисунке 108.

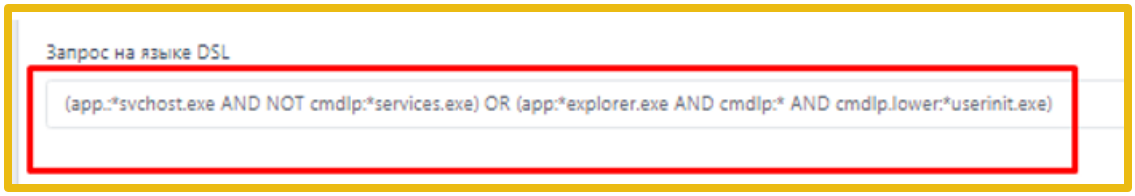


Рисунок 108 – Сложный DSL-запрос

С помощью приведенного запроса выполняется поиск событий запуска подозрительных процессов **svchost.exe** и **explorer.exe**. Для этого проверяется командная строка родительских процессов.

В основном экземпляры штатных процессов **svchost** запускаются процессом **services.exe**, а **explorer.exe** – процессом **userinit.exe**. Дополнительное условие для проверки командной строки родительского процесса «**cmdlp:***» необходимо для случаев установки агента «на горячую». Агент устанавливается на работающую систему и сразу начинает отправлять события. В этой ситуации агент для консистентности представления информации формирует синтетические события запуска процессов. Но получить информацию о родительском процессе для синтетического события запуска не всегда возможно, в частности, для **explorer.exe** это невозможно, поскольку его родительский процесс **userinit.exe** уже завершен. В результате выполнения запроса выявлен запуск **svchost.exe** антивирусом Microsoft Defender.

Для удобства помимо фильтрации событий на основе запросов с помощью языка Elasticsearch Query DSL на форме **Активность** представлены поля для фильтрации.

Фильтры в представлении страницы **Активность** по умолчанию позволяют сортировать события по следующим критериям:

1) Количество отображаемых событий на странице;

2) Группа (на странице отобразятся события, пришедшие от агентов выбранной группы);

3) Источник события (на странице отобразятся события, соответствующие выбранному источнику: **Сеть**, **Файлы**, **Реестр**, **Журналы**, **Процессы**, **Сессии**, **Защита файлов**, **Система**, **Вызовы**, **Контроль USB**, **Статистика**);

4) Период регистрации событий на сервере;

5) Подтип события (для каждого источника события существуют свои подтипы события, см. таблицу 61);

6) Агент;

7) Платформа (ОС Windows или Linux);

8) Критичность (на странице отобразятся события с критичностью не ниже выбранной);

9) Действие, связанное с событием.

Таблица 61 – Типы и подтипы событий

Тип события	Подтипы события
Сеть (**t:0** в DSL)	Исходящее подключение (**st:0** в DSL)
	Входящее подключение (**st:1**)
	Завершение сетевого подключения (**st:16**)
	Отправка (**st:2**)
	Прием (**st:3**)
	DNS-запрос (**st:5**)
	DNS-ответ (**st:11**)
	Входящий DNS-запрос (**st:13**)
	Исходящий DNS-ответ (**st:14**)
	SSL HELLO (**st:6**)
	Открытие локального порта на прием (LISTEN) (**st:10**)
	ICMP-сообщение (**st:15**)
	Обнаружение: срабатывание сетевого исключения (**st:12**) (устаревшее, оставлено для совместимости с ранними версиями агента)
	Обнаружение: срабатывание индикатора компрометации (**st:8**)
	Другие обнаружения (**st:7**)
Файлы (**t:1**)	Создание нового файла (**st:0**)
	Переименование файла (**st:1**)
	Удаление файла (**st:2**)
	Изменение атрибута или времени создания файла (**st:3**)
	Запись файла (**st:7**)
	Чтение файла (**st:8**)
	Прямой доступ к диску (тому) на чтение (**st:12**)

Тип события	Подтипы события
	Прямой доступ к диску (тому) на запись (**st:13**)
	Создание именованного канала (**st:14**)
	Подключение к именованному каналу (**st:15**)
	Создание альтернативного потока для файла (**st:22**)
	Доступ к файлу (**st:16**)
	Обнаружение: срабатывание индикатора компрометации для файла (**st:17**)
	Обнаружение: срабатывание исключения для файла (**st:18**) (устаревшее, оставлено для совместимости с ранними версиями агента)
	Обнаружение: файл классифицирован как вредоносный (ML на агенте) (**st:19**)
	Обнаружение: файл классифицирован как вредоносный (YARA-правила) (**st:20**)
	Создание файла с потенциально активным содержимым (**st:23**)
	Модификация файла с потенциально активным содержимым (**st:24**)
	Изменение параметров безопасности файла (**st:26**)
	Другие обнаружения (**st:4**)
Реестр (**t:2**)	Создание нового ключа (**st:0**)
	Удаление ключа (**st:1**)
	Запись значения ключа (**st:2**)
	Удаление значения ключа (**st:3**)
	Переименование ключа (**st:4**)
	Восстановление ключа из файла (**st:5**)
	Замена данных ключа из файла (**st:6**)
	Другие обнаружения (**st:7**)
Журналы (**t:3**)	Событие журнала (**st:0**)
	Успешный вход в систему (**e_id:4624** в DSL)
	Отказ входа в систему (**e_id:4625**)
	Выход из системы (**e_id:4634**)
	Пользователь инициировал выход из системы (**e_id:4647**)
	Попытка входа в систему с использованием явных учетных данных (**e_id:4648**)
	Создан пользователь (**e_id:4720**)
	Включен (enabled) аккаунт пользователя (**e_id:4722**)
	Попытка изменения пароля пользователя (**e_id:4723**)
	Попытка сброса пароля пользователя (**e_id:4724**)
	Отключен (disabled) аккаунт пользователя (**e_id:4725**)
	Удален пользователь (**e_id:4726**)
	Изменен аккаунт пользователя (**e_id:4738**)
	Заблокирован пользователь (**e_id:4740**)
	Разблокирован пользователь (**e_id:4767**)
	Пользователь отключил сеанс терминального сервера, не выполнив выход из системы (**e_id:4779**)

Тип события	Подтипы события
	Изменено имя пользователя (**e_id:4781**)
Процессы (**t:4**)	Старт процесса (**st:1**)
	Завершение процесса (**st:2**)
	Загрузка образа (**st:3**)
	Загрузка образа в сторонний процесс (**st:20**)
	Загрузка драйвера (**st:0**)
	Создание нити в стороннем процессе (**st:7**)
	Доступ к процессу (**st:6**)
	Доступ к нити процесса (**st:18**)
	Уведомление модуля Antimalware Scan Interface Windows (**st 22**)
	Обнаружение: подмена командной строки (**st:13**)
	Обнаружение: изменение системной защиты процесса (**st:16**)
	Другие обнаружения (**st:23**)
Сессии (t:6)	Создание пользовательской сессии (**st:1**)
	Завершение пользовательской сессии (**st:2**)
	Подключение к пользовательской сессии (**st:3**)
	Отключение от пользовательской сессии (**st:4**)
	Выполнен вход пользователя (**st:5**)
	Выполнен выход пользователя (**st:6**)
	Блокирование сессии пользователя (**st:7**)
	Разблокирование сессии пользователя (**st:8**)
	Изменен статус удаленного управления сессии пользователя (**st:9**)
Антишифр (**t:8**)	Заблокирован вредоносный процесс (**st:0**)
	Создана резервная копия файла (**st:1**)
Система (**t:5**)	WMI (**st:0**)
	Изменение системного времени (**st:2**)
	Завершение работы (**st:3**)
Вызовы (**t:7**)	Вызовы: RPC (remote procedure call) (**st:0**)
Контроль USB (**t:9**)	Устройство USB подключено (**st:0**)
	Устройство USB отключено (**st:1**)
	Зафиксирована запрещенная попытка чтения (**st:2**)
	Зафиксирована запрещенная попытка записи (**st:3**)
	Зафиксирована запрещенная попытка выполнения управляющего запроса (**st:4**)
	Зафиксирована запрещенная попытка запуска исполняемого файла (**st:5**)
	Статистика чтения/записи данных (**st:6**)
Статистика	Нет подтипов события

При выборе типа события **Статистика** в карточке события будут отображаться следующие сведения:

1) Уникальный идентификатор агента;
2) Загрузка процессора;
3) Загрузка памяти;
4) Количество процессов;
5) Количество нитей;
6) Количество открытых описателей;
7) Объем прочитанных с диска данных в секунду;
8) Объем записанных на диск данных в секунду;
9) Объем переданных данных по сети в секунду;
10) Объем принятых данных по сети в секунду;
11) Временная зона;
12) Разница во времени с сервером;
13) Признак нахождения в режиме network containment
14) Общее количество сетевых соединений;
15) Загрузка процессора службой агента;
16) Время последнего обновления аналитики по наборам;
17) Состояние функций защиты (0 – вкл., 1 – выкл.);
18) Причина завершения работы;
19) Парольная защита от удаления агента (1 – вкл., 0 – выкл.);
20) Загрузка процессора службой агента;
21) Использование памяти службой (Мбайт) агента;
22) Загрузка процессора драйвером агента;
23) Использование памяти драйвером (Мбайт) агента.

На странице **Активность** можно составлять запросы тремя способами:

– только с помощью языка запросов (все поля фильтрации сброшены);

– только с помощью полей фильтрации, с заполнением их соответствующими значениями (строка запроса при этом пустая);

– комбинированным – используются и поля фильтрации, и текст запроса.

Комбинированный способ удобен, когда наряду с несколькими односложными условиями (например, требуется поиск по конкретному единственному типу события и на конкретном агенте) события фильтруются на основе целого набора возможных значений некоторого поля.

Наиболее простым примером использования формы **Активность** является ретроспективный анализ на предмет выявления артефактов «свежих» угроз. Например, в одном из контуров агентской сети было проведено расследование некоторого инцидента, в результате которого были выявлены: хеши, IP-адреса, DNS-имена, имена исполняемых файлов, связанные с этим инцидентом. Далее обычно происходит поиск в других контурах, с целью определения факта компрометации других агентов. Пример такого запроса представлен на рисунке 109.

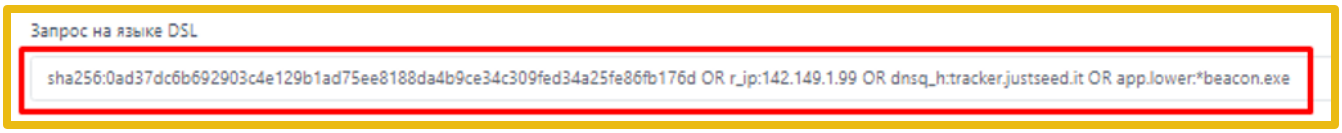


Рисунок 109 – Пример запроса для ретроспективного анализа угроз

В результате выполнения запроса было выявлено обращение по DNS-имени, связанному с вредоносной активностью.

Для полей событий с числовыми значениями возможно использование операторов сравнения значений (>, <, >=, <=).

Пример запроса для вывода сетевых событий, у которых размер сетевого пакета превышает 100 байт, представлен на рисунке 110.

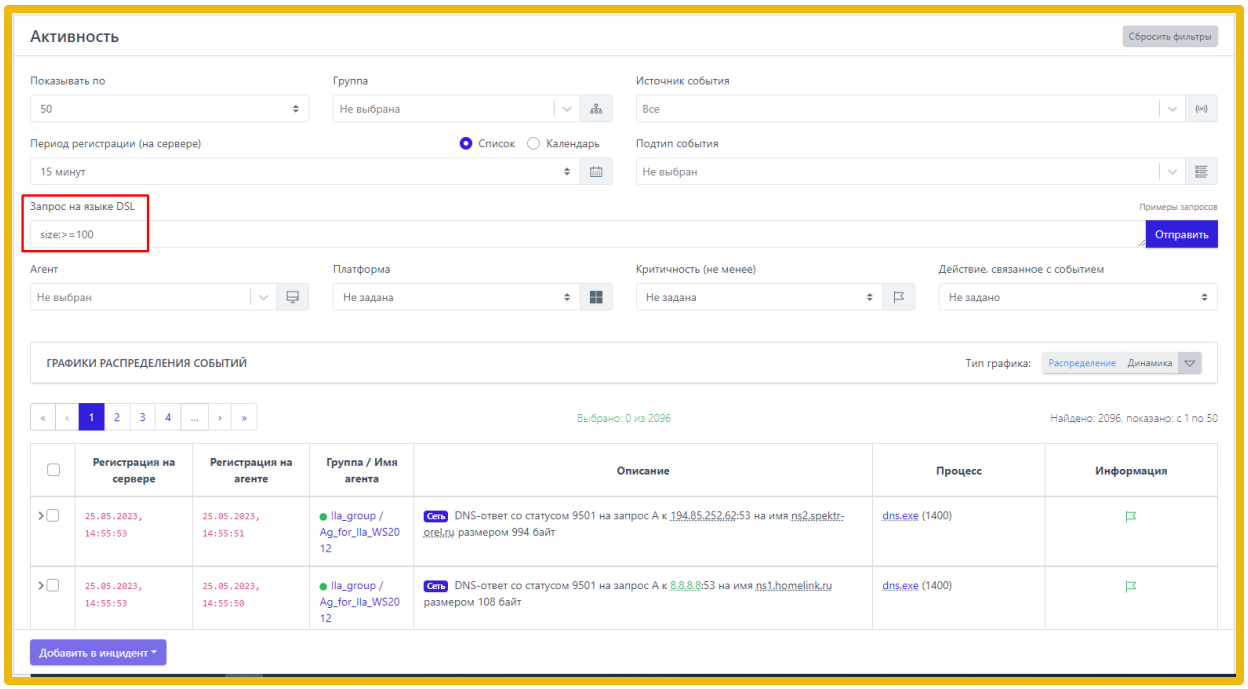


Рисунок 110 – Пример запроса с числовым значением

Также допускается фильтрация для диапазона значений. Пример фильтрации событий входящих сетевых подключений для диапазона сетевых портов [1080;1800] представлен на рисунке 111.

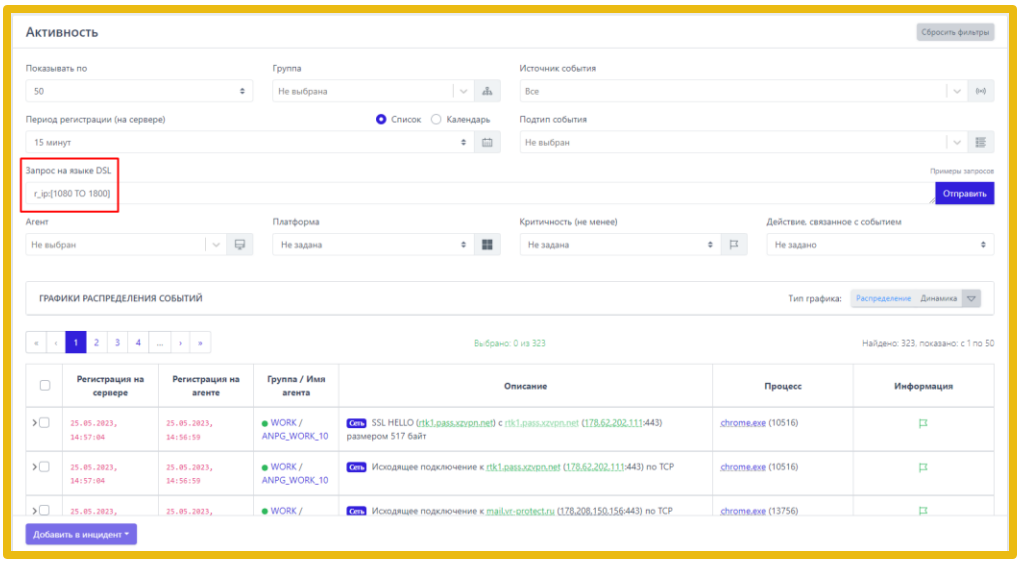


Рисунок 111 – Пример запроса с диапазоном значений

Следует отметить, что наиболее частой ошибкой при поиске, например, исполняемого модуля, является указание его названия без расширения. Иллюстрация такой ситуации представлена на рисунках 112 – 113.

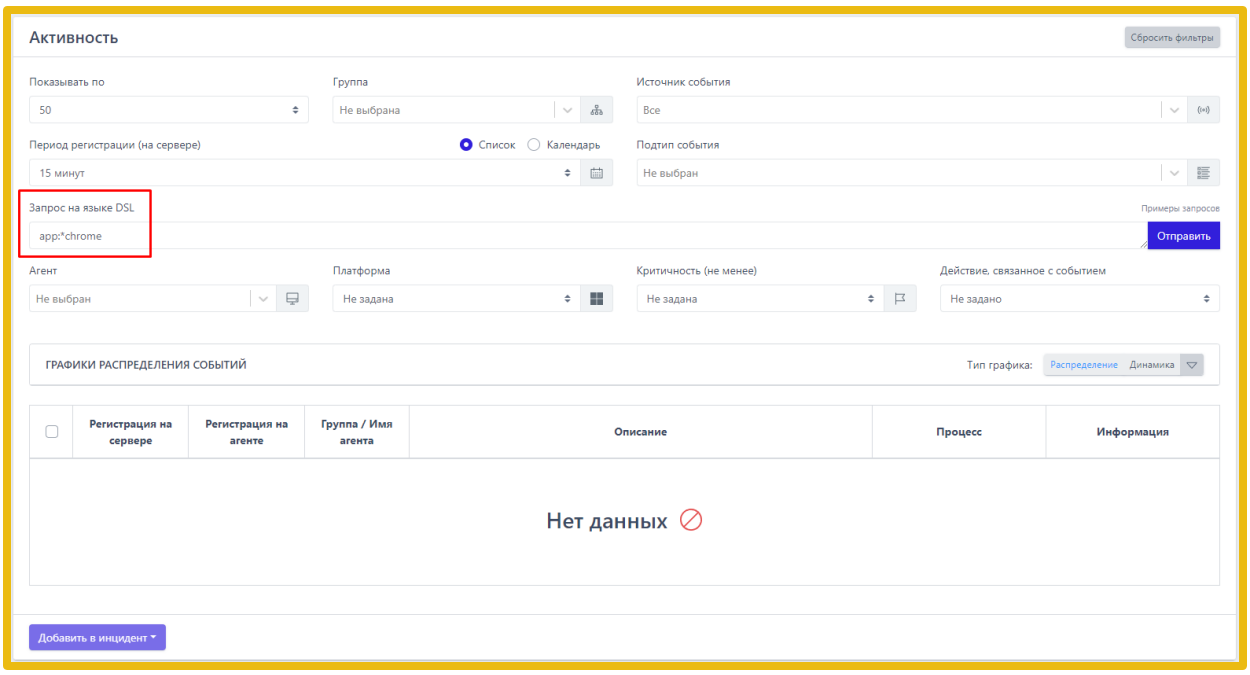


Рисунок 112 – Пример неправильного DSL-запроса

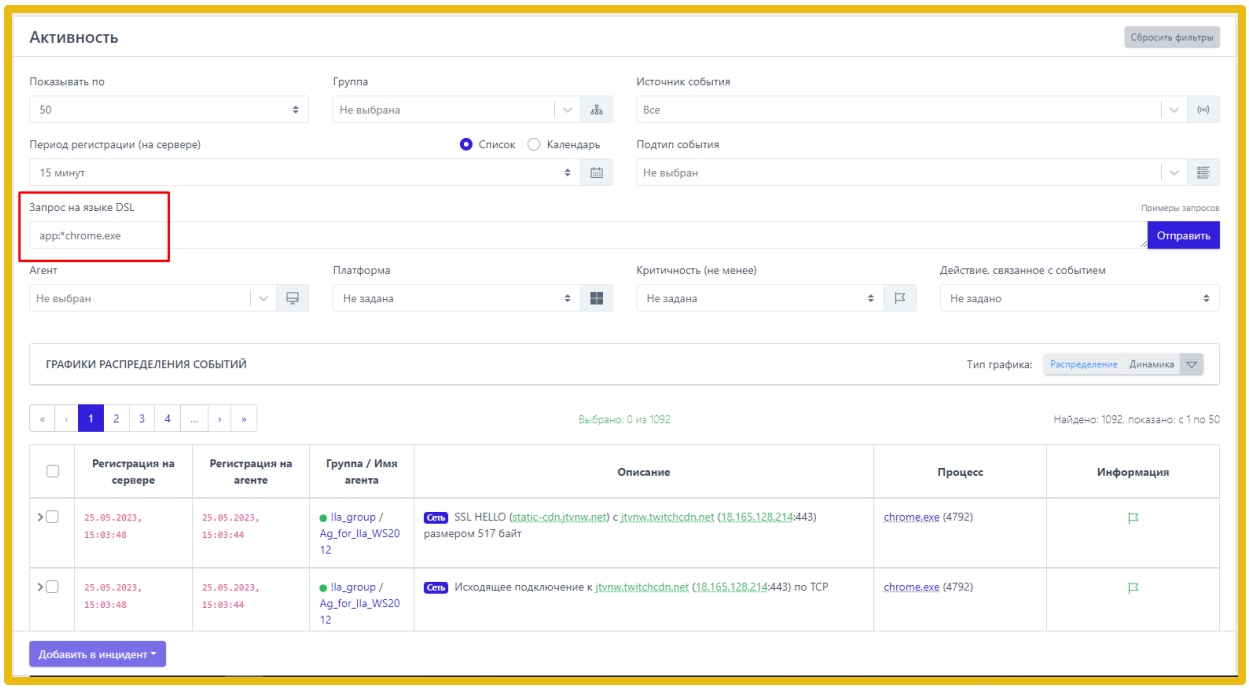


Рисунок 113 – Исправленный вариант DSL-запроса

С помощью первого запроса не найдено ни одного события, однако после добавления расширения сразу найдены требуемые события. Это связано с тем, что поиск осуществляется не по подстроке, а по строке

целиком. Но для гибкости допускается использовать регулярные выражения. Поиск без указания расширения должен выглядеть, как на рисунке 114.

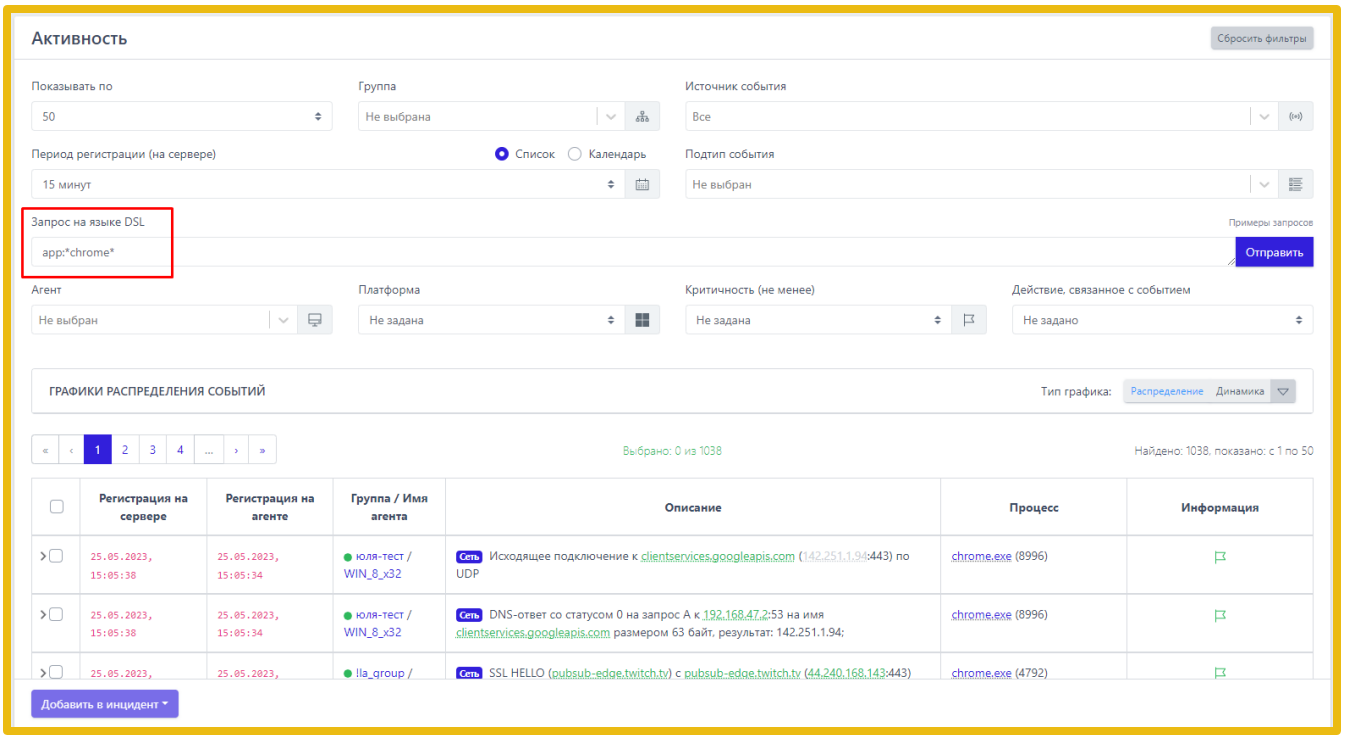


Рисунок 114 – Использование регулярных выражений для DSL-запроса

Удобно пользоваться оператором отрицания (NOT). Ниже представлен запрос, с помощью которого можно отфильтровать события создания новых .exe-файлов для всех процессов, кроме **svchost.exe** (рис. 115).

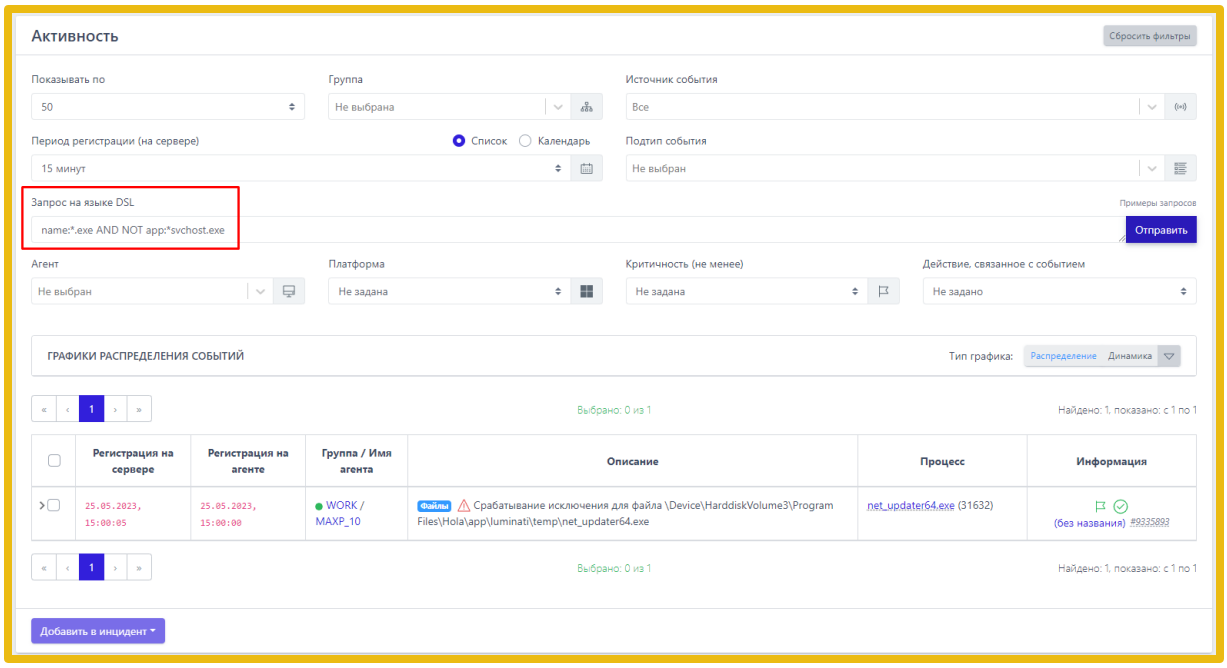


Рисунок 115 – Пример использования оператора NOT

Делая выводы, необходимо сказать, что для проведения ретроспективного анализа и проактивного поиска угроз и аномальной активности в защищаемой инфраструктуре следует использовать DSL-запросы и систему фильтров.

Для глубокого изучения всех обстоятельств и составных частей конкретного события на странице **Активность** предусмотрены карточки события. Они помогают аналитику разобрать информацию, полученную от конечной точки, защищаемой агентом. Эта информация касается всех значимых подсистем операционной системы Windows или Linux: сеть, файлы, процессы и т.д. Поля карточки меняются в зависимости от типа и подтипа события, при этом есть данные, которые содержатся во всех карточках, например, имя агента или время регистрации события на сервере.

Значительный интерес для аналитика в карточке события могут представлять битовые флаги, например, поведенческие признаки процесса или флаги исполняемого файла процесса.

Их можно применять при создании индикаторов атак. Подробный перечень битовых флагов содержится в подразделе 9.

В поле **Описание** таблицы на странице **Активность** и в карточке события для некоторых типов событий представлены артефакты, анализируемые TI-платформой:

1) IP-адреса;

2) Доменные имена;

3) Хеш-суммы.

В зависимости от состояния артефакт отображается разным цветом:

– безопасный – зеленый цвет (fe2.update.microsoft.com);

– об артефакте нет информации – светло-серый цвет (150.171.16.39);

– анализ артефакта выполняется в данный момент – синий цвет (s350iva.storage.yandex.net);

– вредоносный – красный цвет (35.155.156.153);

– подозрительный – оранжевый цвет (185.243.218.110).

В верхней части страницы отображается область с диаграммами (**Графики распределения событий**), на которых в графическом виде представлены типы и подтипы событий в соответствии с настроенными в данный момент фильтрами. Чтобы показать графики, необходимо нажать кнопку  . Если график **Распределение** показывает, как события распределяются в количественном соотношении по типам и подтипам, то **Динамика** показывает, как распределяются типы событий в динамике по дням, при этом доступен как линейный, так и столбчатый график. Для переключения между видами графиков используются кнопки 

(рис. 116).

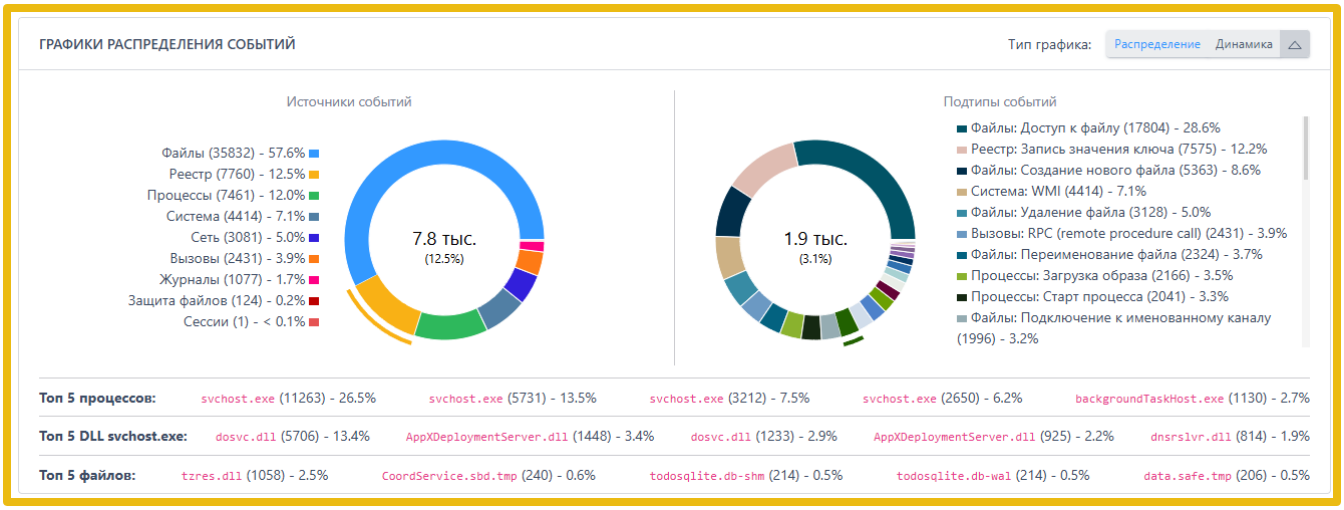


Рисунок 116 – Графики распределения событий

Ниже графиков аналитик может просмотреть топ 5 наиболее часто встречающихся процессов в защищаемой инфраструктуре, топ 5 динамически загружаемых библиотек в хост-процессе svchost.exe, а также топ 5 файлов.

11.26.2. Просмотр зашифрованной информации на страницах «Активность», «Инциденты», «Инцидент» и «Процесс»

При поиске информации на странице **Активность** и **Процесс** или расследовании инцидента аналитик может столкнуться с командными строками, содержащими зашифрованные по алгоритму Base64 команды. Для их расшифровки необходимо выполнить следующие действия:

1) Выделить зашифрованный текст;
2) После выделения текста появится кнопка **Декодировать Base64** ( );
3) Нажать кнопку (откроется окно **Декодирование Base64**) (рис. 117);
4) Если необходимо, то скопировать декодированное значение в буфер обмена.

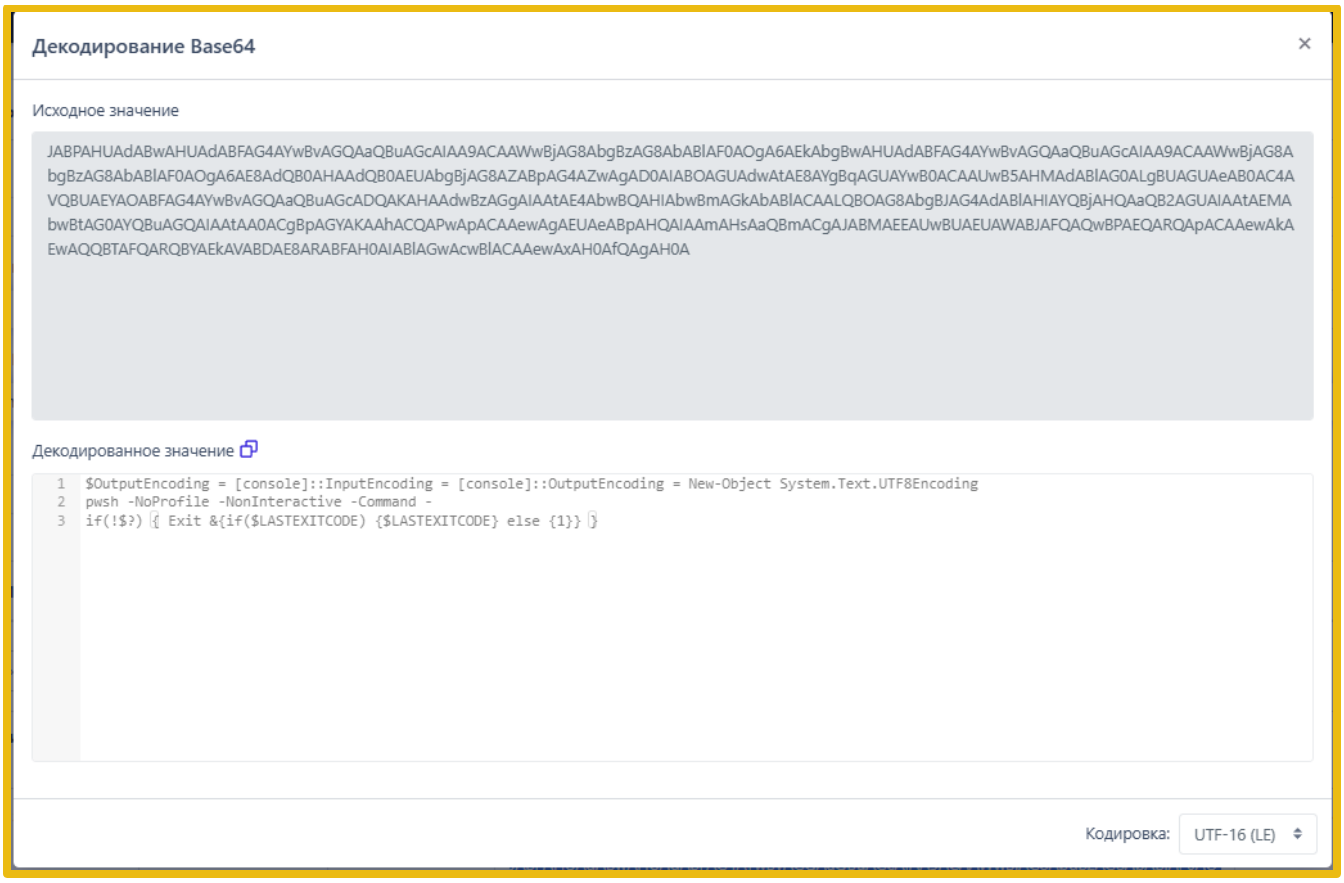


Рисунок 117 – Декодирование Base64

11.26.3. Концепция «Pyramid of Pain»

Все индикаторы, которые могут указывать на присутствие злоумышленников в защищаемой системе, можно ранжировать в соответствии с их значением для атакующего, то есть как много проблем обнаружение этих индикаторов доставит злоумышленнику. Такую концепцию называют «Pyramid of Pain» (рис. 118).

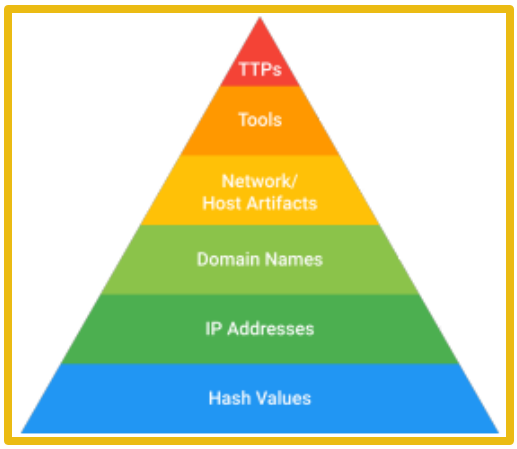


Рисунок 118 – Pyramid of Pain

Внизу пирамиды находятся индикаторы, обнаружение которых доставляет меньше всего проблем злоумышленникам, сверху самые значимые, обнаружение которых наносит максимальный урон их действиям.

Хеши. Большинство хеш-алгоритмов преобразуют входные данные таким образом, что на выходе получается уникальный для этих входных данных хеш. Это значит, что, если содержимое файла отличается хотя бы на один бит, значение его хеша будет также отлично. С одной стороны, индикаторы на основе хешей являются самыми точными, то есть на их основе можно с наибольшей уверенностью определить вредоносные файлы, а с другой стороны, любое изменение этих файлов, вроде перестановки бита или добавления нуля в конце, изменяет их хеш. Это делает их наименее значимыми индикаторами.

IP-адреса. Любой более или менее продвинутый злоумышленник может менять адреса с помощью небольших усилий, например, используя анонимный прокси-сервер Tor или похожий инструмент. Именно по этой причине IP-адреса находятся внизу пирамиды.

Имена доменов. Имена доменов менять немного сложнее, чем IP-адреса, так как для работы они должны быть зарегистрированы. Однако существует большое количество DNS-провайдеров со слабыми

стандартами регистрации, поэтому на практике сменить домен не очень тяжело, в среднем на это может уйти день или два.

Артефакты сети и хоста. Здесь начинается негативное влияние на злоумышленника при обнаружении. Если аналитик может обнаружить и отреагировать на индикаторы этого уровня, то злоумышленнику придется поработать над переконфигурацией или перекомпиляцией своих инструментов. Например, вы обнаруживаете, что утилита HTTP-разведки, которую использует злоумышленник, применяет отличительную строку User-Agent во время изучения вашего веб-контента. Если заблокировать любой запрос, использующий эту строку, то это вынудит злоумышленника потратить свои ресурсы на то, чтобы понять, как именно вы обнаружили их утилиту.

Инструменты. Обнаружение и реагирование на индикаторы этого уровня забирает у злоумышленника возможность использовать один или несколько его инструментов. Чаще всего это происходит, когда аналитик обнаруживает артефакты инструмента различными способами, например, с помощью YARA-сигнатур, если они способны обнаруживать вариации файла даже со средними изменениями.

Тактики, техники и процедуры. Обнаружение и реагирование на индикаторы этого уровня напрямую затрагивает поведение злоумышленника, а не его инструменты. Изменение поведения является самым сложным и затратным для злоумышленника, поэтому, чем больше тактик, техник и процедур можно обнаружить в ходе направленного поиска угроз, тем более защищенной будет система.

11.27 Обзор событий

Обзор событий – это инструмент, позволяющий исследовать события, поступающие от агентов, позволяет аналитику быстро оценить происходящее в защищаемой инфраструктуре. Обзор событий представляет собой сводную аналитическую надстройку над хранилищем телеметрии EDR, которая дает аналитику подборку топ-позиций по ключевым измерениям (правила, MITRE, файлы и т.д.) и возможность перейти к списку конкретных событий.

Типовые сценарии использования раздела:

– поиск отклонений в телеметрии за последний час, смену или сутки;

– первичная оценка ситуации в начале рабочего дня;

– анализ активности конкретного агента, пользователя или приложения;

– подготовка выборки событий для создания инцидента вручную;

– охота за угрозами (threat hunting) — выборка событий по правилам или техникам MITRE;

– проверка остутствия всплеска ложных срабатываний после развертывания новых политик.

Примечание

Раздел **Обзор событий** требователен к ресурсам системы: построение агрегатов выполняется на бэкенде по всему массиву событий, попадающих под заданный временной диапазон и фильтры. Перед открытием рекомендуется установить разумные ограничения по времени и по списку агентов — это снижает нагрузку на сервер и ускоряет отображение.

Страница **Обзор событий** позволяет пользователю просматривать события, распределенные по категориям:

1) Графики распределения событий и график динамики событий;
2) Агенты;
3) Правила;
4) Техники MITRE;
5) Исполняемые файлы;
6) Библиотеки (DLL/SO);
7) Командные строки;
8) Модули;
9) Хеши;
10) Пользователи;
11) Сессии (разделяются на локальные и дистанционные);
12) Файлы и точки автозапуска (файлы);
13) Реестр и точки автозапуска (реестр);
14) Сеть;
15) Настраиваемая агрегация.

Графики распределения событий и графики динамики событий – в блоке представлены графики, повторяющие графики со страницы **Активность**, на которых показана разбивка событий по источнику и

подтипам. Кроме того, блок информации с графиками содержит описание топ-5 процессов в представленной выборке, топ-5 DLL svchost.exe и топ-5 файлов в представленной выборке событий.

Агенты – В блоке представлена сводная информация о количестве событий, пришедших с агента за выбранный период времени. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **agent_id**. Раздел может быть полезен, например, чтобы быстро посмотреть, с каких агентов приходит значительное количество событий и при необходимости принять меры. В блоке также содержится информация о сетевых адресах агентов, доменах и именах компьютера, а также операционных системах, на которых агенты установлены.

Правила – в блоке представлены события, распределенные по правилам (внутренние правила Программы и индикаторы атак), цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным запросом по полю **rul**. Помогает увидеть, какие правила генерируют наибольший поток событий, что может быть полезно для поиска ложных срабатываний. Отображается до 500 правил с наибольшим количеством событий за выбранный период времени. Правила можно фильтровать по строке **Поиск**. Для поиска по вхождению строки необходимо использовать символ * (примеры – *domain – любые значения, оканчивающиеся на domain, 192.168.* – любые значения, начинающиеся с 192.168, *dotnet* - любые значения, в которых есть упоминание dotnet).

Техники MITRE – в блоке представлена сводная информация о событиях, распределенных по техникам MITRE. Применяется для обзора, по каким техникам сейчас больше всего активности. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **mitre**. Отображается 100 и более техник MITRE с наибольшим количеством событий за выбранный период времени.

Исполняемые файлы – в блоке представлена сводная информация по событиям, распределенным по исполняемым файлам. Блок показывает, с какими событиями и с каким количеством событий связан тот или иной исполняемый файл. Выявляет наиболее активные процессы в инфраструктуре. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **app**. Отображается до 500 исполняемых файлов с наибольшим количеством событий за выбранный период времени.

Взаимодействие процессов – в блоке представлена сводная информация по событиям, распределенным по процессам. Агрегация по парам «родитель — потомок». Используется для обнаружения нетипичных цепочек запуска. Цифра с количеством событий является ссылкой на страницу **Активность** с

предзаполненным DSL-запросом по полю **app** и **tpath**. Отображается до 500 процессов с наибольшим количеством событий за выбранный период времени.

Библиотеки (DLL/SO) – в блоке представлена сводная информация по событиям, распределенным по библиотекам DLL или SO. Блок показывает, сколько раз была загружена та или иная библиотека. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **path**. Отображается до 500 загружаемых библиотек с наибольшим количеством событий за выбранный период времени.

Командные строки – в блоке представлена сводная информация по событиям, распределенным по командным строкам. Блок показывает, какие события связаны с той или иной командной строкой. Позволяет увидеть повторяющиеся сомнительные команды. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **cmdl**. Отображается до 500 командных строк с наибольшим количеством событий за выбранный период времени. В случае, если командная строка содержит закодированный в Base64 текст, аналитик может расшифровать этот текст с помощью кнопки **Декодировать Base64** (), для этого необходимо выделить закодированный текст в командной строке, после чего кнопка появится.

Модули – в блоке представлена сводная информация по событиям, распределенным по модулям. Блок показывает, какие события связаны с тем или иным модулем-инициатором. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **who**. Отображается до 500 модулей с наибольшим количеством событий за выбранный период времени.

Хеши – в блоке представлена сводная информация по событиям, распределенным по хешам. Блок показывает, какие события связаны с тем или иным хешем. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **sha256**. Отображается до 500 хешей с наибольшим количеством событий за выбранный период времени.

Пользователи – в блоке представлена сводная информация по событиям, распределенным по пользователям. Блок показывает, какие события связаны с тем или иным пользователем. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полям **usr**, **sid** и **dom**. Отображается до 500 пользователей с наибольшим количеством событий за выбранный период времени. В блоке кроме имени аналитику доступна информация о домене и SID пользователя.

Сессии – в блоке представлена сводная информация по событиям, распределенным по сессиям. Блок показывает, какие события, происходящие с тем или иным пользователем, связаны с локальными и дистанционными сессиями. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полям **sess_usr** и **sess_dom** для локального пользователя и **sess_usr**, **sess_dom** и **sess_claddr** для дистанционного.

Файлы и точки автозапуска (файл) – в блоке представлена сводная информация по событиям, распределенным по файлам, то есть блок показывает агрегацию событий вокруг того или иного имени файла. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **name** для файлов и **arun** и **name** для точек автозапуска.

Реестр и точки автозапуска (реестр) – в блоке представлена сводная информация по событиям, распределенным по реестру, то есть блок показывает агрегацию событий вокруг того или иного ключа реестра. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полю **reg** для реестра и **asep** и **reg** для точек автозапуска.

Сеть – в блоке показано количество событий, связанных с исходящими подключениями, входящими подключениями, DNS-запросами и SSL HELLO собщениями, то есть агрегируются сетевые события по определенному хосту. Цифра с количеством событий является ссылкой на страницу **Активность** с предзаполненным DSL-запросом по полям **r_ip**, **host** и **proto** для входящего подключения, по полям **r_ip**, **host**, **proto** и **out** для исходящего подключения, по полям **dnsq_h** и **dnsq_t** для DNS и по полю **ssl_h** для SSL.

Настраиваемая агрегация – помимо предустановленных агрегаций на странице **Обзор событий** доступна агрегация по различным полям модели данных RT Protect EDR. Это очень полезная функция для анализа событий в защищаемой инфраструктуре, например, создав агрегацию по основному полю **agent_id** и дополнительному полю **r_ip_a** можно получить таблицу взаимодействовавших по сети агентов. С помощью настраиваемой агрегации аналитик может сам выбрать, по какому полю или комбинации полей строить топ событий. Кроме агрегаций по полям, представленным в списках (**Основное поле** и **Дополнительное поле**), доступна агрегация по другим полям модели данных (подробнее об этих полях можно узнать в разделе 9). Настраиваемая агрегация строится по любому полю события из предустановленного списка:

– Общие (t, rul, svrt и т.д.);

– Сетевые (proto, host, r_ip и т.д);

– Инициатор (who);

– Сведения о файле (ftype, sha-256, sha-1 и т.д.);

– Файлы (name, fnew, strm и т.д.);

– Процессы (integ, path, tpath и т.д.);

– Сессии (local, sess_usr, sess_dom и т.д);

– Реестр (reg, key, val_n, val_d);

– WMI (wmi, ns, wmi_local и т.д.);

– Журналы (e_prv, e_chn, e_id, e_msg);

– RPC (rpc_id, rpc_opname, c_path);

– USB (usb_mr, usb_pt, usb_sn и т.д.).

В EDR данные могут принимать следующие значения: строки, числа и булевские значения (т.е. true или false). В поле **Значение по умолчанию для основного поля** возможно указывать только эти значения для соответствующих полей агрегации, при этом строковые значения должны быть указаны в кавычках. Сам фильтр **Значение по умолчанию для основного поля** задает значение заполнителя для событий, у которых это поле отсутствует, чтобы они не выпадали из агрегации. Агрегация по полю отбрасывает события, у которых этого поля нет. Если аналитик строит топ по полю usr, то события, где usr вообще отсутствует (поле не заполнено) не попадут ни в одну строку таблицы и не будут посчитаны. Их как будто нет. Часто это и и представляет наибольший интерес – увидеть, сколько событий вообще без пользователя/без подписи/без командной строки. По умолчанию аналитик этого не увидит. Поле **Значение по умолчанию для основного поля** сообщает системе: «События, у которых основного поля нет, не выбрасывай — собери их в отдельный бакет и подпиши его определенным значением». Аналитик задаёт «искусственную метку», под которой соберутся все события без поля usr. Теперь они появляются в таблице отдельной строкой со своим счётчиком. Например, основное поле usr (пользователь), значение по умолчанию "". Результат на рисунке 119.

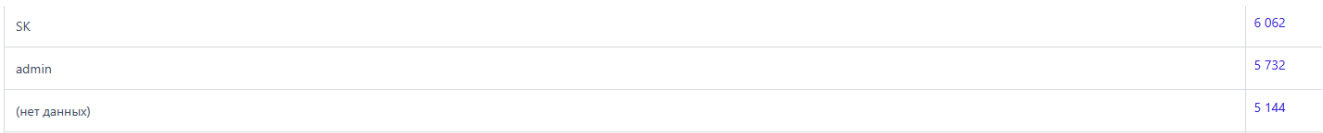


Рисунок 119 – Пример поиска значений по умолчанию для основного поля

Строка «(нет данных)» — это не реальный пользователь, а те события, у которых поле usr пустое. Без этого фильтра таблица бы не содержала это значение. Подсказка к полю (ⓘ) советует строковое значение писать в кавычках (`"system"`). Это потому, что значение интерпретируется в контексте типа данных поля (если основное поле строковое, значение по умолчанию тоже должно быть валидной строкой).



Примечание

Если поле у всех событий заполнено, то фильтр ни на что не влияет, строка со значением не появится в списке.

Информацию на странице **Обзор событий** можно фильтровать. На странице доступны следующие фильтры:

1) Максимальный размер агрегации (максимальное количество элементов агрегации);
2) Группа;
3) Источник события (тип события);
4) Период регистрации события на сервере или агенте;
5) Подтип события;
6) Запрос на языке DSL;
7) Агент;
8) Платформа;
9) Критичность (не менее установленной);
10) Действие, связанное с событием.

Необходимо помнить, что при выборе длительного периода регистрации (месяц и более), реализация запроса может занимать значительное количество времени.

11.28 Настройка профилей

В области **Профили** аналитик может настраивать параметры работы профилей агента.

Профили – это элементы Программы, которые позволяют задавать требуемый уровень защищенности для определенной инфраструктуры или отдельных частей защищаемой инфраструктуры,

настраивать модуль Антишифра агента, понижать или увеличивать нагрузку на те или иные подсистемы Программы, например, файловый монитор, изменять настройки безопасности сетевого монитора и т.д. Профиль опреляет, как агент защищает хост и какие события собирает. Такой подход дает возможность повысить эффективность использования программных инструментов для обнаружения аномальной активности на конечных точках с агентами, а также позволяет управлять нагрузкой на защищаемую инфраструктуру и Программу.

Все изменения, сделанные в профиле, могут быть отменены с помощью кнопки **Отменить внесенные изменения** (). При этом необходимо учитывать, что при переходе к другим страницам отменить внесенные изменения будет нельзя, а изменения на странице профиля будут сохранены.

При работе с профилями и передаче изменений в них агентам необходимо помнить, что для применения на агентах измененных конфигураций требуется время, поэтому следует убедиться для корректной работы с профилем, что конфигурация применена на агенте или агентах.

11.28.1. Профиль Антишифра

В современном цифровом мире киберугрозы становятся все более изощренными и опасными. Одной из самых серьезных проблем для организаций и частных пользователей являются ransomware-атаки, или атаки шифровальщиков. Эти вредоносные программы шифруют данные на устройствах жертв, требуя выкуп за их расшифровку. В таких условиях необходимо использовать специализированные решения, такие как модули противодействия шифровальщикам, которые способны предотвратить или минимизировать ущерб от ransomware-атак.

Модуль Антишифра прежде всего направлен на защиту от угроз нулевого дня, выполняя перехват и эвристический анализ файловой активности каждого процесса в системе в режиме реального времени.

Это позволяет выявлять характерные для шифровальщиков паттерны поведения, после чего блокировать их действия.

Важно

Режим «только детектирование» не распространяется на работу модуля Антишифр.

Модуль защиты от шифровальщиков (Антишифр) является важной частью RT Protect EDR: он останавливает работу шифровальщиков на компьютерах с установленным агентом Windows в режиме реального времени, позволяя защищать все каталоги системы от шифрования. Данное утверждение справедливо для третьих версий агентов и выше. Модуль Антишифра можно включать как с активным модулем ремедиации, так и без него (модуль ремедиации появляется в версиях программы 4.0, соответственно для третьих версий и ниже описания, касающиеся модуля ремедиации, неактуальны).



Важно

Антишифр работает только в агентах Windows.

Антишифр позволяет настраивать модуль ремедиации (модуль выполняет функции отката действий, выполненных вредоносной программой на определенный период времени, но не более, чем на 72 часа). Под настройками модуля понимается возможность включения тестового режима работы модуля, сохранения данных для восстановления реестра, возможность отправлять события создания резервной копии для операций резервирования файлов, возможность установить максимальное время хранения резервных копий, максимального размера резервируемых файлов и возможность установить процент доступного для заполнения резервными копиями дискового пространства.

Управление модулем Антишифра осуществляется с помощью профилей.

– экспортировать настройки профиля Антишифра в файл формата TXT;

– импортировать настройки из ранее экспортированного профиля Антишифра (поддерживаются файлы в формате TXT).

Информация о профилях Антишифра представлена в табличном виде. В таблице отображаются следующие поля:

– Название профиля;

– Привязано агентов;

– **Управление** (здесь находятся кнопки редактирования, удаления и сохранения профилей – ).

Чтобы создать новый профиль Антишифра, необходимо нажать кнопку Добавить профиль и в открывшемся окне ввести название нового профиля, после чего нажать кнопку Добавить (рис. 120).

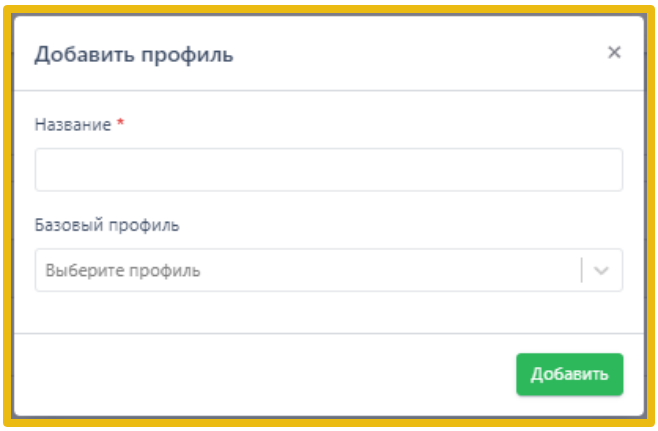


Рисунок 120 – Добавление профиля Антишифра

Если новый профиль Антишифра требуется создать на основе ранее сохраненного, то в поле выбора **Базовый профиль** следует назначить из выпадающего списка один из существующих профилей Антишифра и нажать кнопку Добавить.

С помощью кнопки **Редактировать** ( ) можно изменить название профиля (рис. 121).

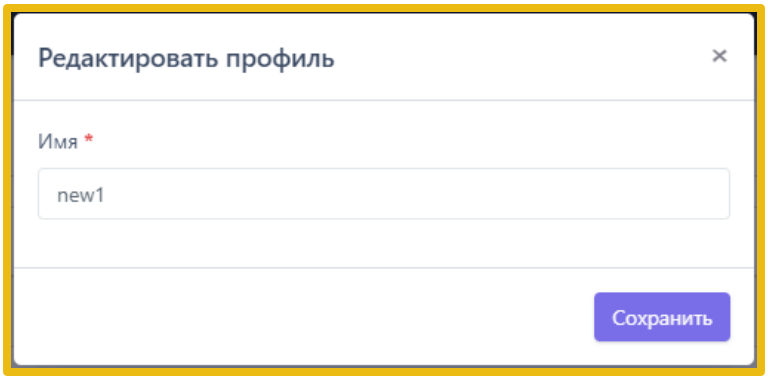


Рисунок 121 – Редактирование названия профиля Антишифра

Значок рядом с названием профиля или сверху страницы сообщает пользователю о том, что один или несколько профилей Антишифра не применены, для корректной работы их необходимо передать агентам с помощью кнопки **Передать все профили агентам** ( ).

Для удаления профиля или нескольких профилей Антишифра необходимо отметить их флажками и нажать кнопку **Удалить выбранные**.

Если требуется установить параметры защиты данных, отличающиеся от параметров существующих профилей Антишифра, то следует нажать название профиля, после чего откроется страница **Профиль Антишифра**.

Тестовый режим ремедиации – позволяет переключаться между тестовым и основным режимом работы. Тестовый режим отличается от основного режима тем, что реальная резервная копия файла не создаётся, при этом все остальные механизмы, такие как протоколирование изменений, связанные с именами файлов и реестра, отправка событий о занятости внутреннего хранилища, а также отправка событий об успешном резервировании файла осуществляется, хотя резервирования как такового в этом случае не происходит. Нужно это для того, чтобы оценить, какие файлы и в каком количестве будут резервироваться, какими процессами они вызываются. На основе этой аналитики можно для определённых доверенных процессов отключить резервирование. Это похоже на работу режима **Только детектирование** в **Профиле безопасности агента**. Основные различия между тестовым и штатным режимом работы модуля ремедиации приведены в таблице 62.

Таблица 62 – Различия между тестовым и штатным режимом ремедиации

Опция	Штатный режим	Тестовый режим
Реальные копии файлов/реестра	Создаются	Не создаются
Резервирование имен/каталогов	Да	Да (модуль считает, сколько файлов и какого суммарного объема он бы сохранил, но данные на диск не пишет))
Фильтрация по размеру файла	Да	Да
Отправка событий	Да	Да
Завершение процессов-шифровальщиков	Да	Нет
Расход дискового пространства	Да	Минимальный
Назначение	Защита	Оценка нагрузки и настройка политик

Флаг **Защита при нехватке свободного места** запрещает любые изменения файлов, если на диске недостаточно места для их резервного копирования. Это не дает шифровальщикам уничтожить оригиналы данных, когда создать резервную копию невозможно.

Существует тип атаки, когда вредонос сначала выделяет всё свободное место на диске, чтобы установленная система резервирования не могла создать резервную копию, после чего начинает шифровать файлы «поверх» оригиналов. Если опция включена, модуль ремедиации заблокирует любую попытку изменения файла, если на диске нет места для его резервной копии. Данные останутся в безопасности.

Флаг **Резервирование альтернативных потоков данных (ADS)** включает резервирование дополнительных метаданных и потоков NTFS (Alternate Data Streams). Если отключено, резервируется только основное содержимое файла. В файловых системах вроде NTFS у одного файла может быть несколько независимых наборов данных. Обычный пользователь видит через Проводник только основной поток. Альтернативные потоки скрыты и явно не отображаются, но в них тоже хранятся данные, которые необходимы приложениям для нормальной работы. Эта опция заставляет систему резервировать все потоки, которые есть у файла.

Флаг **Резервирование прав доступа файлов** определяет необходимость сохранения оригинальных прав доступа к файлам. Опция отвечает за сохранение дескрипторов безопасности (то есть прав доступа) при попытке их поменять. Злоумышленники часто удаляют дескриптор безопасности у файлов и операционная система сама блокирует пользователю доступ к его же собственным файлам. При включенной опции модуль ремедиации сохраняет оригинальную копию прав доступа и при необходимости восстанавливает их.

Флаг **Сохранять данные для восстановления реестра Windows** – опция управляет механизмом создания резервных копий ключей реестра Windows перед внесением в него изменений. Это позволяет откатить нежелательные или вредоносные изменения, возвращая параметры системы в рабочее состояние в случае их повреждения.

Флаг **Отправлять события "Создана резервная копия" для операции резервирования файлов** определяет необходимость отправки на сервер события **Антишифр: Создана резервная копия**. Если флаг снят, то такие события отправляться не будут. На странице **Активность** всегда можно будет увидеть, какие файлы можно восстановить при ремедиации и в рамках каких процессов они создавались. Важный нюанс: для изменений в реестре такие события на сервер не отправляются, они фиксируются только для файлов.

Поле **Максимальное время хранения резервных копий (в часах)** Определяет максимальное время хранения резервных копий файлов и данных реестра Windows. По истечении этого срока устаревшие данные удаляются. Важно: если выделенное под хранилище место закончится раньше, старые копии будут удалены

принудительно для освобождения пространства. Допустимое значение: от 1 до 72 часов. По истечении этого времени, резервные копии файлов и реестра, которые были созданы раньше, будут удалены. В целом рекомендованное значение максимального времени хранения резервных копий желательно устанавливать в диапазоне от 12 до 16 часов. Необходимо также помнить, что чем более длительный срок для востановления копий мы указываем, тем меньше вероятность успешного восстановления копий, которые были зарезервированы в первую очередь. Вероятность полного восстановления копий, которые были зарезервированы 70 часов назад, ниже, чем вероятность полного восстановления копий, которые были зарезервированы 5 часов назад.

Поле **Максимальный размер резервируемого файла (МБ)** определяет максимальный размер резервируемого файла в мегабайтах. Если размер резервируемого файла будет превышать размер указанного значения, то такой файл резервироваться не будет. Значение является 32 битным, беззнаковым числом. При нулевом значении ограничения на размер не осуществляются.

Поле **Квота доступного дискового пространства (%)** определяет размер дискового пространства, которое предоставляется модулю ремедиации для хранения резервных копий и служебной информации. Это значение задаётся в процентном соотношении от размера раздела, на котором включено резервирование. Важно помнить, что значение будет рассчитываться и применяться для каждого раздела отдельно. Значение задаётся в диапазоне от 1 до 30. Квотирование и ремедиация недоступны для FAT и FAT32, а также в разделах USB-накопителей.

Как работает ремедиация?

Ремедиация – это процесс восстановления затронутых шифровальщиком файлов и ключей/значений реестра в программе RT Protect EDR.

Модуль ремедиации работает по принципу «сначала зарезервируй, а потом дай изменить». Он прозрачно создаёт резервные копии файлов и ключей реестра Windows перед тем, как их кто-то изменит или удалит. Если потом окажется, что изменения сделал шифровальщик/вредонос, оператор EDR может вернуть систему к исходному состоянию — восстановить зашифрованные/удалённые файлы и повреждённые ветки реестра.

Главное правило работы модуля ремедиации – если процесс из одного узла пытается изменить или удалить файл, который создал другой узел, то модуль ремедиации сразу делает резервную копию этого файла. Копия изменяемого файла для этого узла будет сделана единожды, сколько бы раз узел в этот файл не писал.

Все журналы и резервные копии хранятся локально, на том томе, где происходили изменения. Данные не уходят в облако или по сети. Например, при удалении файла с диска D, резервная копия сохранится на ээтом же диске.При этом само хранилище резервных копий защищено драйвером агента. Его нельзя прочитать, изменить или удалить. Шифровальщик не сможет получить доступ к резервным копиям в ходе атаки, и если он попытается это сделать, то драйвер заблокирует операцию.

Для пользователя ремедиация производится в две фазы:

1) Автоматическая защита/резервирование в фоне;

2) Ручное восстановление по требованию при расследовании инцидента.

После того как администратор включил модуль и подсистему Ремедиации в профиле Антишифра и передал его агентам, на конечной точке начинает работать фоновая защита:

– при любой попытке изменить/удалить защищаемый файл агент сначала передает его оригинал в локальное хранилище резервных копий и только затем разрешает операцию, то же самое происходит для ключей реестра перед их изменением;

– каждое такое резервирование может порождать в EDR событие «Антишифр: Создана резервная копия файла», аналитик может увидеть эти события на странице **Активность** и понять, что объект защищён и его можно восстановить.

– резервные копии хранятся ограниченное время и в пределах квоты диска.

Когда инцидент обнаружен, например, видны массовые модификации файлов или сработало правило по шифровальщику, аналитик инициирует восстановление.

Чтобы восстановить файлы и ключи реестра, можно воспользоваться тремя инструментами:

1) Сценарий реагирования на странице **Процесс**;

2) Нативная команда **remed** в онлайн-терминале;

3) Запуск задачи в Планировщике задач.

Во всех случаях прежде всего необходимо определить любой процесс из вредоносной группы для которой планируется сделать ремедиацию. Необходимо помнить, что изменения всегда отменяются для всех

процессов группы целиком . Проще всего найти процесс из вредоносной группы в событиях **Инцидента**. Здесь можно сразу перейти на страницу **Процесс**, кликнув по имени процесса из вредоносной группы, и воспользоваться первым в списке инструментом – дефолтным сценарием реагирования, который активируется кнопкой **Реагирование.** Но сначала нужно выбрать соответствующую вредоносную группу процессов (на странице **Процесс** идентификатор группы обозначается иконкой ). После нажатия кнопки Реагирование необходимо выбрать операцию ремедиации. Откроется окно, в котором автоматически будет установлен **hid** логической группы, которая объединяет несколько совместно работающих процессов и время, в течение которого была активной группа процессов (если работа группы была завершена), в противном случае (если время не установлено), то его необходимо выставить вручную, используя календарь (но не более, чем на 72 часа назад или на время, установленное в профиле Антишифра).



Важно

При необходимости можно сделать корректировку времени. Для чего это нужно? Представьте ситуацию: легитимный процесс работал 3 дня, а заразился из-за уязвимости всего 10 минут назад.

Если откатить работу за все три дня , то можно потерять значительный объем данных, восстановленных из сильно устаревших копий, поэтому лучше сузить диапазон вручную, чтобы отменить только операции, который произвел шифровальщик после заражения.

После выбора временного диапазона пользователю останется только определить, какие операции следует отменить (операции с файлами вместе с ключами реестра, файлами или ключами реестра по отдельности) и нажать кнопку **Отправить**.

На странице агента в области **Запуски задач агента** в то же время создается запуск, по которому можно отследить вывод команды: наименование команды, сколько операций сделал модуль ремедиации. Тут речь идёт не о количестве восстановленных файлов и ключей реестра, а именно об отменённых изменениях. Под операцией подразумевается, например, создание файла, переименование файла, восстановление файла из резервной копии. Если шифровальщик зашифрует 1 файл, 8 только переименует, а один создаст, то в

сообщении будет фигурировать, что отменено именно 10 операций. Аналогичным образом будут отображаться операции с реестром (рис. 122).

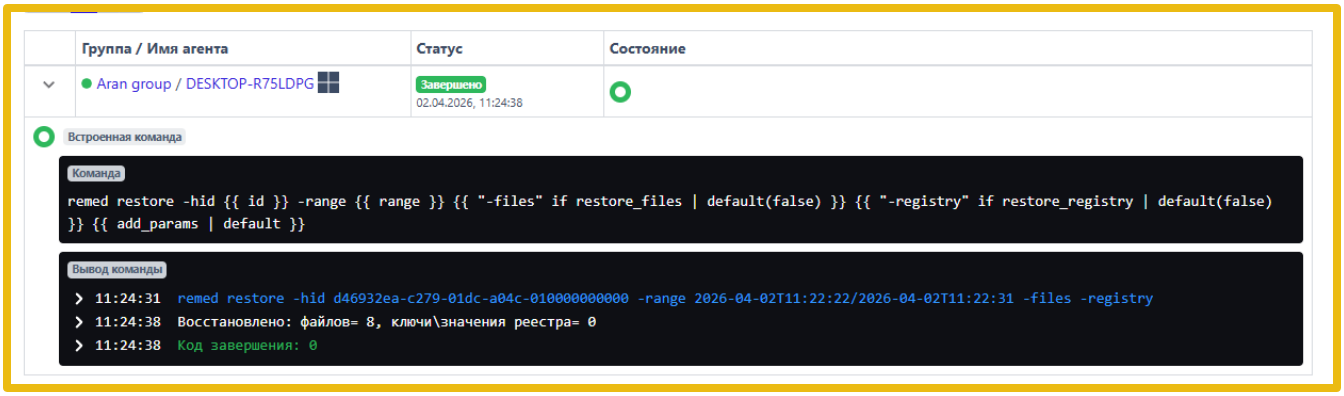


Рисунок 122 – Вывод запуска задачи на агенте

То есть ремедиация подразумевает, что созданные вредоносом файлы и ключи реестра будут удалены, переименованные файлы и ключи реестра получат исходное имя и место расположения, а удалённые или зашифрованные восстановятся к первоначальному виду из резервной копии.

При работе с командой в онлайн-терминале и создании сценария в планировщике задач алгоритм действия такой же – определить hid группы процессов, совершавшей вредоносные действия, указать временной период, на который будет выполнена ремедиация, определить, какие операции будут отменены (операции с файлами, реестром или и то, и другое), после чего написать соответствующую команду и выполнить её, а для сценария в планировщике задач необходимо создать задачу, после чего также запустить её.

11.28.2. Профили безопасности агента

Профиль безопасности агента – это профиль настроек Программы.

Опции **Профиля безопасности агента** – это опции настройки нагрузки на систему с помощью увеличения или уменьшения потока событий, регистрируемых на агенте, а также управления уровнем безопасности, который будет предоставлять агент.

На странице **Профили безопасности агента** аналитик может создавать и редактировать профили, с помощью которых для верифицированных агентов устанавливаются параметры безопасности. В соответствии

с этими параметрами будут формироваться события и инциденты, присылаемые агентом в модуль администрирования.

Набор инструментов для работы с профилями не отличается от набора инструментов для настроек профилей защиты данных или создания и редактирования наборов индикаторов компрометации, атак и т.д.

Аналитик может выполнить следующие операции на странице **Профили безопасности агента**:

– добавить новый профиль безопасности;

– сохранить изменения в профиле и передать изменения агентам, которым назначен выбранный профиль;

– редактировать название профиля безопасности;

– удалить один или несколько профилей безопасности.

Чтобы изменить параметры безопасности, аналитику необходимо выбрать профиль безопасности агента и настроить его в соответствии с требуемыми параметрами.

Профиль безопасности агента

На странице **Профиль безопасности агента** аналитик может настроить параметры, в соответствии с которыми будут обнаруживаться события на агентах. Такая предварительная настройка позволит управлять нагрузкой на систему.

Настройки профиля безопасности агента подразделяются на следующие группы:

– параметры оптимизации потока событий;

– общие настройки безопасности;

– фильтрация WMI-событий;

– параметры безопасности монитора процессов;

– настройки Antimalware Scan Interface Windows (AMSI);

– параметры безопасности файлового монитора;

– настройки противодействия сетевым атакам;

– настройки безопасности сетевого монитора;

В нижней части страницы находятся кнопки применения настроек, экспорта и импорта профиля безопасности (). Кроме того, после изменения профиля появляется кнопка отката этих изменений (). Экспорт и импорт файла осуществляется в формате txt.

В области **Оптимизация потока событий** аналитик может управлять отправкой с агентов следующих событий:

1) Исключать файловые события ранней стадии запуска процессов;
2) Фильтровать файловые события;
3) Исключать файловые события префетчера;
4) Исключать события чтения исполняемых файлов, связанные с их исполнением;
5) Исключать события чтения исполняемых файлов;
6) Исключать события чтения любых файлов;
7) Исключать файловые события процесса-создателя файла;
8) Исключать события изменения параметров безопасности файлов;
9) Исключать события доступа к процессам и нитям;
10) Исключать события загрузки известных модулей;
11) Исключать события установки сетевых соединений для протокола DNS;
12) Исключать события завершения сетевых соединений;
13) Фильтровать события модификации реестра;
14) Исключать события RPC-вызовов;
15) Исключать события со статусом «Разрешено» (кроме ключевых);
16) Исключать все события со статусом «Разрешено»;
17) Оптимизировать поток файловых событий;
18) Оптимизировать поток сетевых событий;
19) Оптимизировать поток событий межпроцессного взаимодействия;
20) Оптимизировать поток событий реестра.

Установив или сняв определенные флаги, аналитик может увеличить или уменьшить количество событий, присылаемых агентом в модуль администрирования. Это позволяет снизить информационный шум или, наоборот, увеличить отображаемую активность, чтобы изучить ее в полном объеме.

С помощью общих настроек безопасности аналитик может установить режим «только детектирование», который позволяет отключить противодействие угрозам в режиме реального времени, то есть действия, которые могут нанести вред защищаемой инфраструктуре не будут блокироваться, но при этом не будет и ложноположительных срабатываний, которые могут привести к запрету на запуск какой-либо полезной программы, действия которой EDR может посчитать нелегитимными в соответствии со своими внутренними или созданными аналитиками правилами.



Важно

Режим «только детектирование» не распространяется на работу блокирующих исключений, то есть действие «блокировать», установленное по отношению к исключениям для программ, файлов или сетевых исключений будет исполняться, несмотря на выбор этого режима.

Кроме того, в общих настройках доступна опция Принудительное подавление событий процессов при превышении лимита.

После общих настроек аналитик может также настроить фильтрацию по WMI-событиям. Для WMI доступны три способа фильтрации:

1) По вызову метода;
2) По созданию процесса;
3) По ключевым словам, указанным в профиле безопасности.

В добавление к вышеуказанным методам фильтрации в профиле добавлена опция для отключения генерации событий WMI. Для этого необходимо выбрать пункт фильтрации **Не отправлять события**.

Ключевые слова задаются аналитиком по принципу включения/исключения подстрок, то есть можно задать, какие слова должны содержать строки WMI-запросов, или можно задать, какие слова при фильтрации событий, поступающих от WMI, строки запросов содержать не должны.



Важно

Все поля ввода профиля безопасности агента поддерживают ввод до 255 символов (байтов).

В области **Настройки безопасности монитора процессов** администратор может настроить реакции Программы на события определенного типа:

– создание нити в стороннем процессе (кроме авторизованных программ Windows);

– доступ к стороннему процессу/нити (кроме авторизованных программ Windows.

Доступны следующие реакции:

1) Разрешить;

2) Блокировать только для неподписанных программ;

3) Блокировать.

При выборе реакции **Блокировать** события соответствующего типа будут отображаться в разделе **Инциденты**, а их активность будет блокироваться Программой. Кроме того, для событий создания нити в стороннем процессе и доступа к стороннему процессу/нити возможно настроить уровень важности, который соответствует уровню критичности события (от уровня **Информация** до уровня **Критичный**).

Настраивать AMSI можно в области **Настройка Antimalware Scan Interface Windows (AMSI)**. Аналитик может включать/отключать работу AMSI, ограничивать размер содержимого в событиях AMSI, выбирать политику резервирования бесфайлового содержимого, ограничивать максимальное использование диска для хранения резервных копий содержимого AMSI, а также определять политику YARA-сканирования AMSI-содержимого.

Для безопасности файлового монитора в Программе предусмотрена настройка реакции на прямой доступ к жесткому диску (кроме авторизованных программ Windows), а также выбор режима глубокого сканирования файлов. Аналитик может выбрать для профиля безопасности одну из следующих реакций на события прямого доступа к жесткому диску:

– Блокировать;

– Блокировать запись;

– Блокировать запись только для неподписанных программ;

– Разрешить.

Примечание

Список программ с доверенными подписями содержит проверенное общеупотребительное ПО.

Также в настройках безопасности файлового монитора можно установить флаги **Подсчитывать хеш SHA-1**, **Подсчитывать хеш MD5** и **Подсчитывать хеш Imphash**. По умолчанию эти функции отключены, так как создают существенную нагрузку на файловый монитор и на работу ОС соответственно.

В случае выбора режима «только детектирование» изменение настроек безопасности монитора процессов и файлового монитора будет заблокировано, за исключением выбора режима глубокого сканирования файлов.

Доступно четыре режима глубокого сканирования файлов:

1) Не сканировать;

2) **ML** (сканирование с помощью машинного обучения);

3) **YARA-правила** (сканирование на основе YARA-правил, созданных в разделе с аналитикой);

4) **ML и YARA-правила** (сканирование и с помощью машинного обучения, и с помощью YARA-правил).

По умолчанию устанавливается режим **Не сканировать**, чтобы снизить нагрузку на файловый монитор. Кроме того, пользователь может задать расширения файлов с потенциально активным содержимым. Это позволит расширить набор обрабатываемых сканером файлов, то есть добавить к базовым PE-файлам, которые обрабатываются по умолчанию, файлы с указанными здесь расширениями, например, PDF, PS1, PSM1 и т.д.

Примечание

На агенте Linux поддерживается обработка только исполняемых файлов и файлов с расширением .so.

Нежелательно указывать здесь расширения для PE-файлов, например, EXE, так как эти файлы сканируются Программой по умолчанию.

Примечание

Ввод нескольких значений в поле **Расширения файлов с потенциально активным содержимым** осуществляется через разделитель |, а в поле **IP-адреса клиентов, DNS-запросы которых не обрабатываются и исключаются из телеметрии** осуществляется через разделитель ;.

Если включен режим глубокого сканирования, то активируется опция сканирования исполняемых файлов. Администратор может выбрать проверять все исполняемые файлы, сканировать файлы без электронной подписи или сканировать файлы без доверенной электронной подписи.

Совет

Не рекомендуется включать глубокое сканирование в случае совместной работы с антивирусами сторонних вендоров. Это создает значительную нагрузку на файловую систему.

Кроме указанных выше настроек в Программе предусмотрены настройки противодействия сетевым атакам и настройки безопасности сетевого монитора.

Настройки безопасности сетевого монитора включаются и отключаются флагами **Активная защита от сканирования сетевых портов, Запретить входящие сетевые подключения, Отправлять события ICMP**. Также в настройках безопасности сетевого монитора находится поле **IP-адреса клиентов, DNS-запросы которых не обрабатываются и исключаются из телеметрии**.

Чтобы логика настроек применялась на агентах, для которых установлен профиль безопасности, после его изменения необходимо нажать кнопку **Передать профиль агентам** ( ).

В некоторых случаях профиль безопасности может иметь некорректный или устаревший формат, его можно исправить, нажав кнопку **Восстановить по умолчанию** или **Актуализировать профиль**. Актуализация профиля необходима, если в профиле безопасности появляются новые параметры со значениями по умолчанию.

Подробное описание опций профиля безопасности агента

Оптимизация потока событий

Исключать файловые события ранней стадии запуска процессов.

Ранней стадией запуска процессов считается период разворачивания процесса с момента его старта и до момента начала загрузки им критических системных библиотек (например, ntdll, kernel32 и т.п. в Windows). Если данная опция выставлена, то в обозначенный период файловые события процессов отправляться не будут. Считается, что в этот период работает только код системного загрузчика процессов, а его файловые события нерелевантны в контексте ИБ.

Фильтровать файловые события.

Если данная опция выставлена, то из потока исключаются следующие файловые события:

– Windows:

1) операции чтения для файлов desktop.ini, *.mui, *.manifest, *.icm, *cat со стороны любых процессов;

2) операции чтения для файлов tzres.dll, stdole2.tlb, sortdefault.nls, hosts, *.ttf в системном каталоге (подкаталоге) со стороны любых процессов;

3) операции чтения/записи файлов в каталогах (подкаталогах) c:\users\<username>\appdata\{local|locallow|roaming}со стороны процессов браузеров;

4) операции с именованными каналами mojo.*, crashpad_*, wkssvc со стороны процессов браузеров.

Исключать файловые события префетчера.

Префетчер – это компонент ОС, ускоряющий запуск процессов за счет предподготовки определенных данных. Если данная опция выставлена, то файловые события префетчера отправляться не будут. Поскольку префетчер – это доверенный системный компонент, работающий на начальном этапе разворачивания процессов, его файловые события нерелевантны в контексте ИБ.

Исключать события чтения исполняемых файлов, связанные с их исполнением.

Для загрузки исполняемых файлов ОС производит их чтение с диска. Агент может отличить обычное чтение файлов (в т.ч. исполняемых), которое может выполнять любой процесс, от чтения с целью исполнения их кода, которое выполняет сама система, что является менее значимым в контексте ИБ. Поэтому предусмотрена опция, позволяющая полностью исключить из потока подобные файловые события.

Исключать события чтения исполняемых файлов.

Система или процессы могут производить чтение исполняемых файлов для тех или иных целей, например, доступ к ресурсам (исполняемые файлы Windows в формате PE) или получение файловых метаданных. Данная опция позволяет исключить из потока такие файловые события.

Исключать события чтения любых файлов.

Данная опция позволяет безусловно исключить из потока любые события чтения любых файлов. Поскольку события чтения файлов являются одними из самых массовых, исключение их из потока существенно (кратно) сокращает событийный трафик, однако может сократить возможности аналитика по расследованию инцидентов ИБ.

Исключать файловые события процесса-создателя файла.

Если тот или иной процесс создает новый файл на диске, то он в дальнейшем, как правило, записывает в него какие-то данные.

Сам факт создания нового файла в большинстве случаев уже является достаточным в контексте ИБ, поэтому дальнейшую файловую активность процесса-создателя файла в отношении созданного им файла можно исключить, установив данную опцию.

Исключать события изменения параметров безопасности файлов.

Данная опция позволяет исключить из потока события изменения параметров безопасности файлов: изменение владельца, основной группы владельца файла, списка избирательного управления доступом (DACL), системного списка управления доступом (SACL) и уровень целостности файла (MIC/Integrity level).

Исключать события доступа к процессам и нитям.

Данная опция позволяет безусловно исключить из потока любые события межпроцессного взаимодействия. Поскольку события межпроцессного взаимодействия являются достаточно частыми, исключение их из потока существенно сокращает событийный трафик, однако может сократить возможности аналитика по расследованию инцидентов ИБ.

Исключать события загрузки известных модулей.

Данная опция позволяет исключать из потока события загрузки «известных» исполняемых модулей. Поскольку события загрузки исполняемых модулей множатся событиями старта процессов, данная оптимизация позволяет существенно сократить поток событий.

К «известным» модулям относятся следующие модули:

– модули, подписанные Microsoft Windows или Microsoft Corporation;

– модули, чьи хеши или имена файлов внесены в файловые исключения, назначенные агенту, со статусом «Разрешено»;

– следующие модули Windows:

1) %systemdisk%\windows\system32\shcore.dll;

2) %systemdisk%\windows\system32\sechost.dll;

3) %systemdisk%\windows\system32\rpcrt4.dll;

4) %systemdisk%\windows\system32\combase.dll;

5) %systemdisk%\windows\system32\ntdll.dll;

6) %systemdisk%\windows\system32\wow64.dll;

7) %systemdisk%\windows\system32\wow64win.dll;

8) %systemdisk%\windows\system32\wow64cpu.dll;

9) %systemdisk%\windows\system32\kernel32.dll;

10) %systemdisk%\windows\system32\kernelbase.dll;

11) %systemdisk%\windows\system32\advapi32.dll;

12) %systemdisk%\windows\system32\msvcrt.dll;

13) %systemdisk%\windows\system32\ucrtbase.dll;

14) %systemdisk%\windows\system32\gdi32.dll;

15) %systemdisk%\windows\system32\user32.dll;

16) %systemdisk%\windows\system32\win32u.dll;

17) %systemdisk%\windows\system32\comdlg32.dll;

18) %systemdisk%\windows\WinSxS*\comdlg32.dll;

19) %systemdisk%\windows\system32\comctl32.dll;

20) %systemdisk%\windows\WinSxS*\comctl32.dll;

21) %systemdisk%\windows\system32\shell32.dll;

22) %systemdisk%\windows\system32\shlwapi.dll;

23) %systemdisk%\windows\system32\oleaut32.dll;

24) %systemdisk%\windows\system32\version.dll;

25) %systemdisk%\windows\system32\imm32.dll;

26) "%systemdisk%\windows\system32\winmm.dll";

27) "%systemdisk%\windows\system32\ws2_32.dll";

28) "%systemdisk%\windows\system32\mswsock.dll";

29) "%systemdisk%\windows\system32\setupapi.dll";

30) "%systemdisk%\windows\system32\dwmapi.dll";

31) "%systemdisk%\windows\system32\winspool.drv";

32) "%systemdisk%\windows\system32\msctf.dll";

33) "%systemdisk%\windows\system32\uxtheme.dll";

34) "%systemdisk%\windows\system32\userenv.dll";

35) "%systemdisk%\windows\system32\msimg32.dll";

36) "%systemdisk%\windows\system32\usp10.dll";

37) "%systemdisk%\windows\system32\lpk.dll";

38) "%systemdisk%\windows\system32\mscoree.dll";

39) "%systemdisk%\windows\system32\bcrypt.dll";

40) "%systemdisk%\windows\system32\sspicli.dll";

41) "%systemdisk%\windows\system32\sxs.dll";

42) "%systemdisk%\windows\system32\windows.storage.dll";

43) "%systemdisk%\windows\system32\wininet.dll";

44) "%systemdisk%\windows\system32\ole32.dll";

Для ОС семейства Linux точный путь до каждого модуля индивидуален для конкретной ОС (Ubuntu, RedOs, Debian и т. д.). Ниже представлен перечень модулей (слева) и пример пути для ОС Ubuntu 20.04 (справа).

1) libcap – /usr/lib/x86_64-linux-gnu/libcap-ng.so.*;

2) libpcre – /usr/lib/x86_64-linux-gnu/libpcre.so.*;

3) libpthread – /usr/lib/x86_64-linux-gnu/libpthread-*.so;

4) librt – /usr/lib/x86_64-linux-gnu/librt-*.so;

5) libcrypt – /usr/lib/x86_64-linux-gnu/libcrypt.so.*;

6) libcrypto – /usr/lib/x86_64-linux-gnu/libcrypto.so.*;

7) libdl – /usr/lib/x86_64-linux-gnu/libdl-*.so;

8) libgcc – /usr/lib/x86_64-linux-gnu/libgcc_s.so.*;

9) libm – /usr/lib/x86_64-linux-gnu/libm.so;

10) libc – /usr/lib/x86_64-linux-gnu/libc-*.so, /usr/lib/x86_64-linux-gnu/libc.so;

11) libstdc++ – /usr/lib/x86_64-linux-gnu/libstdc++.so.*;

12) libz – /usr/lib/x86_64-linux-gnu/libz.so.*;

13) libzstd – /usr/lib/x86_64-linux-gnu/libzstd.so.*;

14) libselinux – /usr/lib/x86_64-linux-gnu/libselinux.so.*.

Исключать события установки сетевых соединений для протокола DNS.

Данная опция управляет отправкой событий входящих и исходящих подключений к UDP-порту 53 (протокол DNS).

Как правило, сами события подключения к DNS-серверу имеют малую практическую ценность, поэтому для сокращения трафика могут исключаться из потока.

Исключать события завершения сетевых соединений.

Данная опция управляет отправкой событий завершения соединений. Данные события являются парными для событий установки входящих и исходящих соединений и, таким образом, могут создавать большой поток, поэтому для сокращения трафика могут исключаться из потока.

Фильтровать события модификации реестра.

Данная опция управляет режимом отправки событий модификации значений реестра Windows. Если опция установлена, то отправляются только события модификации релевантных с точки зрения ИБ значений реестра (точки автозапуска, настройки безопасности, опции групповых политик и др. – конкретный перечень может меняться от версии к версии агента), что сокращает поток событий без существенного ухудшения защитных свойств системы.

Если опция не установлена, то отправляются все без исключения события модификации значений реестра.

Исключать события RPC-вызовов.

Опция позволяет исключить из потока события источника **Вызовы: RPC**.

Исключать события со статусом "Разрешено" (кроме ключевых).

Статус «Разрешено» назначается событиям в результате действия исключений (заданных аналитиком или встроенных в агент). Данная опция позволяет исключать из потока те из событий со статусом «Разрешено», у которых нет ассоциированного с ними правила.

Исключать все события со статусом "Разрешено".

Данная опция подразумевает безусловное исключение из потока всех событий со статусом «Разрешено» (вне зависимости от наличия или отсутствия ассоциированного с ними правила).

Оптимизировать поток файловых событий.

Оптимизация потока файловых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Оптимизировать поток сетевых событий.

Оптимизация потока сетевых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Оптимизировать поток событий межпроцессного взаимодействия.

Оптимизация потока событий межпроцессного взаимодействия заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Оптимизировать поток событий реестра.

Оптимизация потока событий реестра заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Фильтрация WMI-событий.

Данная опция позволяет выбрать один из режимов фильтрации WMI-событий Windows:

1) Создание процесса – будут доступны только события создания процессов посредством WMI (вызов метода Create объекта класса Win32_Process);

2) Вызов метода – будут доступны только события вызовов методов классов;

3) По ключевым словам – будут доступны события WMI, удовлетворяющие условиям наличия/отсутствия подстрок, перечисленных в соответствующих полях ниже;

4) Не отправлять события – WMI-события полностью исключаются из потока.

В любых режимах фильтрации внутренняя аналитика, направленная на выявление техник закрепления в системе Windows посредством WMI, продолжает работать.

Общие настройки безопасности

Режим "только детектирование" (противодействие угрозам в режиме реального времени на агенте отключено).

Если режим «только детектирование» включен, то все блокирующие реакции, заданные для индикаторов компрометации и атак, а также YARA-правил, переопределяются агентом на «детектирование». В этом случае в поле «Причина предпринятого действия» события делается соответствующая пометка, которая позволяет понять, что то или иное событие не заблокировано из-за включенного режима «только-детектирование», но будет блокироваться в «боевом» режиме.

Такой режим работы агента может использоваться в двух сценариях:

– начальный период развертывания EDR, когда аналитиками изучается профиль событий новой информационной системы и подавляются ложные срабатывания;

– демонстрационный режим, позволяющий наблюдать этапы развития атаки и оценивать возможности агента по детектированию/реагированию на каждом этапе (в «боевом» режиме атака была бы заблокирована на раннем этапе).

Режим «только детектирование» не распространяется на блокирующие действия, предписанные сетевыми и файловыми исключениями.

Принудительно подавлять события процессов при превышении лимита.

Данная опция включает/отключает механизм принудительного ограничения потока событий процессов. Если процесс в течение 10 минут генерирует более 100 тысяч событий, то передача на сервер его событий с критичностью **Информация** прекращается на 1 час (события с более высокой критичностью продолжат передаваться). Передача событий процесса возобновляется при назначении ему исключений или их изменении, а также по истечении периода ограничения.

Кроме того, предусматривается возможность запрещения принудительного подавления событий с помощью флага **Запрет принудительного подавления событий** исключений для программ.

Важно

При этом необходимо помнить о возможности исключения телеметрии основных источников (процессы, файлы, сеть, реестр) или аналитической активности (файловые и сетевые исключения, а также индикаторы атак) путем указания соответствующего флага в разделе **Исключения для программ**

Настройки безопасности монитора процессов

Реакция на создание нити в стороннем процессе (кроме авторизованных программ Windows).

Данная опция управляет политикой агента для Windows в отношении внедрения кода одним процессом в другой (сторонний).

Указанная здесь критичность будет использована при формировании агентом события внедрения кода. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке внедрения кода.

Действие определяет автоматизированную реакцию на внедрение кода со стороны агента. Возможны следующие действия:

– блокировать;

– блокировать только для неподписанных программ;

– разрешить.

Логика опции не распространяется на программы, у которых есть право внедрения кода в сторонние процессы, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Реакция на доступ к стороннему процессу/нити (кроме авторизованных программ Windows).

Данная опция управляет политикой агента для Windows в отношении доступа одного процесса к другому процессу (стороннему) или его нити (потоку). Указанная здесь критичность будет использована при формировании агентом события доступа. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке доступа. Действие определяет автоматизированную реакцию на доступ со стороны агента. Возможны следующие действия:

– блокировать;

– блокировать только для неподписанных программ;

– разрешить.

Логика опции не распространяется на программы, у которых есть право доступа к сторонним процессам/нитям, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Настройки Antimalware Scan Interface Windows (AMSI)

Разрешить работу AMSI.

Включение механизма AMSI позволяет EDR проверять запускаемые скрипты (JavaScript, VBScript), командные сценарии (powershell, wscript, cscript), макросы Office VBA и исполняемые модули (в том числе бесфайловые), загружаемые в процессы.



Важно

Механизмы AMSI поддерживаются начиная с Windows 10 и Windows Server 2016.

Когда AMSI включен, EDR генерирует соответствующие события, проверяет артефакты по наборам ИК, YARA-правилам и TI-платформе (если настроена соответствующая интеграция). Нагрузка на Программу при сканировании AMSI зависит от количества правил.

Ограничение размера содержимого в событиях AMSI.

Содержимое AMSI – это текст или двоичные данные, являющиеся объектом контроля. Текстовое содержимое может быть включено в событие EDR в непосредственном виде для удобства анализа.

Данная опция ограничивает максимальный размер текстового содержимого, включаемого в событие (но не более 32766 символов). Ограничение в 0 символов отключает отправку содержимого. Если содержимое ограничивается по размеру (т.е. отправляется частично), то оно становится предметом резервирования, согласно установленной ниже политике.

Политика резервирования AMSI-содержимого.

Зачастую ВПО использует бесфайловые (fileless) техники атак или же вредоносное содержимое удаляется для сокрытия следов атаки. Резервирование заключается в сохранении на диск содержимого (объектов контроля) AMSI для обеспечения возможности его последующей загрузки по требованию на сервер EDR с целью углубленного анализа. Предусматриваются следующие опции резервирования:

1) Резервирование отключено;
2) Резервирование бесфайлового (fileless) содержимого;
3) Резервирование любого содержимого.

По умолчанию резервируется только бесфайловое (fileless) содержимое. Если текстовое содержимое целиком включено в событие, то оно не резервируется. Если содержимое зарезервировано, то в событие включается ссылка, позволяющая загрузить его на сервер EDR.

Ограничение максимального использования диска для хранения резервных копий содержимого AMSI.

Данная опция позволяет ограничить объем дискового пространства для хранения резервных копий содержимого (объектов контроля) AMSI. Минимальное ограничение – 1 Мб, максимальное – 100 Мб. По умолчанию действует ограничение в 10 Мб. При достижении установленного ограничения более старые резервные копии будут удаляться для высвобождения места для хранения более новых.

Политика Yara сканирования AMSI содержимого.

Данная опция управляет механизмом сканирования AMSI-содержимого движком YARA. Сканирование производится по набору YARA-правил для файлов, назначенному агенту. При срабатывании YARA-правил в поток событий добавляется обнаружение «Файл классифицирован как вредоносный (YARA-правила)».

Предусмотрены следующие политики сканирования:

1) Сканирование отключено;
2) Сканирование бесфайлового (fileless) содержимого;
3) Сканирование любого содержимого.

По умолчанию сканирование отключено.

Сканирование бесфайлового содержимого позволяет находить вредоносные сигнатуры в памяти.

Сканирование содержимого, имеющего ассоциированный файл, также может быть полезно, поскольку в уведомлениях AMSI содержимое деобфусцировано, что дает больше возможностей по написанию универсальных YARA-правил.

Настройки безопасности файлового монитора

Реакция на прямой доступ к жесткому диску (кроме авторизованных программ Windows).

Данная опция управляет политикой агента для Windows в отношении прямого доступа того или иного процесса к жесткому диску для его чтения или записи. Указанная здесь критичность будет использована при формировании агентом события доступа. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке доступа.

Действие определяет автоматизированную реакцию на доступ со стороны агента. Логика опции не распространяется на программы, у которых есть право доступа к жесткому диску, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО. По умолчанию опцию рекомендуется устанавливать в значение **Блокировать запись только для неподписанных программ**, это позволит уменьшить количество ложноположительных срабатываний, а значит, необходимо будет создавать меньше исключений. Кроме того, опция позволит противодействовать вирусам, напрямую обращающимся к жесткому диску. Например, вирус-шифровальщик **petya** шифрует главную загрузочную запись, включением опции мы предотвращаем эту возможность.

Подсчитывать хеш SHA-1.

По умолчанию агент при обработке файлов с потенциально активным содержимым подсчитывает хеш SHA256. Данная опция заставляет его подсчитывать еще и хеш SHA-1, а также проводить матчинг файловых индикаторов компрометации и исключений соответствующего типа. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Подсчитывать хеш MD5.

По умолчанию агент при обработке файлов с потенциально активным содержимым подсчитывает хеш SHA256. Данная опция заставляет его подсчитывать еще и хеш MD5, а также проводить матчинг файловых индикаторов компрометации и исключений соответствующего типа. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Подсчитывать хеш Imphash.

Данная опция включает подсчет хеша Imphash для PE-файлов. Метод import hashing (Imphash) заключается в вычислении хеш-значений на основе имён библиотек и импортируемых функций с учетом порядка их расположения внутри исполняемого файла.

Этот хеш может использоваться для быстрой группировки и идентификации связанных образцов вредоносного ПО. Существуют различные модификации подсчета хеша Imphash, формирующие различные значения хеша для одного и того же файла. Агент для подсчета использует алгоритм, аналогичный YARA. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Режим глубокого сканирования файлов.

Обязательная часть анализа со стороны агента для всех файлов с потенциально активным содержимым включает в себя подсчет хеш-сумм, матчинг индикаторов компрометации и файловых исключений. Для файлов формата PE (Windows Portable Executable) дополнительно производится разбор электронной подписи и метаинформации о файле. Глубокое сканирование подразумевает дополнительные проверки – YARA-правила и/или статический анализ на основе машинного обучения (ML), способный выявить характерные признаки вредоносного файла с использованием технологий искусственного интеллекта. Следует иметь ввиду, что сканирование с использованием ML может давать большое количество ложных срабатываний. YARA-правила являются эффективным средством сигнатурного анализа и позволяют выявить известные угрозы. При выборе данной опции для сканирования будет использован набор YARA-правил, назначенный агенту. Большое количество YARA-правил может замедлить работу системы.

Глубокое сканирование исполняемых файлов.

Для исполняемых файлов дополнительно доступно управление режимом глубокого сканирования, исходя из их электронной подписи (ЭП):

Все. Глубокое сканирование производится для любых исполняемых файлов вне зависимости от их ЭП. Данный режим глубокого сканирования исполняемых файлов может замедлить работу систему;

Без ЭП. Глубокое сканирование исключается для подписанных исполняемых файлов;

Без доверенной ЭП. Глубокое сканирование исключается только для подписанных доверенной ЭП исполняемых файлов, остальные файлы будут сканироваться (даже если они подписаны). Конкретный

перечень доверенных издателей может меняться и доступен в актуальной документации. К доверенным издателям относятся такие вендоры как Microsoft, Google, Apple, Intel и т.п.

Не обрабатывать файлы *.ni.dll (нативные образы .NET Framework).

Файлы нативных образов .NET Framework создаются в результате предкомпиляции утилитой NGEN управляемых (managed) образов для ускорения работы .NET-приложений. При каждой перекомпиляции меняется хеш-сумма нативного образа – даже несмотря на то, что исходный управляемый образ не изменялся. Это приводит к многочисленным проверкам по сути одного и того же файла (хеш меняется из-за изменения метаданных) и «засорению» кеша (cash trashing) модуля мониторинга файловой активности агента, что в конечном итоге оказывает негативный эффект на производительность агента в целом.

Кроме того, многочисленные вариации хеш-сумм одного и того же файла отправляются для проверки на TI-платформу и учитываются в подсистеме мониторинга распространения, что тоже создает избыточную нагрузку на эти модули.

Данная опция отключает обработку со стороны агента нативных образов .NET Framework – подсчет хешей, матчинг исключений и индикаторов, и отправку соответствующих событий в поток.

Расширения файлов с потенциально активным содержимым.

По умолчанию файловая аналитика (подсчет хешей, матчинг индикаторов и др.) производится только для исполняемых файлов и только при их запуске (или загрузке, если исполняемый файл – это динамически загружаемая библиотека). Данная опция позволяет дополнительно указать расширения файлов (помимо исполняемых), для которых также требуется включить файловый анализ, который будет производиться в режиме реального времени при доступе к ним.



Совет

Не стоит добавлять в этот перечень расширения исполняемых файлов (EXE, DLL, SYS, OCX, SCR, COM и т.п.) – исполняемые файлы анализируются в любом случае (при попытке их запуска) и определяются по содержимому.

Настройки противодействия сетевым атакам

Активное противодействие сканированию портов.

Данная опция включает режим эмуляции открытых TCP-портов, таким образом, что при сканировании все TCP-порты выглядят открытыми.

Это существенно затрудняет для злоумышленника идентификацию работающих сетевых сервисов, снижает вероятность атаки на них и осложняет горизонтальное распространение в сети.

Противодействие сетевым атакам на контроллеры доменов.

Данная опция включает сетевые защитные механизмы агента в отношении контроллеров доменов Windows в инфраструктуре.

IP-адреса контроллеров доменов.

Список IP-адресов контроллеров доменов, действующих в инфраструктуре. Разделитель значений – символ ;



Важно

Максимальная длина записи IP-адресов – 1000 символов.

Реакция на атаку DCSync.

Данная опция определяет реакцию агента на потенциальную сетевую атаку DCSync в отношении контроллеров доменов:

– детектирование;

– детектирование и блокирование.

Настройки безопасности сетевого монитора

Активная защита от сканирования сетевых портов.

Данная опция включает режим эмуляции открытых TCP-портов таким образом, что при сканировании все TCP-порты выглядят открытыми. Это существенно затрудняет для злоумышленника идентификацию работающих сетевых сервисов, снижает вероятность атаки на них и осложняет горизонтальное распространение в сети.

Запретить входящие сетевые подключения.

При включении данной опции все входящие TCP-подключения будут отвергаться. Если агент не выполняет роль сервера в информационной системе, то в целях безопасности все входящие подключения к нему можно запретить.

Отправлять события ICMP.

При включении данной опции в поток событий будут включаться события сетевого взаимодействия по протоколу ICMP.

IP-адреса клиентов, DNS-запросы которых не обрабатываются и исключаются из телеметрии.

Список IP-адресов, для которых DNS-запросы (исходящие клиентские и входящие серверные) и соответствующие ответы на них не обрабатываются и безвозвратно исключаются из телеметрии.

11.28.3. Профили контроля USB

Профили контроля USB предназначены для управления и регулирования использования USB-устройств на конечных точках, работающих под управлением операционных систем Windows. Эти профили предоставляют администраторам возможность применять политики безопасности, ограничивать использование неавторизованных устройств и отслеживать активность USB-устройств в сети. Внедрение профилей контроля USB позволяет организациям предотвращать утечки данных, заражение вредоносным ПО и другие риски, связанные с использованием съемных накопителей.

Основные функции профилей контроля USB включают:

Белые и черные списки устройств: аналитики могут создавать списки разрешенных (белый список) или запрещенных (черный список) USB-устройств. Это гарантирует, что только авторизованные устройства могут подключаться к конечным точкам, а неавторизованные или потенциально опасные устройства блокируются.

Разрешения: профили контроля USB позволяют детально настраивать разрешения, такие как доступ только для чтения, доступ для записи или полная блокировка определенных типов устройств (например, накопителей, принтеров, смартфонов и т.д.).

Мониторинг и уведомления в реальном времени: Профили обеспечивают отслеживание активности USB-устройств в реальном времени, предоставляя информацию о событиях и инцидентах, связанных с неавторизованными или подозрительными подключениями. Это помогает выявлять потенциальные угрозы безопасности и оперативно принимать меры.

Соответствие требованиям и аудит: профили контроля USB помогают организациям соответствовать нормативным требованиям, для чего может использоваться подробное описание событий с USB-устройствами на странице **Активность**. Эти события могут применяться для аудита и подтверждения соблюдения политик безопасности.

В настоящий момент контроль USB-устройств осуществляется только для агентов Windows.

Используя профили контроля USB, организации могут значительно повысить безопасность конечных точек, снизить риск потери данных и сохранить контроль над использованием USB-устройств в своей сети.



Важно

Профиль контроля USB не предназначен для работы в режиме детектирования.

Контроль в Программе осуществляется как над отдельными устройствами, так и над их классами:

1) Накопители;
2) Медиа-устройства;
3) Принтеры;
4) Сканеры;
5) Беспроводные устройства;
6) Коммуникационные устройства и мобильные телефоны;
7) Устройства взаимодействия с пользователями (HID-устройства);
8) Токены (смарт-карты и токены);
9) Другие;
10) Любые устройства.

Под управлением понимается задание различных разрешений для выбранных устройств: на чтение, запись, запуск программ с устройства, сбор статистики операций ввода/вывода или блокирование устройства. При этом в потоке событий будут формироваться события, связанные в том числе с нарушением разрешающей политики, например, пользователь попытается запустить программу с USB-накопителя при наличии соответствующего запрета на запуск, что приведет к формированию события на странице **Активность**.

Доступны следующие типы событий:

1) Устройство USB подключено;

2) Устройство USB отключено;

3) Зафиксирована запрещенная попытка чтения;

4) Зафиксирована запрещенная попытка записи;

5) Зафиксирована запрещенная попытка выполнения управляющего запроса;

6) Зафиксирована запрещенная попытка запуска исполняемого файла;

7) Статистика чтения/записи данных;

Для съемных носителей реализована расширенная настройка блокировки. Можно отдельно заблокировать запуск исполняемых файлов с носителя, а можно заблокировать запись данных на носитель, реализовав режим «только для чтения». При этом вносятся изменения в соответствующие ответы на специфические запросы, а именно – выставляется признак того, что устройство «только для чтения», в результате чего ОС в принципе не формирует стандартные запросы записи, завершая их с соответствующим статусом, а в пользовательском интерфейсе отсутствует возможность удалить или создать файл, при попытке отформатировать носитель будет выдано сообщение, что носитель защищен от записи.

Если в данном режиме сработает событие заблокированной попытки записи, то это значит, что скорее всего используется специальное ПО, которое пытается обойти данное ограничение ОС, формируя SCSI-запросы напрямую через механизмы SCSI Pass-Through.

Страница «Профили контроля USB»

На странице отображается таблица с профилями с тремя основными полями:

1) Название профиля;

2) **Привязано агентов** (показывает, сколько агентов работает с этим профилем);

3) **Управление** (содержит кнопки управления профилем).

На странице можно выполнить следующие операции:

1) Добавлять профили контроля USB;

2) Передавать агентам все профили, созданные и сохраненные на странице, а также отдельный профиль;

3) Редактировать название профиля;

4) Удалить профиль.

Чтобы добавить профиль, необходимо нажать кнопку **Добавить профиль**. Откроется окно **Добавить профиль**. Обязательной для заполнения является строка **Название**. Можно добавить любой из ранее созданных профилей в качестве базового профиля, но это действие является необязательным.

Для удаления профиля необходимо нажать кнопку  или воспользоваться групповым удалением, выделив соответствующие профили и нажав кнопку **Удалить выбранные профили**.

Для передачи агентам всех профилей, имеющихся на странице **Профили контроля USB**, необходимо нажать кнопку  .

Страница «Профиль контроля USB»

Страница **Профиль контроля USB** разделена на две основные области:

1) Базовые настройки;

2) Конфигурации контроля USB-устройств.

Базовой настройкой является то, включена ли подсистема контроля USB-устройств или нет. Включение выключение осуществляется с помощью кнопок  .

В области конфигурации контроля USB-устройств по умолчанию представлены общие универсальные конфигурации устройств.

Пользователь может добавить уникальную конфигурацию, нажав кнопку **Добавить правило**. Откроется окно **Создание правила контроля устройства USB**. Здесь нужно ввести информацию об уникальном идентификаторе устройства в формате **VID_PID_MI_SERIAL** или группы устройств в формате **VID_PID_MI**, эту информацию об устройствах можно узнать на странице **Активность** в событии **Устройство USB подключено.**

VID – идентификатор производителя в шестнадцатеричном формате (2 байта).

PID – идентификатор продукта в шестнадцатеричном формате (2 байта).

MI – номер интерфейса в шестнадцатеричном формате (1 байт, задается опционально, если у устройства есть несколько интерфейсов).

SERIAL – серийный номер устройства (задается опционально в виде строки без пробелов).

После ввода уникального идентификатора следует выбрать тип контролируемого устройства и добавить необходимые разрешения, по умолчанию устройство будет заблокировано.

Кроме операции блокирования устройства возможно установить следующие разрешения:

1) На чтение (для USB-накопителей);

2) На запись (для USB-накопителей);

3) На запуск программ (для USB-накопителей);

4) Полный доступ (для накопителей включает в себя разрешение на чтение, запись и запуск, для всех остальных устройств включает в себя разрешение на чтение и запись);

5) На получение статистики операций ввода/вывода (для всех типов устройств).

Здесь же можно настроить критичность для некоторых событий с USB-устройств:

1) Устройство USB подключено;

2) Устройство USB отключено;

3) Зафиксирована запрещенная попытка чтения;

4) Зафиксирована запрещенная попытка записи.

При выборе критичности от уровня **Средняя** и выше в программе будет создан инцидент, который отобразится на странице **Инциденты**, при этом необходимо отметить, что инциденты, связанные с модулем контроля USB, являются отдельными сущностями, независимыми от остальных инцидентов.

Для завершения операции по добавлению правила необходимо нажать кнопку **Создать**.



Примечание

Номер интерфейса может быть не задан, если у устройства отсутствует интерфейс или требуется задать правило для всех интерфейсов.

Если серийный номер не задан, то правило будет применяться ко всем устройствам заданного производителя с указанным кодом продукта.

Также можно задавать только идентификатор производителя (VID), чтобы разрешать или блокировать работу устройств определенных производителей, в сочетании с возможностью выбора типа контролируемого устройства **Любой** это дает возможность гибко настраивать политики контроля USB-устройств в организации. Например, мы запрещаем работу всех устройств выбранного производителя и добавляем разрешающие правила для определенных устройств по идентификатору с указанием серийного номера устройства или

полностью разрешаем применение устройств только определенного производителя, запрещая все остальные устройства.

Пользовательские конфигурации, в отличие от универсальных (они выделяются желтым цветом на странице), можно удалять, для этого в строке с конфигурацией присутствует кнопка  или можно воспользоваться групповым удалением, выделив нужные правила и нажав кнопку **Удалить выбранные**.

Для редактирования любых конфигураций в каждой из них присутствует кнопка  .

Для сохранения изменений и применения профиля требуется нажать кнопку  , после чего откроется окно подтверждения действия. После того, как пользователь нажмет кнопку **Подтвердить**, профиль будет применяться для назначенного агента.

На странице профиля имеется возможность для импорта/экспорта данных из профиля в формате txt.

Данные кнопки имеют вид:

–  – экспортировать профиль в файл формата txt;

–  – импортировать данные из файла в профиль (формат txt).

Конфигурации в профиле можно активировать и деактивировать по отдельности или группой. Для выполнения операций по отдельности используются кнопки **Деактивировать/Активировать** ( / ). Каждая операция требует подтверждения.

Для активации/деактивации группы конфигураций необходимо отметить их флагом () и нажать кнопку группового применения **Активировать выбранные элементы** () или **Деактивировать выбранные элементы** ().

Быстрое создание конфигураций контроля USB на странице «Активность»

Для событий, источником которых является модуль контроля USB, конфигурационное правило может быть добавлено с помощью мастера создания правил для USB-устройств на странице **Активность**. Для этого в каждой строке события, источником которого является **Контроль USB**, присутствует кнопка  . Нажатие кнопки открывает окно **Мастер создания правил для USB-устройств** с предзаполненными полями **Уникальный идентификатор** (VID_PID_MI_SERIAL), **Тип устройства** и полем **Профиль**, в котором можно выбрать профиль для

сохранения правила. Уникальный идентификатор отличается в зависимости от типа устройства, например, может отсутствовать номер интерфейса или серийный номер.

При нажатии кнопки **Далее** открывается окно **Создание правила контроля USB-устройства**, в котором необходимо установить разрешения для выбранного устройства.

Для завершения операции необходимо нажать кнопку **Создать**, после чего новая конфигурация появится на странице выбранного профиля контроля USB.

Важно

Правила начинают работать для вновь подключенных устройств, применение правил «на лету»не предусмотрено: сначала должны быть применены правила для агента, и только после этого при подключении устройства будут осуществлены действия, определяемые правилом.

11.28.4. Журнал безопасности

На странице **Журнал безопасности** в табличном виде представлена информация о действиях пользователей. События таблицы можно фильтровать по количеству отображаемых событий (фильтр **Показывать по**), имени пользователя (фильтр **Пользователь**), критичности события (фильтр **Критичность**), периоду регистрации, а также выполнять поиск по типу события.

Все возможные действия пользователей, отображаемые в таблице, разделены на типы и подтипы.

Для типа действия **Авторизация пользователя** предусмотрены следующие подтипы:

– вход в систему;

– выход из системы;

– выход из системы на всех устройствах.

Для типа действия **Работа с пользователем** предусмотрены следующие подтипы:

– создание нового пользователя;

– редактирование пользователя;

– изменение пароля пользователя;

– удаление пользователя из системы;

– блокировка пользователя;

– разблокировка пользователя;

– запрос на изменение пароля пользователя;

– запрос ссылки для сброса пароля;

– сброс пароля пользователя;

– создание роли;

– редактирование роли;

– удаление роли;

– назначить роль пользователям;

– отозвать роль пользователям.

Для типа действия **Работа с агентом** предусмотрены следующие подтипы:

– верификация агентов;

– отмена верификации агента;

– редактирование агента;

– потеря связи с агентом;

– изменение состава ПО на агенте;

– добавление агентов в группу;

– удаление агентов из группы;

– отправка команды агенту;

– отправка команды группе агентов;

– загрузка нового дистрибутива агента на сервер;

– удаление дистрибутива агента с сервера;

– сетевая изоляция агентов;

– снятие сетевой изоляции агентов;

– включение функции защиты агентов;

– выключение функции защиты агентов;

– включение автоматического обновления агентов;

– выключение автоматического обновления агентов;

– включение сопоставления с золотым образом;

– выключение сопоставления с золотым образом;

– включение парольной защиты от удаления агентов;

– выключение парольной защиты от удаления агентов;

– изменение критичности у агентов;

Для типа действия **Конфигурация** предусмотрены следующие подтипы:

– создание нового набора;

– удаление набора;

– добавление новых данных в набор;

– удаление данных из набора;

– импорт данных в набор;

– редактирование данных в наборе;

– копирование данных между наборами;

– перемещение данных между наборами;

– активация элементов в наборе;

– деактивация элементов в наборе;

– передача набора агентам;

– передача профиля агентам;

– применение конфигурации наборов к агентам;

– применение конфигурации профилей к агентам;

– применение конфигурации к агентам;

– создание начальной конфигурации;

– редактирование конфигурации;

– удаление конфигурации;

– синхронизация наборов аналитики с TI.

Для типа действия **Работа с файлами агента** предусмотрены следующие подтипы:

– загрузка файла агента на сервер;

– удаление файла агента с сервера;

– загрузка файла пользователя на сервер;

– удаление файла пользователя с сервера;

– создание задачи для группового скачивания файлов;

– отмена задачи для группового скачивания файлов;

– удаление файла группового скачивания с сервера.

Для типа действия **Работа с инцидентом** предусмотрены следующие подтипы:

– создание инцидента;

– смена ответственного за инцидент;

– редактирование инцидента;

– закрытие инцидента;

– назначение инцидента;

– удаление инцидента;

– добавление событий в инцидент;

– исключение событий из инцидента;

– создание инцидента в рамках обнаружения.

Для типа действия **Действие с лицензией** предусмотрен следующий подтип:

– установка новой лицензии на сервере.

Для типа действия **LDAP** предусмотрены следующие подтипы:

– создание конфигурации LDAP;

– изменение конфигурации LDAP;

– удаление конфигурации LDAP;

– активация конфигурации LDAP;

– деактивация конфигурации LDAP;

– изменение пароля привязанного пользователя LDAP;

– добавление пользователя LDAP;

– привязка пользователя LDAP;

– удаление пользователя LDAP;

– добавление сетевого адреса LDAP;

– изменение сетевого адреса LDAP;

– удаление сетевого адреса LDAP.

Для типа действий **Планировщик задач** предусмотрены следующие подтипы:

– добавление сценария;

– редактирование сценария;

– удаление сценария;

– активация сценария;

– деактивация сценария;

– добавление задачи;

– редактирование задачи;

– удаление задачи;

– запуск задачи;

– завершение выполнения задачи;

Для типа действий **TI** предусмотрены следующие подтипы:

– создание конфигурации TI;

– изменение конфигурации TI;

– удаление конфигурации TI;

– активация конфигурации TI;

– деактивация конфигурации TI;

– изменение API-ключа конфигурации TI.

Для типа действий **SIEM** предусмотрены следующие подтипы:

– создание конфигурации экспорта событий;

– изменение конфигурации экспорта событий;

– удаление конфигурации экспорта событий;

– активация экспорта событий;

– деактивация экспорта событий;

– изменение настроек конфигурации экспорта событий.

Для типа действий **Журнал безопасности** предусмотрены следующие подтипы:

– изменение конфигурации журнала безопасности.

Для типа действий **Действие с лицензией** предусмотрены следующие подтипы:

– установка новой лицензии на сервере.

Для типа действий **Сервисы** предусмотрены следующие подтипы:

– состояние сервисов.

Для типа действий **Экспорт событий безопасности** предусмотрены следующие подтипы:

– создание конфигурации webhook-экспорта событий журнала безопасности;

– изменение конфигурации webhook-экспорта событий журнала безопасности;

– удаление конфигурации webhook-экспорта событий журнала безопасности;

– активация webhook-экспорта событий журнала безопасности;

– деактивация webhook-экспорта событий журнала безопасности;

– сброс очереди экспортируемых событий журнала безопасности.

Уполномоченный пользователь может управлять событиями, отображаемыми в журнале безопасности. Для изменения списка отображаемых событий пользователю необходимо нажать кнопку **Редактировать конфигурацию** (), после чего определить, какие подтипы событий, регистрируемых в Программе, будут доступны для журналирования. Часть событий не поддерживаются, но оставлены для обратной совместимости с ранними версиями агента, это события назначения агентам различных типов конфигураций (назначение агентам профиля безопасности, набора индикаторов атак, набора индикаторов компрометации и т.д.)

Пользователь может указывать максимальный период хранения событий журнала безопасности в днях. По умолчанию это значение устанавливается на 30 дней.

11.29 Дистрибутивы

Сборки агентов, сохраняемые на странице с дистрибутивами, позволяют обновлять агентов в автоматическом режиме, если у них включена опция **Автообновление** на странице **Агент** или **Агенты** (опция включается по умолчанию при верификации новых агентов).

На странице **Дистрибутивы** отображается информация о Windows и Linux-дистрибутивах агента в виде таблицы со следующими полями:

1) Имя (содержит название дистрибутива агента);

2) Версия;

3) Дата изменения;

4) Размер (показывает размер файла дистрибутива агента);

5) Платформа (показывает название ОС, на которую устанавливается дистрибутив агента);

6) Архитектура (показывает разрядность ОС, на которую устанавливается дистрибутив агента);

7) Управление (содержит кнопку скачивания дистрибутива ).

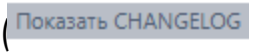
При нажатии кнопки скачивания дистрибутива произойдет сохранение выбранного дистрибутива на хост, с которого осуществлен доступ к серверу управления.

С помощью элемента > рядом с названием дистрибутива агента можно просмотреть дополнительную информацию:

1) Минимальная версия целевой платформы;

2) Описание (содержит описание изменений дистрибутива по сравнению с предшествующей версией);

3) MD5 (содержит 32-х символьное значение хеша для дистрибутива агента, рассчитанного по алгоритму MD5).

4) Кнопки просмотра лога изменений дистрибутива (

).

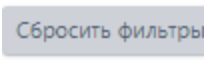
На странице **Дистрибутивы** для фильтрации информации имеется система фильтров, которая представлена следующими фильтрами:

– Показывать по (изменяется количество записей в таблице);

– Имя (данные фильтруются по имени агента);

– Версия (данные фильтруются по номеру версии дистрибутива агента);

– Платформа (данные фильтруются по имени целевой платформы: версии Linux, Windows).

– При нажатии кнопки 

происходит сброс выставленных фильтров.

11.30 Интеграции

Интеграции – это инструмент администратора Программы для настройки взаимодействия между EDR, TI-платформой, LDAP-сервером и SIEM.

TI-платформа – это централизованная платформа, предназначенная для приема, агрегации, анализа, хранения и распределения данных разведки о киберугрозах. EDR осуществляет взаимодействие с ней для усиления аналитических возможностей Программы.

От настроек интеграции зависит, какие артефакты будет проверять TI-платформа, будут ли обнаруживаться уязвимости в Программе, какое количество артефактов будет обрабатываться в одном запросе и т.д.

LDAP (Lightweight Directory Access Protocol) — это протокол, то есть набор правил, для доступа к службам каталогов. Настройка интеграции EDR с LDAP-сервером позволяет создать связь между ними, чтобы пользователи, созданные в службе каталогов, могли заходить под своими учетными записями в модуль управления EDR.

SIEM (Security Information and Event Management) — это класс программного обеспечения и услуг, предназначенный для анализа, сбора, агрегации и корреляции в реальном времени событий безопасности и данных из различных источников в ИТ-инфраструктуре организации.

На странице **Интеграции** показана информация с настройками параметров взаимодействии EDR с TI-платформой, LDAP и SIEM (рисунок 123).

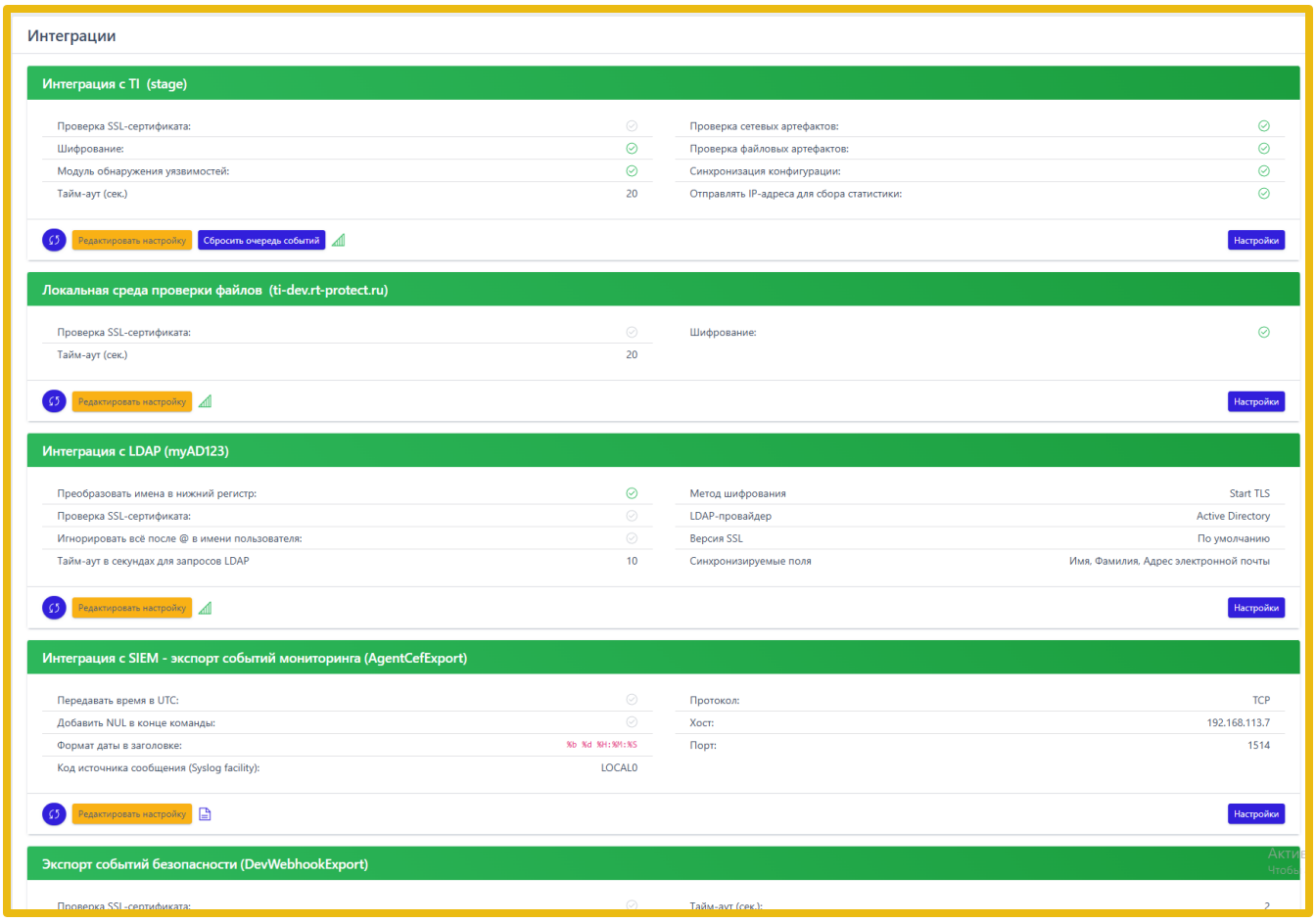


Рисунок 123 – Общий вид страницы Интеграции

Администратор сервера может просматривать настройки интеграций на данной странице, редактировать настройки, а также добавлять новые профили с настройками интеграций.

На странице имеются следующие области с информацией об интеграциях:

– Интеграция с TI;

– Локальная среда проверки файлов;

– Интеграция с LDAP;

– Интеграция с SIEM (экспорт событий мониторинга);

– Экспорт событий безопасности.

11.30.1. Интеграция с TI

В области **Интеграция с TI** администратор может настроить взаимодействие между сервером EDR и сервером TI. На странице в области **Интеграция с TI** показаны настройки интеграции, которые активны на данный момент.

Для редактирования настроек интеграции необходимо нажать кнопку Редактировать настройку, после чего откроется окно редактирования, представленное на рисунке 124.

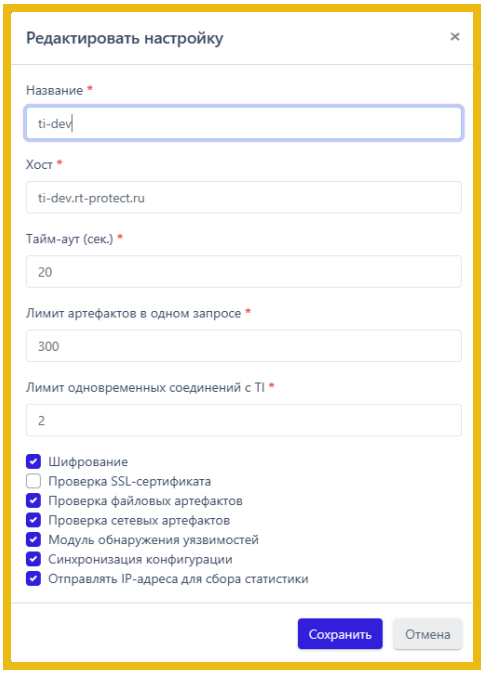


Рисунок 124 – Окно редактирования настроек интеграции с TI

После редактирования настроек следует нажать по иконке **Сохранить**.

В области **Интеграция с TI** для перехода на страницу со списком профилей с настройками следует нажать по иконке Настройки.

Страница со списками профилей настроек представлена на рисунке 125.

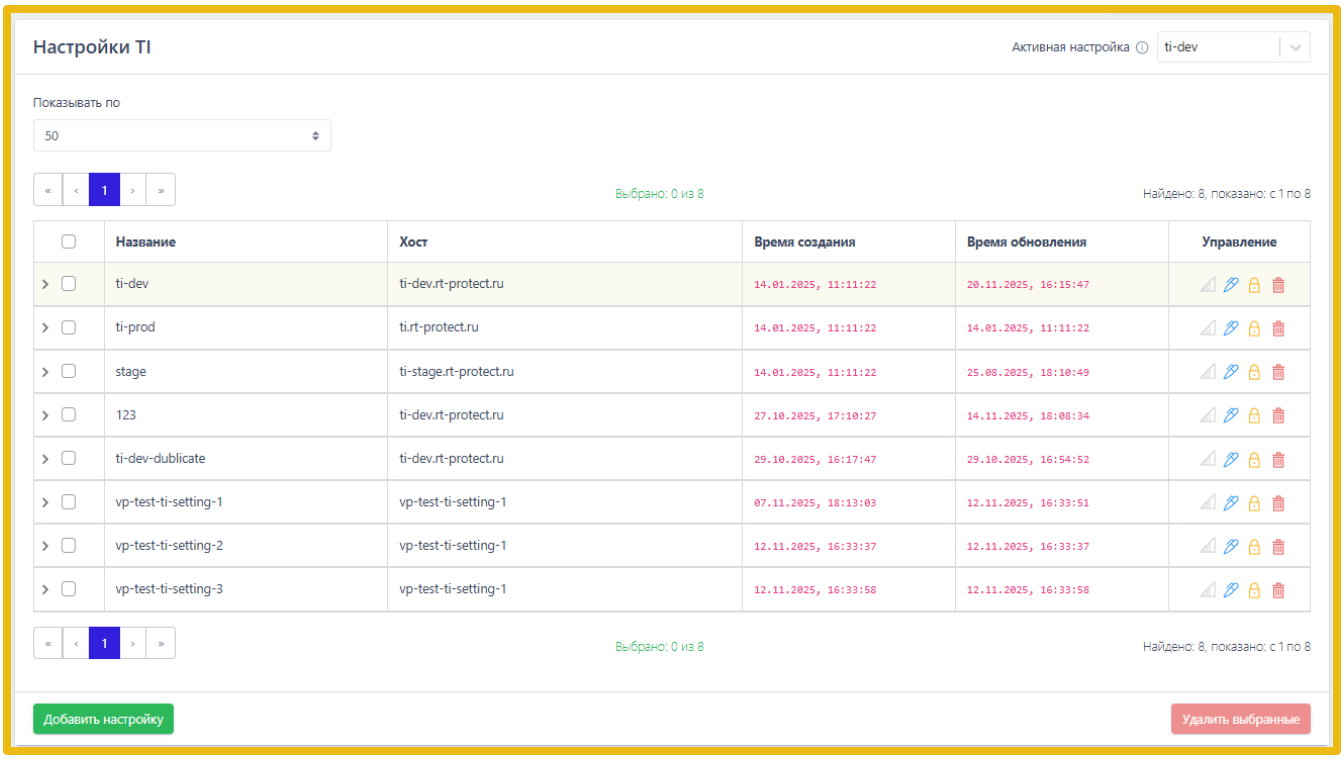


Рисунок 125 – Список профилей с настройками интеграции с TI

Информация на данной странице представлена в виде таблицы со следующими областями:

– кнопка выбора;

– иконка, раскрывающая информацию по параметрам настройки ( );

– название профиля настройки;

– имя хоста TI, с которым производится интеграция;

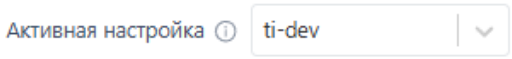
– время создания профиля с настройками;

– время обновления профиля с настройками;

– управление (проверка соединения между TI и EDR ( ), редактирование настройки ( ), изменение API-ключа настройки TI ( ), удаление настройки ( )).

Важно

Следует обратить внимание на следующие моменты: сделать активными сразу две настройки нельзя, при деактивации (выключении настройки) с TI, взаимодействие с сервером EDR будет отключено, что повлияет на аналитические возможности сервера EDR.

Выбор активной настройки осуществляется администратором в строке **Активная настройка** (

).

Важно

В случае отсутствия активной настройки интеграция будет отключена.

На странице можно добавить настройку, нажав по иконке 

.

Параметры для заполнения при добавлении новой настройки аналогичны параметрам, указанным в окне редактирования настройки, за исключением поля API-ключ.

Для добавления настройки необходимо нажать кнопку **Настройки** и далее нажать кнопку **Добавить настройку**. Откроется окно **Добавить настройку** (рис. 126).

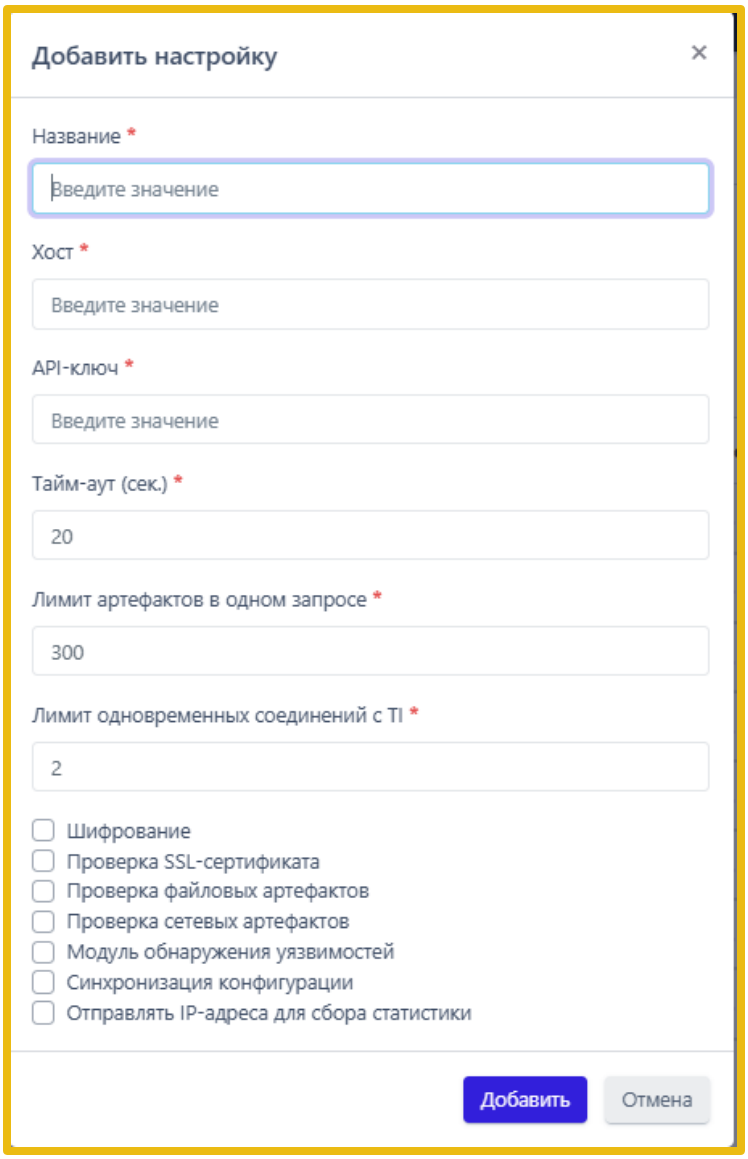


Рисунок 126 – Окно добавления настройки интеграции между TI-платформой и EDR

Название – в поле указывается название настройки интеграции.

Хост – в поле указывается имя хоста TI платформы (домен).

API-ключ – в поле указывается API-ключ. API-ключ — это уникальная строка символов (токен), которая используется для аутентификации запроса к API. API-ключ выдается производителем TI-платформы при наличии интеграции между TI-платформой и EDR.

Тайм-аут – (в секундах) ограничивает время ожидания ответа от сервера TI. Сервер TI должен ответить за это время или быстрее.

Лимит артефактов в одном запросе – определяет, сколько артефактов отправляется из EDR на TI-платформу в одном пакете.

Лимит одновременных соединений с TI – определяет лимит одновременных соединений между EDR и TI-платформой. Оптимальное значение лимита – 2 соединения.

Шифрование – опция включает или отключает шифрование при передаче запросов-ответов между EDR и TI-платформой.

Проверка SSL-сертификата – опция включает и выключает процесс проверки подлинности и валидности SSL-сертификата. Сертификат — это цифровой «паспорт» сайта. SSL – это криптографический протокол, который обеспечивает безопасную передачу данных между браузером и сервером. Проверка возможна только в том случае, если сертификат TI-платформы выпущен авторизованным центром сертификации, который может удостоверить данный сертификат, иначе эту проверку следует отключить (для самоподписанных сертификатов).

Проверка файловых и сетевых артефактов – опции включают и выключают проверку в EDR файловых артефактов (хеши SHA-256) или сетевых артефактов (IP-адреса и домены).

Модуль обнаружения уязвимостей – опция включает/отключает модуль обнаружения уязвимостей в EDR.

Синхронизация конфигурации – опция включает/отключает синхронизацию между EDR и TI-платформой внешних наборов аналитики, то есть при включенной синхронизации изменения в наборах TI-платформы приведут к изменениям внешних наборов аналитики EDR, и наоборот, при выключенной синхронизации таких изменений во внешних наборах EDR происходить не будет.

Отправлять IP-адреса для сбора статистики – опция включает или отключает отправку IP-адресов для сбора статистики. Суть этой опции в том, что если EDR отсылает пару артефактов IP-адрес+домен, то проверяется только домен (и только по нему может быть сформирован инцидент при соответствующем вердикте), а IP-адрес отбрасывается и не анализируется, но IP-адреса могут быть отправлены и сохранены в активности TI-платформы для дальнейшего разбора. Поэтому включение опции сохраняет такие IP-адреса на TI-платформе, что позволяет в дальнейшем аналитику платформы их проанализировать.

При необходимости конфигурацию настроек или несколько таких конфигураций можно удалить, используя кнопки **Удалить настройку** ( ) или **Удалить выбранные**.

11.30.2. Локальная среда проверки файлов

Интеграция с TI для анализа файлов позволяет EDR отправлять файлы на TI-платформу для их дальнейшей проверки с помощью песочницы. Настройки за небольшим исключением повторяют настройки интеграции с TI для отправки артефактов.

Чтобы настроить интеграцию с TI-платформой для анализа файлов, необходимо выполнить следующие действия:

1) Определить название для интеграции;
2) Задать актуальное значение хоста TI-платформы (IP-адрес или имя хоста);
3) Задать актуальное значение API-ключа;
4) Определить тайм-аут;
5) Включить или отключить шифрование;
6) Включить или выключить проверку SSL-сертификата.

11.30.3. Интеграция с LDAP

В области **Интеграция с LDAP** администратор может настроить взаимодействие между серверами EDR и LDAP-сервером. С помощью иконки 

можно редактировать текущую настройку. Окно заполнения параметров при редактировании представлено на рисунке 127.

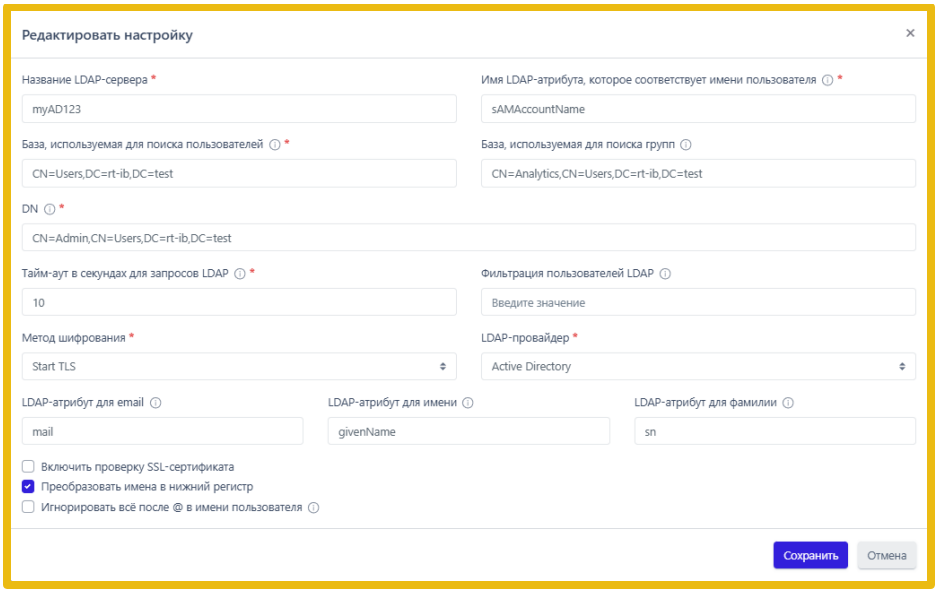
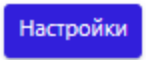


Рисунок 127 – Редактирование настроек

Для просмотра профилей созданных настроек требуется нажать по иконке 

.

Информация на странице Настройки LDAP представлена в виде таблицы со следующими полями:

1) Кнопка раскрытия информации по настройке;
2) Кнопка выбора;
3) Название LDAP-сервера;
4) DN;
5) Метод шифрования;
6) Сетевые адреса LDAP;
7) Время создания;
8) Время обновления;
9) Управление.

Примечание

Активная в данный момент настройка выделяется светло-желтым цветом .

Настройки, в которых не указаны сетевые адреса, нельзя выбрать из списка в строке **Активная настройка**.

В поле **Управление** с помощью иконок возможно выполнить следующие действия:

– проверить соединение с LDAP (нажать по иконке , дождаться ответа, успешное подключение будет отмечено иконкой , неуспешное);

– редактировать настройку (нажав по иконке);

– настроить сетевой адрес и порт LDAP-сервера (нажав по иконке);

– изменить пароль LDAP-сервера (нажав по иконке);

– удалить настройку интеграции с LDAP-сервером (нажав по иконке).

Для настройки интеграции с LDAP необходимо выполнить следующие действия:

1) **Определить название LDAP-сервера**.

2) **Определить имя LDAP-атрибута, которое соответствует имени пользователя**. Настройка **Имя LDAP-атрибута, которое соответствует имени пользователя** может принимать разные значения в зависимости от типа LDAP-провайдера и корпоративных стандартов. В качестве примеров можно привести sAMAccountName (логин для входа в домен Windows (короткое имя), самый частый вариант для корпоративных сетей Windows), uid (уникальный идентификатор пользователя, используется в OpenLDAP, FreeIPA), userPrincipalName (полное имя пользователя в формате email). Правильно для Active directory выбирать атрибут sAMAccountName или userPrincipalName, а для OpenLDAP и FreeIPA атрибут uid.

3) **Определить базу, используемую для поиска пользователей**. Это корневая папка или начальная точка в дереве LDAP-каталога, с которой начинается поиск пользователей. Типичным вариантом базы будет CN=Users, DC=mycompany, DC=local (стандартное расположение в AD). В OpenLDAP и FreeIPA также используется понятие Base DN (база для поиска) и атрибут для имени пользователя, однако, в отличие от AD, в OpenLDAP и FreeIPA обычно используются другие атрибуты и структура каталога.

4) **Определить базу, используемую для поиска групп (DN группы для ограничения доступа)**. Настройка, которая указывает системе, где именно в LDAP-каталоге искать группы для проверки членства пользователей и назначения прав доступа.

5) **Определить DN**. DN (Distinguished Name) — это строка, которая однозначно идентифицирует запись в LDAP-каталоге. Она строится путем соединения относительных имен самой записи и всех ее родительских записей вплоть до корня дерева. DN состоит из одной или нескольких пар атрибут=значение, разделенных запятыми. Движение идет от самой конкретной записи к корню дерева. DN читается справа налево, от корня (самого общего) к записи (самой конкретной). Чем дальше слева оказывается элемент, тем он "ниже" в иерархии. В случае с интеграцией с EDR DN– это логин сервисного пользователя, у которого есть необходимые права на поиск информации о других пользователях, группах и политиках. Программа устанавливает сессию от этого пользователя и начинает проверку по установленному тайм-ауту – функция синхронизации. Ее смысл в том, чтобы актуализировать данные и сессии пользователей. Например, пользователь был заблокирован/удален на стороне LDAP-сервера (при этом у него активная сессия в EDR, следовательно нужно закрыть его сессию на стороне EDR).

6) **Определить тайм-аут в секундах для запросов LDAP**. Если установить значение 0, то тайм-аут будет отсутствовать.

7) **Установить фильтрацию пользователей LDAP**. Фильтры LDAP используются для поиска записей в каталоге, которые соответствуют определенным критериям. Они следуют стандарту, описанному в RFC 4515. Базовый формат: (атрибут=значение). Например, (cn=*) – ищет все записи, у которых вообще существует атрибут cn (Common Name), независимо от его значения.

8) **Выбрать метод шифрования**. Используется для защиты запросов к каталогам. Без шифрования злоумышленник может перехватить логины и пароли. Можно выбрать Start TLS, Simple TLS или Plain.

StartTLS – это команда «давай шифровать», которая позволяет преобразовать существующее незашифрованное сетевое соединение в безопасное, используя протокол TLS.

Simple TLS – это метод установления защищенного соединения, при котором TLS-шифрование запускается в самом начале сессии, до какой-либо аутентификации.

Plain – это метод аутентификации, при котором клиент отправляет серверу свои учетные данные (логин и пароль) в открытом, незашифрованном виде. Использование Plain-аутентификации делает инфраструктуру уязвимой для некоторых типов атак.

9) **Выбрать LDAP-провайдера**. Это может быть служба каталогов Active Directory, OpenLDAP или FreeIPA.

10) **Определить LDAP-атрибут для email**. Если поле останется пустым, то синхронизации данных не будет. По умолчанию используется атрибут mail.

11) **Определить LDAP-атрибут для имени**. Если поле останется пустым, то синхронизации данных не будет. По умолчанию используется атрибут givenName.

12) **Определить LDAP-атрибут для фамилии**. Если поле останется пустым, то синхронизации данных не будет. По умолчанию используется атрибут sn.

13) **Определить LDAP-атрибут для роли**. Заполняется, если в LDAP есть атрибут, несущий информацию о роли пользователя. Если оставить поле пустым, то синхронизация не выполняется.

14) Установить или снять флаги для следующих компонентов: **Включить проверку SSL-сертификата**, **Преобразовать имена в нижний регистр**, **Игнорировать всё после @ в имени пользователя**. Проверка SSL-сертификата возможна только в том случае, если сертификат LDAP-сервера выпущен авторизованным центром сертификации, который может удостоверить данный сертификат, иначе эту проверку следует отключить (для самоподписанных сертификатов). Если включена опция **Игнорировать всё после @ в имени пользователя**, то EDR игнорирует всё после первой @ в имени пользователя LDAP, отправленном пользователем при входе. Если

используется userPrincipalName в Active Directory, то следует отключить эту опцию, так как userPrincipalName содержит @.

15) Нажать кнопку **Добавить**.

16) **После добавления сервера на страницу Настройки LDAP необходимо добавить адрес и порт**, по которому будет происходить взаимодействие между сервером LDAP и EDR (рис. 128). Обычно значение порта равно 389.

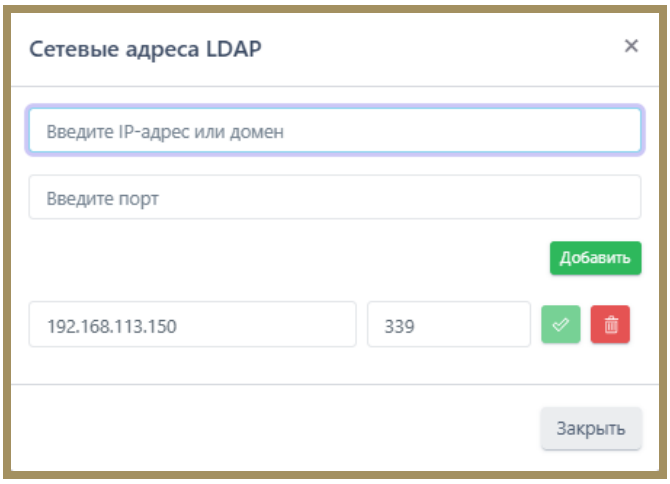


Рисунок 128 – Окно ввода сетевых адресов LDAP

При необходимости конфигурацию настроек или несколько таких конфигураций можно удалить, используя кнопки **Удалить настройку** ( ) или **Удалить выбранные**.

11.30.4. Интеграция с SIEM (экспорт событий мониторинга)

В области **Интеграция с SIEM (экспорт событий мониторинга)** уполномоченный пользователь может настроить взаимодействие между сервером EDR и SIEM. На странице показаны настройки интеграции, которые активны на данный момент.

Для редактирования настроек интеграции необходимо нажать кнопку 

, после чего откроется окно редактирования, представленное на рисунке 129.

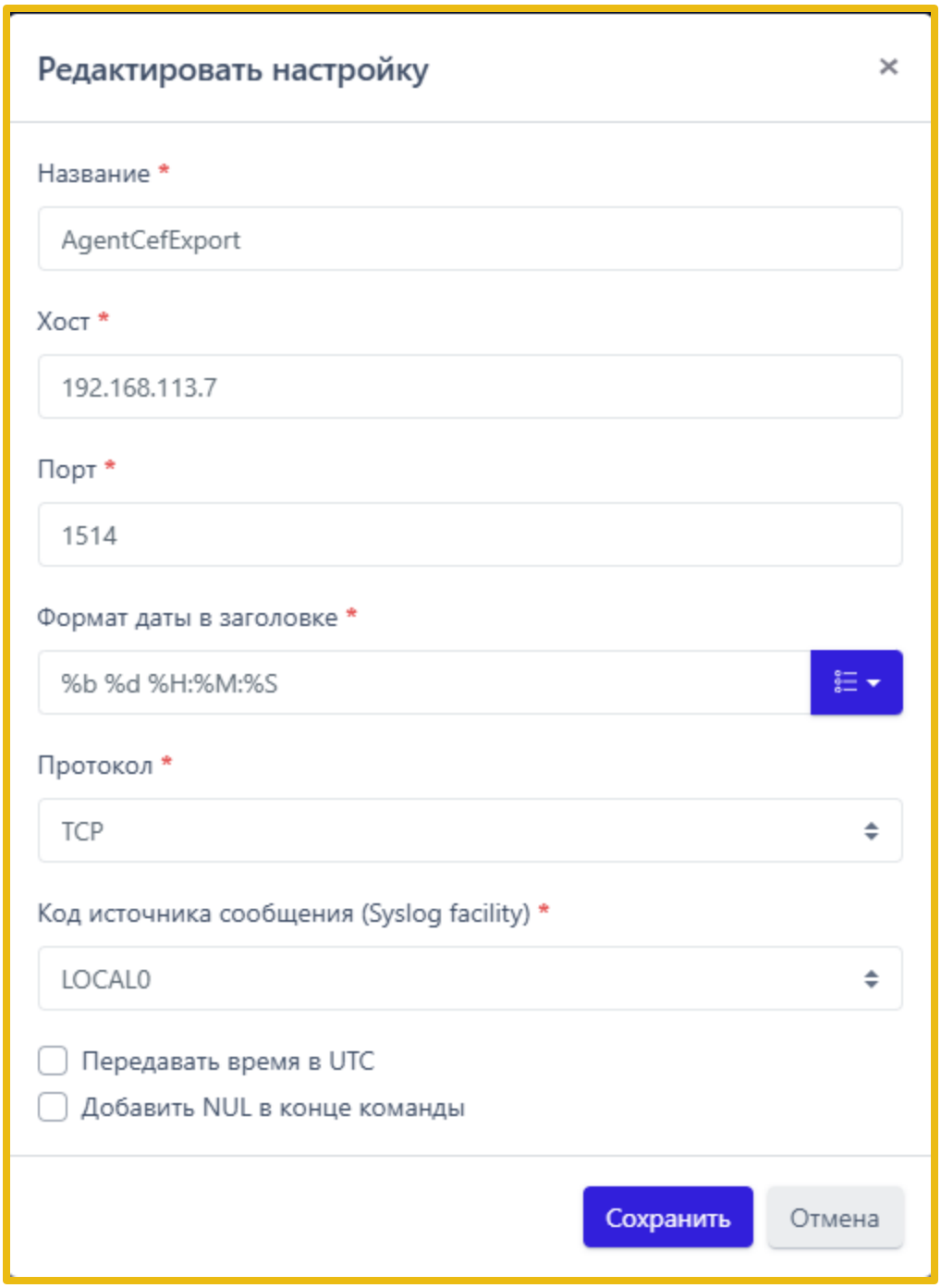


Рисунок 129 – Окно редактирования настроек интеграции с TI

После редактирования настроек следует нажать по иконке **Сохранить**.

В области **Интеграция с SIEM** для перехода на страницу со списком профилей с настройками следует нажать по иконке Настройки.

Страница со списками профилей настроек представлена на рисунке 130.

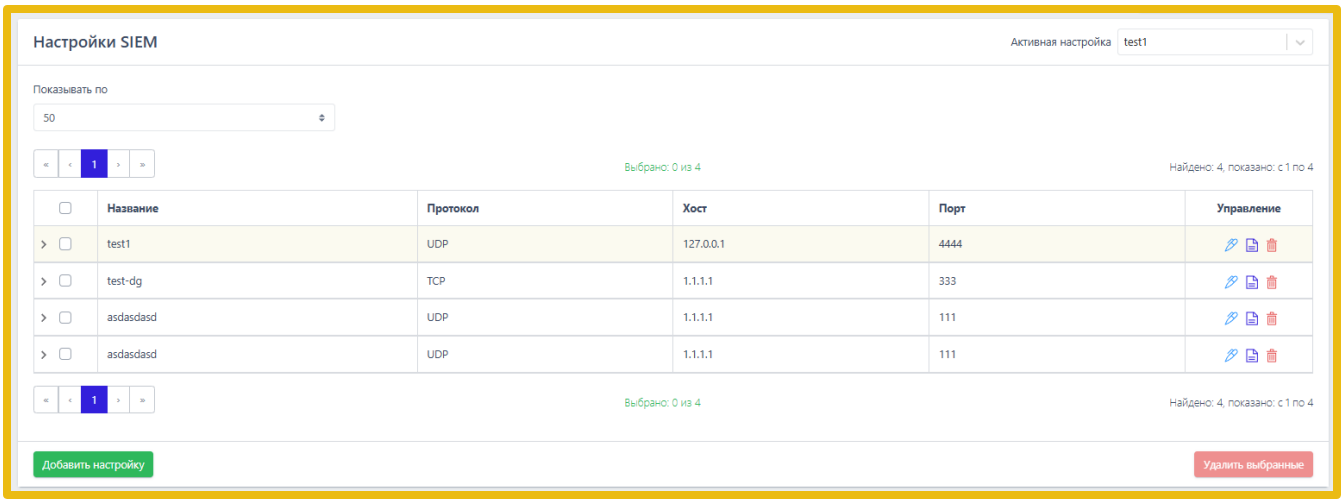


Рисунок 130 – Список профилей с настройками интеграции с SIEM

Информация на данной странице представлена в виде таблицы со следующими областями:

– кнопка выбора;

– иконка, раскрывающая информацию по параметрам настройки (❯);

– название профиля настройки;

– протокол;

– хост;

– порт;

– управление (редактирование настройки ( ), редактирование файла конфигурации экспорта событий ( ), удаление настройки ( )).

Выбор активной настройки осуществляется администратором в строке **Активная настройка** (Активная настройка active-config).

На странице можно добавить настройку, нажав по иконке Добавить настройку (рис. 131).

Параметры для заполнения при добавлении новой настройки аналогичны параметрам, указанным в окне редактирования настройки.

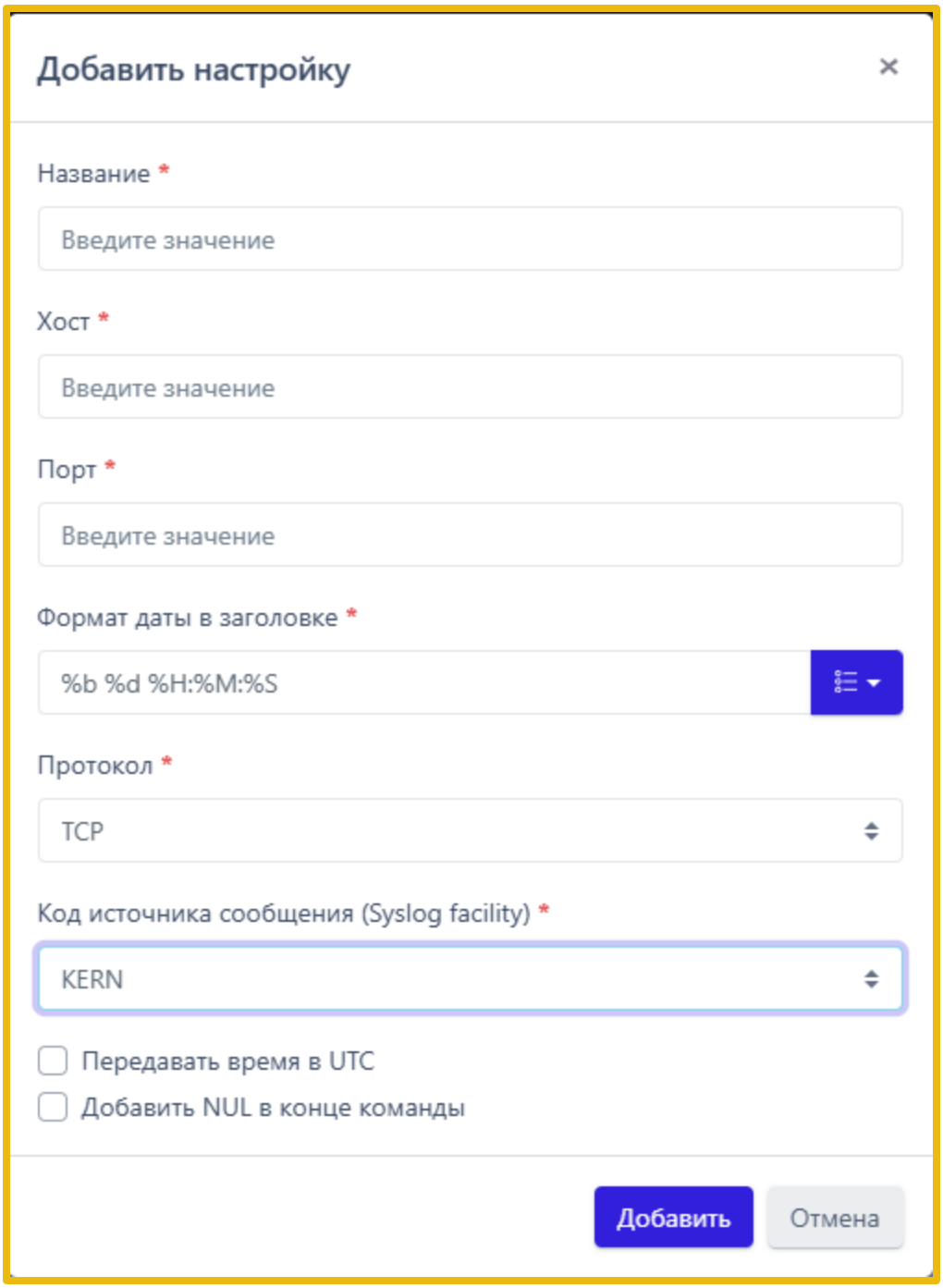


Рисунок 131 – Окно добавления настройки интеграции между TI-платформой и EDR

Название – в поле указывается название настройки интеграции.

Хост – в поле указывается имя хоста SIEM-системы (домен).

Порт – в поле указывается порт для соединения между EDR и SIEM (обычно 514).

Формат даты в заголовке – устанавливает различные форматы дат для заголовка, можно выбрать из нескольких шаблонов (кнопка ).

Протокол – можно выбрать один из представленных в списке протоколов (TCP или UDP).

Код источника сообщения (Syslog facility) – Facility — это один из стандартных параметров протокола syslog (RFC 3164/5424). Он указывает, какая часть системы или какой тип приложения сгенерировал лог-сообщение. В SIEM-системах facility используется для:

1) Фильтрации и маршрутизации событий (например, все сообщения от DAEMON направить в отдельный поток).

2) Нормализации — чтобы понимать, к какой категории относится событие, даже если текст сообщения не содержит явной метки.

3) Приоритизации — некоторые facility по умолчанию считаются более важными, например, KERN.

Опции передачи времени в UTC и добавления NUL в конце команды (опция предназначена для обхода проблемы парсинга многострочных сообщений в реализации протокола Syslog TCP).

После добавления настройки необходимо в поле **Управление** отредактировать файл конфигурации экспорта событий ( ). Файл конфигурации экспорта событий или CEF-файл – это файл в текстовом формате для обмена данными о событиях.

Для понимания, как редактировать CEF-файл, разберем примерную конфигурацию (рис. 132):



```
{
    "cef": {
        "version": 0,
        "device": {
            "vendor": "RT-IB",
            "product": "EDR",
            "version": "1.0"
        },
        "severity": {
            "NORMAL": 1,
            "GUARDED": 3,
            "ELEVATED": 6,
            "HIGH": 8,
            "SEVERE": 10
        }
    },
    "query": {
        "bool": {
            "filter": [
                { "terms":  { "t": [0, 1, 2] }},
                { "terms": { "svrt": [3, 4]}}
            ],
            "must": [
                { "query_string": {
                    "query": "sha256:*",
                    "default_operator": "AND"
                }}
            ]
        }
    },
    "mapping": {
        "default": {
            "app": "filePath"
        },
        "process": {
            "app": "cs2"
        }
    }
}
```

Рисунок 132 – Пример конфигурации CEF-файла

Конфигурация определяет следующие настройки:

1) Обязательные параметры заголовка CEF;

2) Сопоставление уровней критичности (severity);

3) Фильтрацию событий в Elasticsearch;

4) Маппинг полей внутренней модели событий в модель CEF (под маппингом полей подразумевается процесс установления соответствия между полями модели данных из EDR и полями CEF-модели).

Примечание

Подробное описание полей модели данных RT Protect EDR содержится в разделе 9.

Ознакомиться со стандартом CEF, списком полей и их обозначением можно по следующей ссылке:

https://1275.ru/wp-content/uploads/2024/12/cef-implementation-standard-27.pdf

1. Блок cef.

Блок cef содержит параметры, необходимые для формирования обязательной части CEF-заголовка (рис. 133).

```
"cef": {
    "version": 0,
    "device": {
        "vendor": "RT-IB",
        "product": "EDR",
        "version": "1.0"
    },
    "severity": {
        "NORMAL": 1,
        "GUARDED": 3,
        "ELEVATED": 6,
        "HIGH": 8,
        "SEVERE": 10
    }
}
```

Рисунок 133 – Обязательная часть CEF-заголовка

version – версия формата CEF, обычно используется значение 0 (актуальная версия формата), формат заголовка – CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|.

device – описывает источник события в виде:

1) vendor – производитель решения;

2) product – название продукта;

3) version – версия продукта.

severity – маппинг уровней критичности из внутренней модели событий в шкалу CEF (от 0 до 10):

1) Normal (Информация) – 1;

2) Guarded (Низкая) – 3

3) Elevated (Средняя) – 6;

4) High (Высокая) – 8;

5) Severe (Критичная) – 10.

Маппинг позволяет привести внутреннюю модель критичности к стандартной шкале CEF (во внутренней модели существует только 5 уровней критичности, представленные в списке выше), что в свою очередь позволяет внешним SIEM-системам корректно обрабатывать события.

2. Блок query.

Блок описывает запрос к Elasticsearch, по которому отбираются события для экспорта в SIEM:

```
"query": {
    "bool": {
        "filter": [
            { "terms":  { "t": [0, 1, 2] }},
            { "terms": { "svrt": [3, 4]}}
        ],
        "must": [
            { "query_string": {
                "query": "sha256:*",
                "default_operator": "AND"
            }}
        ]
    }
}
```

Рисунок 134 – Пример написания блока query

Блок позволяет определить критерии выборки событий, экспортировать только релевантные события. Блок использует синтаксис Elasticsearch Query DSL. В приведенном выше примере **filter** – фильтрация по типам событий (**t**) и уровням критичности (**svrt**); **must** – обязательное условие наличия поля **sha256**.

3. Блок mapping.

Блок mapping определяет сопоставление полей внутренней модели EDR-событий полям CEF. Общая структура представлена на рисунке 135.



Рисунок 135 – Общая структура блока mapping

default – базовый маппинг, применяемый ко всем событиям, формат базового маппинга – "поле_внутренней_модели":"поле_CEF", например, "app":"filePath", это означает, что внутреннее поле **app** (полное имя исполняемого файла процесса) будет записано в CEF-поле **filePath.** Если событие имеет конкретный тип (например, **process**), используется соответствующий блок маппинга. Он перекрывает значения из default-маппинга только для указанных полей. Правила приоритета – сначала применяется default, если же для типа события определен отдельный блок, то его значения являются более приоритетными, но только для указанных полей, а остальные поля берутся из default-маппинга. Доступные значения типов событий представлены в таблице 63.

Таблица 63 – Наименования событий

Тип события	Обозначение
network	Сеть
filesystem	Файлы
registry	Реестр
etw	Журналы
process	Процессы
system	Система
session	Сессии
calls	Вызовы
antiransomware	Антишифр
usb	Контроль USB

11.30.5. Экспорт событий безопасности

Экспорт через Webhook – современный, легковесный метод доставки событий безопасности в SIEM. При настройке важно корректно задать тайм-аут, SSL-политику и дату начала, чтобы избежать потерь или дублирования событий.

Для корректной работы экспорта необходимо добавить настройку экспорта событий безопасности. После нажатия кнопки **Настройки** откроется страница **Экспорт событий безопасности**, на которой необходимо нажать кнопку **Добавить настройку**. После этого откроется окно **Добавить настройку**, в котором необходимо добавить обязательные настройки (рис. 136).

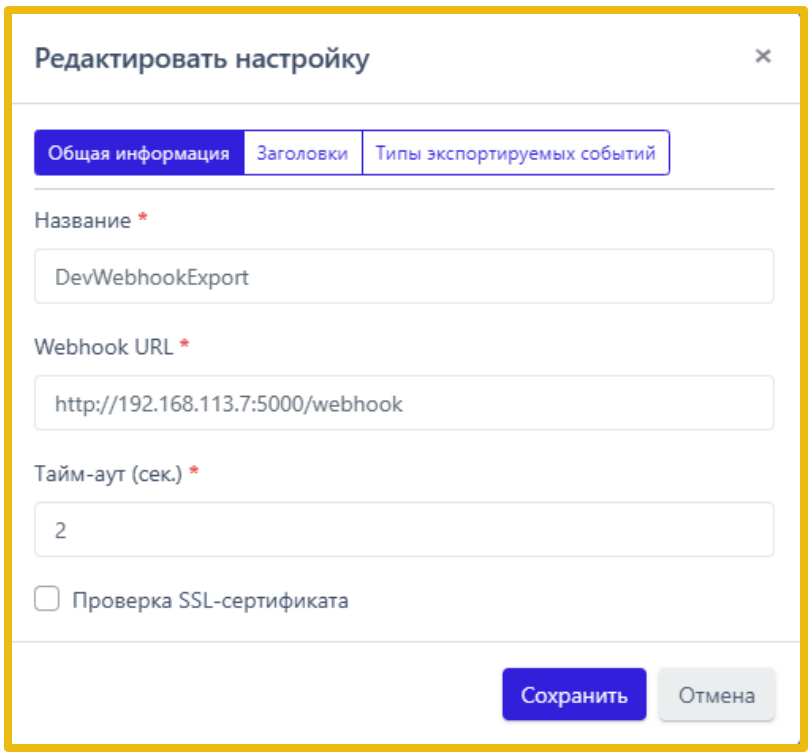


Рисунок 136 – Настройки экспорта событий безопасности

Название – в строке прописывается произвольное название интеграции между EDR и SIEM.

Webhook URL – в строке прописывается конечная точка со стороны SIEM, которая принимает HTTP-запросы от EDR-сервера.

Тайм-аут – временной период, в течение которого должна выполняться отправка событий безопасности.

Дата начала обработки событий – время, с которого будут передаваться события.

Флаг **Проверка SSL-сертификата** – проверяется валидность сертификата SIEM, если флаг установлен.

Для интеграции с SIEM также необходимо настроить заголовки.

Заголовки — это метаданные, которые передаются вместе с HTTP-запросом от EDR к SIEM. Они располагаются в начале HTTP-сообщения до тела (payload) и содержат служебную информацию о запросе: формат данных, способ кодировки, аутентификацию, тип соединения и др. Без заголовков SIEM не сможет правильно интерпретировать пришедшие события. Заголовки решают следующие задачи:

1) Идентификация формата данных – SIEM должен знать, как парсить тело запроса (JSON, XML, plain text);

2) Аутентификация и авторизация – подтверждение, что запрос действительно от легитимного источника;

3) Управление соединением – контроль таймаутов, сжатия, кэширования;

4) Отладка и трассировка – уникальные идентификаторы запросов для поиска проблем.

Основные заголовки, используемые при экспорте событий в SIEM представлены в таблице 64.

Таблица 64 – Примеры заголовков

Заголовок	Пример значения	Назначение
Content-Type	application/json	Указывает формат тела запроса. SIEM ожидает JSON – будет парсить как JSON; если text/plain – обработает как строку.
Authorization	Bearer eyJhbGci… или Basic dXNlcjpwYXNz	Передаёт учётные данные или токен для доступа к webhook URL. Без него SIEM может отклонить запрос.
User-Agent	SecurityAudit/1.0	Идентифицирует программное обеспечение источника (удобно для логирования и фильтрации).
X-Event-ID	a1b2-c3d4-5678	Уникальный идентификатор события, чтобы SIEM мог обнаружить дубликаты.
X-Timestamp	2026-04-30T12:34:56Z	Временная метка события на источнике (если не включена в тело).
X-Forwarded-For	10.0.0.5	Оригинальный IP-адрес, если запрос идёт через прокси.
Content-Encoding	gzip	Если тело сжато (например, для уменьшения трафика).
Accept	application/json	Что ожидает источник в ответе от SIEM (не всегда используется).
Connection	keep-alive	Указывает, переиспользовать ли TCP-соединение для нескольких событий.

Редактирование настройки вкладки «Типы экспортируемых событий» представлено на рисунке 137.

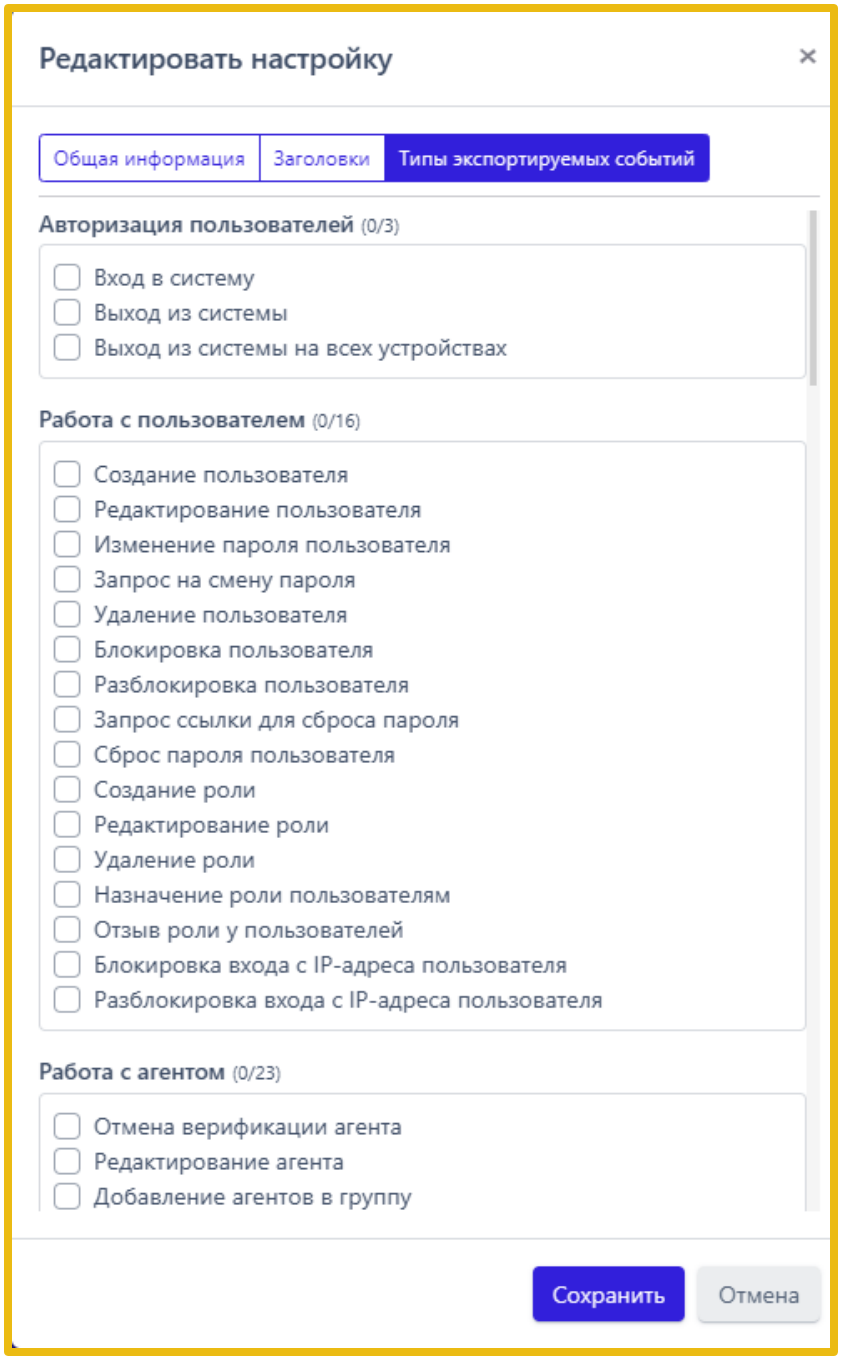


Рисунок 137 – Редактирование настроек экспорта событий, вкладка «Типы экспортируемых событий»

После добавления и сохранения настроек после заполнения формы необходимо нажать кнопку **Добавить**.

11.31 Настройки

В разделе отображаются настройки Elasticsearch. В контексте RT Protect EDR Elasticsearch – это платформа для поиска и анализа событий, отправляемых с агентов серверу.

На странице **Настройки** отображаются следующие характеристики Elasticsearch:

1) Состояние БД;
2) Период хранения данных БД в днях;
3) Количество свободной памяти в кластере БД в процентах;
4) Количество свободного места на дисках в кластере БД.

БД может принимать следующие состояния:

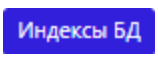
1) Все данные доступны;
2) Имеются нераспределенные реплики/шарды;
3) Часть данных недоступна.

Состояние **Все данные доступны** означает, что кластер Elasticsearch находится в идеальном рабочем состоянии и может гарантировать полную целостность и доступность данных (все шарды активны и распределены, кластер в зеленом состоянии, данные доступны для всех операций). Кластер представляет собой одну или несколько нод (серверов), объединенных в одно целое. Нода – это один экземпляр Elasticsearch (часть кластера). Шарды – это неделимые части индекса, основные единицы хранения данных в Elasticsearch. Они служат для горизонтального масштабирования и повышения производительности. Реплики – это точные копии первичных шардов.

Они обеспечивают отказоустойчивость и повышают производительность чтения данных.

Состояние **Имеются нераспределенные реплики/шарды** говорит о том, что в кластере Elasticsearch есть шарды или реплики, которые не могут быть размещены на каких-либо узлах в соответствии с политикой распределения кластера.

Состояние **Часть данных недоступна** говорит о том, что часть шардов недоступна, а соответствующие данные потеряны и поиск с записью для этих данных невозможны.

Нажатие кнопки 

открывает одноименную страницу, на которой можно просмотреть информацию об индексах и их состояниях. Индекс можно фильтровать по состоянию и статусу (закрыт, активен).

12. Машинное обучение в Программе

12.1 Классификация на сервере

В RT Protect EDR реализован статический анализ инцидентов на основе ИИ. Модель состоит из encoder-трансформера на основе RoBERTa и полносвязной нейронной сети, на вход которой поступают исходные данные инцидентов информационной безопасности (рис. 138). Данная архитектура модели выбрана в связи с большим количеством текстовых признаков, присущих инцидентам. Модель представляет собой отдельный модуль, взаимодействие с которым происходит с помощью API-вызовов. Входным параметром данного модуля является текст, содержащий в себе один или несколько JSON-объектов. Дальнейшие преобразования включают в себя проверку на валидность переданных объектов, нормализацию JSON, агрегацию нескольких JSON в один (в случае, если на вход модуля поступило несколько связанных объектов), фильтрацию полей и приведение их названий к общему виду, а также обогащение с помощью RT Protect TI и дополнительной информации из источника данных Elastic, не вошедшей в исходные JSON-объекты. К признакам, используемым для работы модели машинного обучения, относятся: сработавшее правило, название организации, имя пользователя, командная строка процесса (а также родительского и прародительского процессов), имя модуля-инициатора, путь к модулю-инициатору, путь к запущенному приложению, результаты проверок индикаторов компрометации (sha256, md5, IP-адреса, домены, url), информация о локальном/удалённом хосте, IP-адреса задействованных хостов, описание данных хостов, изменения реестра Windows. Все перечисленные значения опциональны, что позволяет классифицировать различные инциденты информационной безопасности, которые из-за своей специфики могут иметь лишь те или иные признаки.

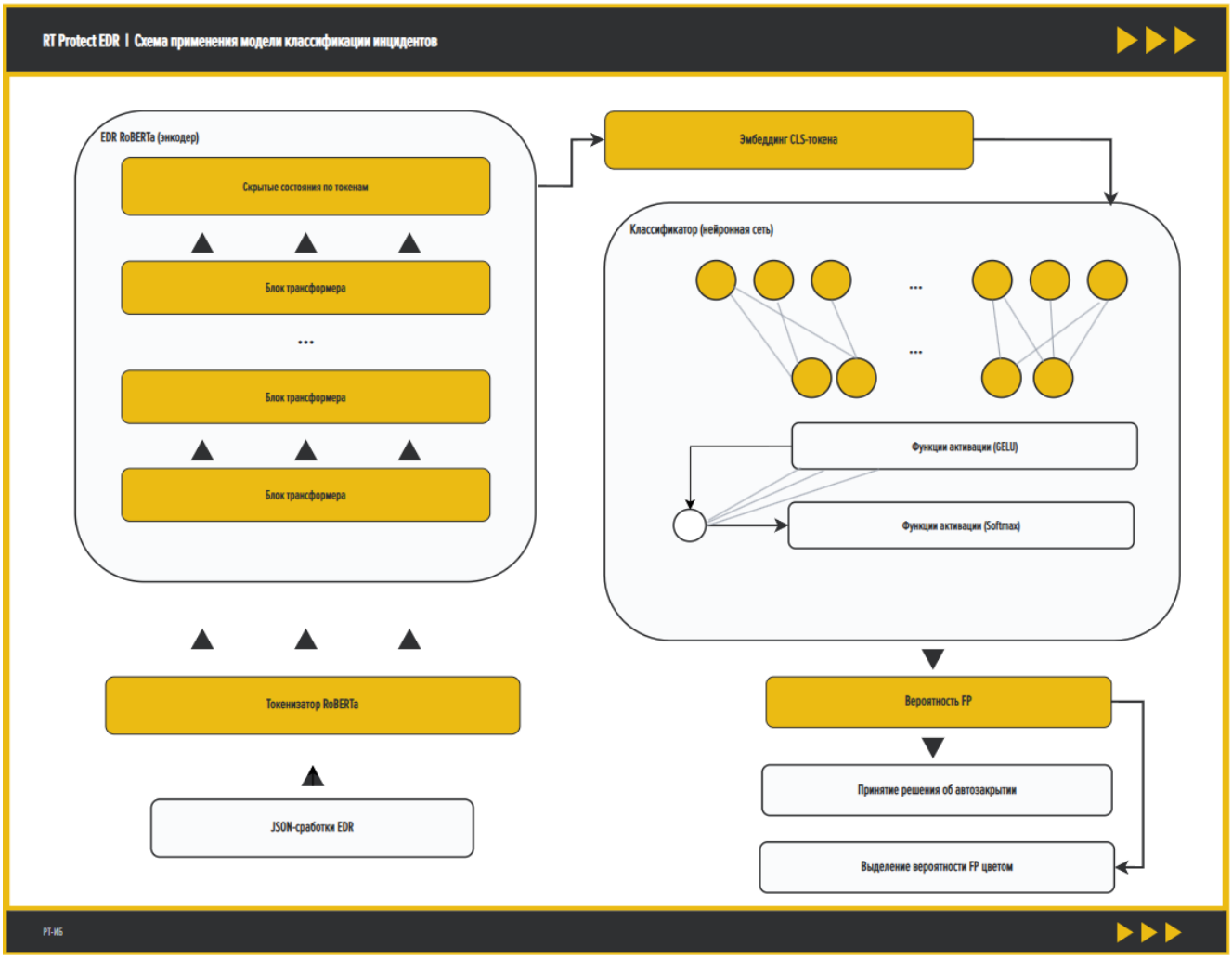


Рисунок 138 – Схема применения модели классификации инцидентов

После данного этапа происходит классификация инцидента. В качестве результата выдается значение в диапазоне [0;1], соответствующее вероятности того, что инцидент является ложноположительным срабатыванием, а также идентификатор autoClose, определяющий, можно ли автоматически закрыть данный инцидент. Модель содержит в себе несколько порогов срабатывания, которые уточняются при переобучении модели. Первая группа порогов содержит один порог (приблизительно от 0.9 до 0.95), который говорит о том, что инцидент является ложным срабатыванием правила и должен быть автозакрыт. Второй тип порогов (примерно 0.3, 0.5 и 0.7) используется для сопоставления инциденту цветовой метки («Красный», «Оранжевый», «Жёлтый» или «Зелёный»), отражающей серьёзность инцидента. Вердикт модели передается как ответ API-вызова, который обрабатывается SOAR-системой для автоматического закрытия инцидента или добавления цветовой метки, использующейся для составления приоритета обработки инцидентов аналитиками первой линии.

Сама модель представляет собой конфигурационные файлы в формате safetensors и json, которые содержит в себе веса признаков модели, словарь токенизатора модели, а также пороговые значения вынесения вердиктов автозакрытия и соответствия цветовым меткам. Эти файлы формируются в результате обучения модели в тестовой лаборатории в автоматическом режиме с помощью Airflow, что позволяет модели оставаться актуальной с течением времени.

Обучение модели производится на языке python с использованием библиотек scikit-learn, pytorch и transformers. В качестве обучающих выборок используются собственные наборы данных. Первый из них это набор данных для обучения без учителя, используемый для получения качественного численного представления посредством моделей, основанных на BERT-архитектуре, а второй уже является набором данных для обучения с учителем RoBERTa-подходом с целью оптимизации классификатора над признаками, полученными из BERT-модели.

12.2 Классификация на агенте

В RT Protect EDR реализован статический анализ исполняемых файлов на основе ИИ. В частности, применяется модель логистической регрессии, на вход которой поступают статические признаки исполняемых файлов. Данный тип модели выбран ввиду ее быстродействия и минимальных требований к вычислительным ресурсам, поскольку она работает в синхронном режиме на агентских компьютерах.

Далее будет описана схема применения модели классификации ПО, применяемая в агенте RT Protect EDR (рис. 139).

Для отслеживания запуска файлов на исполнение драйвер агента в обработчике открытия файлов анализирует флаги открытия файла.

При наличии запрашиваемого доступа «на исполнение» (FILE_EXECUTE), модуль минифильтра драйвера открывает секцию файла (для его последующего чтения в службе) и передает задачу на анализ файла службе агента посредством специального порта взаимодействия (CommunicationPort). Служба, получив задание на анализ файла, передает управление в модуль сбора признаков исполняемого файла. К признакам, необходимым для модели машинного обучения, относятся: физический и виртуальный размер файла (в байтах), флаги из заголовков исполняемого файла (PE-headers), наличие оверлея, имя секции, содержащей

точку входа программы, энтропия файла, количество url-строк, количество строк-путей, количество сигнатур ‘MZ’, количество экспортируемых и импортируемых функций, имена секций и др.

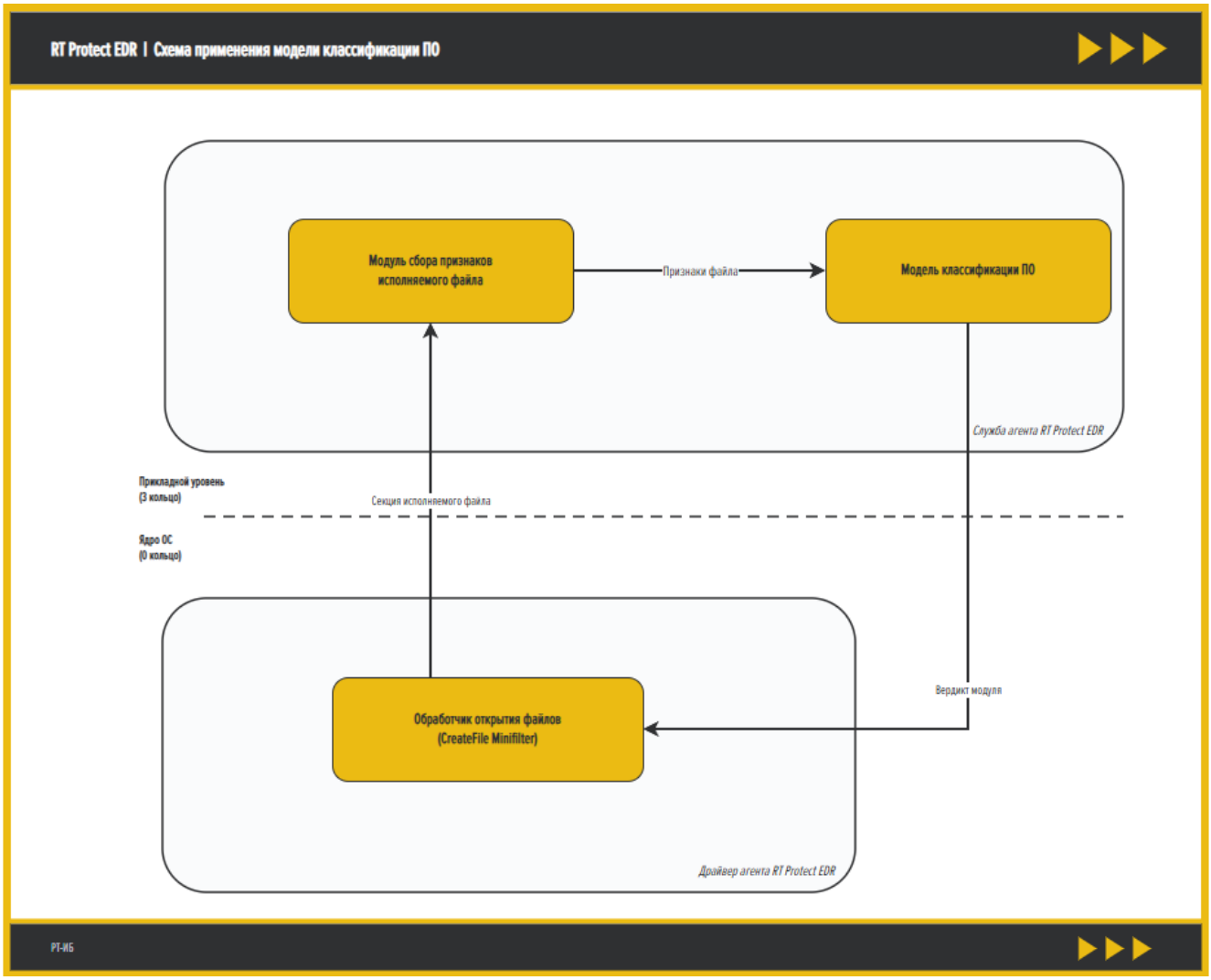


Рисунок 139 – Схема применения модели классификации ПО

После сбора перечисленных признаков вызывается функция классификации файла. На вход она принимает собранные признаки. В качестве результата выдает значение в диапазоне [0;1], соответствующее вероятности того, что файл является вредоносным. Модель содержит в себе 2 порога срабатывания, которые уточняются от версии к версии модели. Первый более низкий порог (приблизительно от 0.8 до 0.9) говорит о том, что файл подозрительный, второй (ближе к 1) – файл вредоносный. Вердикт модели передается обратно в драйвер, который на его основе выполняет предписываемые действия: пропустить, отправить предупреждение (alert) или заблокировать запуск файла с уведомлением.

Сама модель представляет собой конфигурационный файл в формате json, который содержит в себе веса признаков, а также пороговые значения вынесения вердикта. Этот файл формируется в результате обучения модели в тестовой лаборатории, а затем загружается на сервер EDR. В свою очередь сервер EDR рассылает конфигурационный файл модели по агентам.

Обучение модели производится на языке python с использованием библиотеки scikit-learn. В качестве обучающих выборок используются наборы: sophos/SOREL-20M (https://github.com/sophos/SOREL-20M), bodmas (https://github.com/whyisyoung/BODMAS), Malware Dataset IDN (https://ieee-dataport.org/documents/malware-dataset-idn), а также собственный набор файлов, собранных в тестовой лаборатории.

12.3 Список компонентов, используемых в модели ИИ

Полный список сторонних компонентов, используемых в модели машинного обучения, приведен в таблице 65.

Таблица 65 – Сторонние компоненты

№ п/п	Наименование стороннего компонента	Правообладатель	Сведения о документах, подтверждающих наличие оснований на использование компонента	Лицензии	Вид лицензии
	scikit-learn	The scikit-learn developers	https://github.com/scikit-learn/scikit-learn?tab=BSD-3-Clause-1-ov-file#readme	BSD 3-Clause	Свободная лицензия
	pytorch	Facebook, Inc, Idiap Research Institute, Deepmind Technologies, NEC Laboratories America, NYU	https://github.com/pytorch/pytorch/blob/main/LICENSE	BSD-Style	Свободная лицензия
	pandas	AQR Capital Management, LLC, Lambda Foundry, Inc. and PyData Development Team, Open source contributors	https://github.com/pandas-dev/pandas/blob/main/LICENSE	BSD 3-Clause	Свободная лицензия
	numpy	NumPy Developers	https://github.com/numpy/numpy/blob/main/LICENSE.txt	numpy	Свободная лицензия

№ п/п	Наименование стороннего компонента	Правообладатель	Сведения о документах, подтверждающих наличие оснований на использование компонента	Лицензии	Вид лицензии
	transformers	The Hugging Face team	https://github.com/huggingface/transformers/blob/main/LICENSE	Apache License 2.0	Свободная лицензия
	fastapi	Sebastián Ramírez	https://github.com/fastapi/fastapi/blob/master/LICENSE	MIT	Свободная лицензия
	uvicorn	Encode OSS Ltd.	https://github.com/encode/uvicorn?tab=BSD-3-Clause-1-ov-file	BSD 3-Clause	Свободная лицензия
	joblib	The joblib developers	https://github.com/joblib/joblib/blob/main/LICENSE.txt	BSD 3-Clause	Свободная лицензия

13. Создание аналитики на основе MITRE CAR

13.1 Общая информация

Реестр методов обнаружения угроз в сфере кибербезопасности (CAR) MITRE – это база знаний с аналитикой, основанной на модели угроз MITRE ATT&CK.

Данные модели CAR записаны псевдокодом, но могут также включать другие реализации.

Представленная в CAR аналитика содержит следующую информацию:

1) Гипотезу, которая описывает идею аналитического решения;

2) Информационную область, для которой метод обнаружения угрозы был разработан;

3) Ссылки на тактики и техники ATT&CK, которые обнаруживает аналитика;

4) Словарь терминов;

5) Описание на псевдокоде алгоритма того, как аналитический метод может быть внедрен в реальных условиях;

6) Модульный тест, с помощью которого может проверяться аналитическое решение.

Вместе с аналитическими методами обнаружения угроз CAR содержит модель данных для запуска аналитики и сенсоры, которые используются для сбора этих данных.

Интерпретируя псевдокод, можно создавать индикаторы атак в RT Protect EDR. Для этого необходимо, следуя описанию аналитического метода обнаружения угроз и алгоритму, прописанному в шагах псевдокода, записать его в виде индикатора атак в разделе **Индикаторы атак**.

13.2 Пример написания индикатора атаки

Рассмотрим пример с написанием правила для метода обнаружения угроз CAR-2020-11-009: **Доступ к скомпилированному HTML**.

В описании к методу указано, что злоумышленники могут прятать вредоносный код в файлах .chm, когда эти файлы читаются, Windows использует утилиту hh.exe. Запуск утилиты необходимо обнаруживать с помощью индикатора атаки.

В качестве имени индикатора необходимо прописать произвольное значение, например, **RT_win_hh**.

В строке **Критичность** указать низкий уровень критичности.

В строке **Тип индикатора** в качестве типа индикатора атаки необходимо указать **Процессы: старт процесса**.

В строке **Действие** указать значение **детектировать**, а в качестве идентификатора в строке **MITRE «T1218\001»**. Далее выбрать один из режимов обнаружения ИА (обычный, без генерации обнаружения или с однократной генерацией обнаружения).

В поле **Описание** и **Комментарий** можно добавить соответствующие записи для разъяснения созданного правила.

В строке **Условие** необходимо написать, что должно обнаруживаться событие создания процесса hh.exe. В RT Protect EDR лучше всего это сделать с помощью флагов исполняемого файла процесса (exclf).

После описания условий можно проверить его с помощью проверки синтаксиса (кнопка </>), после чего необходимо сохранить правило, нажав кнопку **Добавить** (рис. 140). После сохранения правила в нижней части страницы появится всплывающее окно с сообщением о том, что правило добавлено.

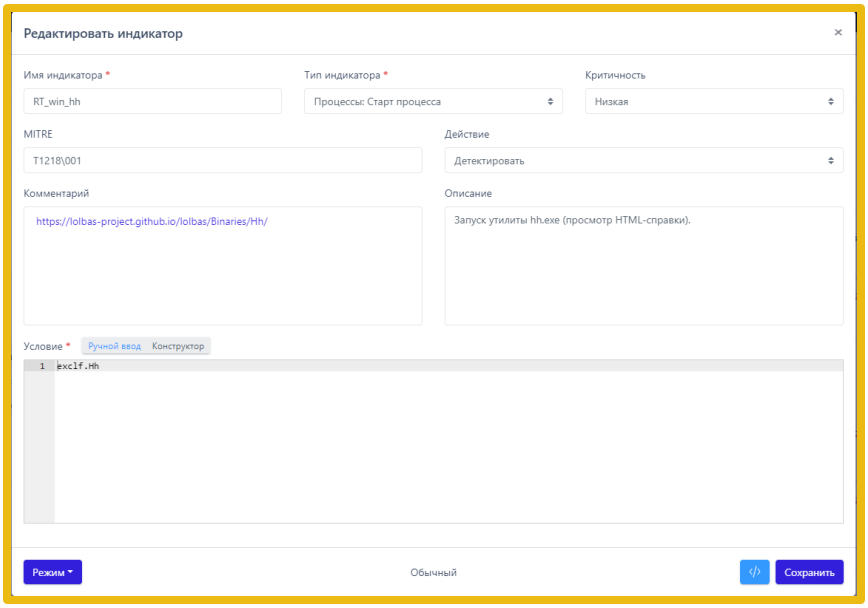


Рисунок 140 – Правило, обнаруживающее запуск hh.exe

После закрытия окна **Добавить индикатор** на странице **Индикаторы атак** появится новая строка с созданным правилом. Для применения правила в наборе необходимо нажать кнопку  внизу страницы.

После сохранения правила следует назначить набор с этим правилом для агентов, на которых будет детектироваться активность, описанная в наборе. Для этого необходимо перейти в раздел **Агенты** и выбрать в списке нужных агентов. Далее нажать кнопку  , откроется окно **Выбор набора**, после чего в строке **Индикаторы атак** выбрать из выпадающего списка набор с правилом **RT_win_hh** и нажать кнопку **Сохранить**.

После обновления аналитических наборов на соответствующих агентах любой запуск утилиты hh.exe на конечных точках с агентами приведет к обнаружению этого события Программой и созданию соответствующей записи на странице **Активность**. Так как в нашем случае указан уровень критичности **Низкая**, то создаваться инцидент не будет (инциденты создаются для событий с уровнем критичности **Средняя** или выше).

14. Перечень сокращений

Аббревиатура	Расшифровка
ГОСТ	Государственный стандарт
ИА	Индикаторы атак
ИК	Индикаторы компрометации
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Средство обнаружения вторжений
ФСТЭК	Федеральная служба по техническому и экспортному контролю
APT	Advanced Persistent Threat
ASCII	American Standard Code for Information Interchange
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
C2 (C&C)	Command and Control
CAR	Cyber Analytics Repository
DLL	Dynamic Link Library
DNS	Domain Name System
DSL	Domain-specific language
EDR	Endpoint Detection & Response
ETW	Event Tracing for Windows
FTP	File Transfer Protocol
HEX	Hexadecimal
HTTP	HyperText Transfer Protocol
IOA	Indicator of Attack
IOC	Indicator of Compromise
JSON	JavaScript Object Notation
ML	Machine Learning
NTFS	New Technology File System
PE	Portable Executable
RAT	Remote Access Trojan
RPC	Remote Procedure Call
SHA-256	Secure Hash Algorithm
SOC	Security Operations Center
SSL	Secure Sockets Layer
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TLSH	Trend Locality Sensitive Hash
TTP	Tactics, Techniques, and Procedures
UAC	User Account Control

Аббревиатура	Расшифровка
UUID	Universally Unique Identifier
WMI	Windows Management Instrumentation

15. Перечень терминов и определений

Термин	Расшифровка термина
Аналитик безопасности	Человек, который занимается анализом информационных рисков компании, разрабатывает и внедряет мероприятия по их предотвращению. В его обязанности также может входить установка, настройка и сопровождение технических средств по защите данных.
Брандмауэр	Технологический барьер, предназначенный для предотвращения несанкционированного или нежелательного сообщения между компьютерными сетями или хостами.
Дамп памяти	Содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы, например, значения регистров процессора и содержимое стека.
Диспетчер служб	Особый системный процесс, реализующий технологию удалённого вызова процедур (RPC). Обеспечивает создание, удаление, запуск и остановку служб ОС. Стартует при загрузке системы, обеспечивает работу журнала событий, а также позволяет выполнять манипуляцию процессами удалённой машины.
Именованный канал	Именованный односторонний или дуплексный канал для обмена данными между сервером канала и одним или несколькими клиентами канала. Все экземпляры именованного канала имеют одно и то же имя канала, но каждый экземпляр имеет собственные буферы и дескрипторы и предоставляет отдельный канал для обмена данными между клиентом и сервером. Использование экземпляров позволяет нескольким клиентам канала одновременно использовать один и тот же именованный канал.
Исполняемый модуль процесса	Набор инструкций, загружаемый в виде исполняемого файла или dll в процесс.
Корреляция событий	Метод для понимания большого количества событий и выявления немногих событий, которые действительно важны в этой массе информации.
Красная команда	Группа лиц, которая выполняет комплексную имитацию реальных атак с целью оценки кибербезопасности атакуемых систем.
Матчинг	Метод анализа и обработки структур данных в языках программирования, основанный на выполнении определённых инструкций в зависимости от совпадения исследуемого значения с тем или иным образцом, в качестве которого может использоваться константа, предикат, тип данных или иная поддерживаемая языком конструкция.
Нити (Threads)	Еще может переводиться как поток, но в терминологии RT Protect EDR встречается чаще всего как нить. Основная единица, которой операционная система выделяет время процессора. Каждая нить имеет приоритет планирования и набор структур, в которых система сохраняет контекст нити, когда ее выполнение приостановлено. Контекст нити содержит все сведения, позволяющие ей безболезненно возобновить выполнение, в том числе набор регистров процессора и стек нити. В контексте процесса может выполняться несколько нитей. Все нити процесса используют общий диапазон виртуальных адресов. Нить может исполнять любую часть программного кода, включая части, выполняемые в данный момент другой нитью.

Термин	Расшифровка термина
Образ	Исполняемый файл, библиотека DLL или драйвер, загруженный Windows в рамках процесса пользовательского режима или ядра.
Оверлей	Метод программирования, позволяющий создавать программы, требующие меньше оперативной памяти. Метод заключается в разделении программы на исполняемые блоки, которые поочерёдно записываются в одну область памяти поверх предыдущих, выполняют свои функции и перезаписываются следующими.
Поведенческий анализ	Механизм, построенный на технологии принятия решения о предоставлении доступа на основе анализа характера выполняемых объектом или программой действий.
Провайдер ETW	Любой компонент, который использует Event Tracing API. Это могут быть как классические провайдеры, созданные до Windows Vista и применяющие MOF-классы, так и провайдеры на основе манифестов, использующие новые интерфейсы, появившиеся в Windows Vista.
Проксирование	Перенаправление трафика.
Процесс	В простейших терминах – это исполняемая в операционной системе программа, активный объект ОС, а иначе, последовательность инструкций, исполняемых в ОС предопределенным образом. В данном случае такими инструкциями будет программный код. При этом программа будет называться процессом в том случае, если загружается в память вместе со всеми ресурсами, которые необходимы для ее работы.
Псевдокод	Компактный, зачастую неформальный язык описания алгоритмов, использующий ключевые слова императивных языков программирования, но опускающий несущественные для понимания алгоритма подробности и специфический синтаксис. Предназначен для представления алгоритма человеку, а не для компьютерной трансляции и последующего исполнения программы.
Ретроспективный анализ	Детальное исследование образов систем, журналов событий, дампов памяти и сетевого трафика за определенный промежуток времени в прошлом с целью выявить следы компрометации.
Синяя команда	Группа лиц, которая проводит анализ информационных систем для обеспечения безопасности, выявления недостатков безопасности, проверки эффективности каждой меры безопасности и обеспечения того, чтобы все меры безопасности продолжали действовать после реализации.
Телеметрия	Совокупность методов сбора информации и измерения параметров, позволяющих получить необходимые сведения об удаленных объектах.
Утилита mimikatz	Программное обеспечение, которое позволяет извлечь пароли пользователей непосредственно из памяти (путем инъекции в lsass.exe библиотеки sekurlsa.dll), из сохраненного дампа памяти компьютера или даже из файла гибернации (используемый в Windows файл для хранения данных и их последующей быстрой загрузки в оперативную память при включении компьютера или ноутбука).
Фишинг	Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.
Форензика	Прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. Форензика является подразделом криминалистики.

Термин	Расшифровка термина
Хеш-сумма	Уникальный идентификатор, который задаётся (автором программы или первым владельцем файла) с помощью «перемешивания» и шифрования содержимого файла по специальному алгоритму с последующей конвертацией результата в обычную строчку символов.
Хост	Любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети.
Эвристический анализ	Метод обнаружения вредоносных программ, при котором антивирусная программа контролирует все действия, выполняемые проверяемой программой. В ходе эвристического анализа отслеживаются потенциально опасные действия, характерные для вирусов и вредоносных программ других типов.
Эксплойт	Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой, так и нарушение её функционирования.
Эксфильтрация	Несанкционированное копирование, передача или получение данных с компьютера или сервера жертвы. Эксфильтрация может осуществляться через интернет или по локальной сети. Как правило, при передаче данных атакующие сжимают и шифруют их, чтобы избежать обнаружения.
Эмуляция	Комплекс программных, аппаратных средств или их сочетание, предназначенный для копирования (или эмулирования) функций одной вычислительной системы на другую, отличную от первой вычислительной системы, таким образом, чтобы эмулированное поведение как можно ближе соответствовало поведению оригинальной системы.
Advapi32.dll	Часть расширенной библиотеки служб API, поддерживающей множество API, в том числе вызовы безопасности и реестра.
AMSI	Компонент операционной системы Windows, который позволяет приложениям и службам взаимодействовать с антивирусным программным обеспечением для проверки содержимого, такого как скрипты и макросы, на наличие угроз. AMSI обеспечивает более глубокое сканирование, выходящее за рамки проверки файлов, и помогает защитить от вредоносных программ, которые скрываются в памяти или используют обфускацию, улучшая общую безопасность системы. Представлен в Windows, начиная с Windows 10.
Anti-Ransomware	Программное обеспечение, защищающее конечные точки от вирусов-шифровальщиков.
APT-атака	Целевая кибератака (таргетированная кибератака) – вид кибератаки, процесс которой контролируется вручную в реальном времени человеком, являющимся центром атаки. Целью данной атаки является хищение защищенной информации из информационной системы конкретной компании, организации или государственной службы.
ASCII	Название таблицы (кодировки, набора), в которой некоторым распространённым печатным и непечатным символам сопоставлены числовые коды. Таблица была разработана и стандартизирована в США, в 1963 году.

Термин	Расшифровка термина
ATT&CK	База знаний компании MITRE Corporation, содержащая описание тактик, приемов и методов, используемых киберпреступниками.
Base64	Стандарт кодирования двоичных данных при помощи только 64 символов ASCII.
BCDEdit	Программа командной строки Windows для управления хранилищами BCD (данных конфигурации загрузки)
C&C (C2)	Инфраструктура управления и контроля (C2), используемая злоумышленниками для управления зараженными устройствами и кражи конфиденциальных данных во время кибератаки.
CAR	Репозиторий аналитики информационной безопасности MITRE.
Cmd	Команда для запуска интерпретатора команд.
Cmd.exe	Интерпретатор командной строки для операционных систем OS/2, Windows CE и для семейства операционных систем, базирующихся на Windows NT.
CMSTP	Утилита командной строки Windows, которая позволяет устанавливать профили менеджера соединений.
Cobalt Strike	Программная платформа для сетевых атак, которая сочетает в себе социальную инженерию, инструменты несанкционированного доступа, обфускацию сетевых шаблонов, сложный механизм развертывания вредоносного кода и т.д.
Combase.dll	Библиотека динамической компоновки, являющаяся основой архитектуры COM для MS Windows. Библиотека содержит заголовки и функции для манипулирования объектами COM: «COM – это независимая от платформы, распределенная, объектно-ориентированная система для создания двоичных программных компонентов, которые могут взаимодействовать. COM является базовой технологией для технологий Microsoft OLE (составные документы) и ActiveX (компоненты с поддержкой Интернета)».
Comctl32.dll	Библиотека динамической компоновки, отвечающая за корректное отображение графических элементов при работе в Windows.
D3FEND	Каталог защитных методов кибербезопасности и их отношения к наступательным/противодействующим методам.
Desktop.ini	Файл конфигурации, который содержит данные настроек внешнего вида системной папки в ОС Microsoft Windows: значок, цвет текста, фоновый рисунок и т. д.
DiskShadow	Утилита командной строки Windows, которая предоставляет функциональные возможности службы теневого копирования томов (VSS).
DismHost	Процесс, который используется для обслуживания образа Windows и исправления различных ошибок, связанных с файлами образа Windows. Обычно он находится в C:\Windows\System32\dism или C:\Windows\SysWoW64\dism
DLL	Динамически подключаемая библиотека.
DNS	Служба имён доменов (механизм, используемый в сети Internet и устанавливающий соответствие между числовыми IP-адресами.
DSL	Предметный язык программирования, специализированный для конкретной области применения.

Термин	Расшифровка термина
Dwmapi.dll	Библиотека динамической компоновки, предоставляющая API-интерфейс диспетчера окон рабочего стола Microsoft (общий интерфейс диспетчера окон рабочего стола DWM), который представляет собой обычный файл и в основном используется в качестве API-интерфейса для эффектов рабочего стола (таких, как эффекты Aero).
EDR	Класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, и других устройствах.
ETW	Высокоэффективная масштабируемая система трассировки с минимальными затратами ресурсов, реализуемая в операционных системах Windows.
False positive	Ложноположительные срабатывания – неправильно обозначенные предупреждения системы безопасности, указывающие на наличие угрозы при ее реальном отсутствии. Эти события увеличивают шум для групп безопасности и могут включать ошибки программного обеспечения, плохо написанное программное обеспечение или нераспознанный сетевой трафик.
FsUtil	Утилита командной строки Windows, которая позволяет решать задачи, связанные с таблицей размещения файлов (FAT) и файловой системой NTFS.
FTP	Протокол передачи файлов по сети.
Gdi32.dll	Библиотека динамической компоновки, которая содержит функции для Windows GDI (интерфейс графического устройства). Эти функции помогают создавать простые двумерные объекты.
HEX	Позиционная система счисления по целочисленному основанию 16.
Hh	Утилита Windows, которая позволяет работать с HTML-справками.
HTTP	Протокол прикладного уровня передачи данных, изначально – в виде гипертекстовых документов в формате HTML, в настоящее время используется для передачи произвольных данных.
Icacls	Утилита командной строки Windows, которая позволяет управлять списками доступа (ACL) к каталогам и файлам.
Imm32.dll	Библиотека динамической компоновки, которая используется диспетчером методов ввода Microsoft Windows (IMM). IMM – это технология, используемая приложением для связи с редактором методов ввода (IME), который работает как служба. IME позволяет пользователям компьютеров вводить сложные символы, такие как иероглифы, с помощью стандартной клавиатуры.
Imphash	Хеш импортируемых библиотек, то есть всех импортируемых программой библиотек, прописанных в исполняемом файле Windows Portable Executable (PE).
Inhibit System Recovery	Техника атаки по методологии MITRE, которая предполагает отключение служб, отвечающих за восстановление операционной системы.
InstallUtil	Утилита командной строки Windows, которая позволяет работать с INF-файлами (файлы сведений об установке, то есть определяющие, какие файлы необходимы для установки программного обеспечения или обновления).
IOA	Индикаторы атак.
IOC	Индикаторы компрометации.
JSON	Текстовый формат обмена данными, основанный на JavaScript.

Термин	Расшифровка термина
Kerberos	Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы.
Keylogger	Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя – нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши.
Kernel32.dll	Динамически подключаемая библиотека, являющаяся ядром всех версий ОС Microsoft Windows. Она предоставляет приложениям многие базовые API Win32, такие как управление памятью, операции ввода-вывода, создание процессов и нитей, а также функции синхронизации.
Kernelbase.dll	Системная динамическая библиотека, которая необходима для связи других динамических библиотек Windows. Другими словами, KernelBase.dll позволяет многим программам использовать одни и те же опции. Яркий пример тому обращение разных приложений к тому же самому общему для всех них файлу принтера DLL при необходимости печати. Повреждение KernelBase.dll, а также отсутствие элемента в системе может привести к закрытию программ, при этом проблема сопровождается сообщениями об ошибке.
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux, включающих тот или иной набор утилит и программ проекта GNU.
Loopback	Программный метод, который направляет полученные данные обратно отправителю без специальной обработки или модификации.
Lpk.dll	Динамическая библиотека языковых пакетов. Применяется Windows и многими приложениями для управления языковым пакетом, используемым для диалогов и сообщений.
Lsass.exe	Служба проверки подлинности локальной системы безопасности. Процесс lsass проверяет данные для авторизации пользователей.
MD5	128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности.
MITRE (The MITRE Corporation)	Американская некоммерческая организация с двумя штаб-квартирами в Бедфорде, штат Массачусетс, и Маклине, штат Вирджиния. Сотрудники компании занимаются исследованиями и разработками в области обороны, здравоохранения, авиации, внутренней безопасности и кибербезопасности.
ML	Класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение за счёт применения решений множества сходных задач.
Mmc	Утилита, которая позволяет администрировать консоль управления Windows.
Msctf.dll	Библиотека динамической компоновки, которая позволяет сделать доступным TSF (Text Services Framework) для использования независимым вендором в приложениях третьих лиц. TSF – это среда COM и API в Windows XP и более поздних операционных системах Windows, которые поддерживают расширенный ввод и обработку текста.

Термин	Расшифровка термина
Msimg32.dll	Компонент расширения для Windows GDI, который содержит новые API для улучшения функциональности GDI32. Интерфейс графического устройства Microsoft Windows (GDI) позволяет приложениям использовать графический и отформатированный текст как на видео, так и на принтере. приложения на основе Windows напрямую не обращаются к графическому оборудованию. Вместо этого GDI взаимодействует с драйверами устройств от имени приложений.
Network containment	Сетевое сдерживание.
Ntdll.dll	Специальная библиотека системной поддержки, необходимая при использовании DLL подсистем. Она содержит функции двух типов: — интерфейсы диспетчера системных сервисов (system service dispatch stubs) к сервисам исполнительной системы Windows; — внутренние функции поддержки, используемые подсистемами DLL и другими компонентами ОС.
NTFS	Стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft. NTFS поддерживает хранение метаданных.
Odbcconf	Утилита командной строки Windows, которая позволяет настраивать драйверы ODBC (интерфейс доступа к базам данных) и имена источников данных.
Ole32.dll	Библиотека динамической компоновки, содержащая основные функции OLE (технологии связывания и внедрения объектов в другие документы и объекты).
Oleaut32.dll	Библиотека динамической компоновки, идентичная ole32.dll.
PE	Формат исполняемых файлов, объектного кода и динамических библиотек, используемый в 32-х и 64-разрядных версиях операционной системы Microsoft Windows.
Powershell	Расширяемое средство автоматизации от Microsoft с открытым исходным кодом, состоящее из оболочки с интерфейсом командной строки и сопутствующего языка сценариев.
Prefetcher	Компонент операционной системы Microsoft Windows, ускоряющий процесс её начальной загрузки, а также сокращающий время запуска программ.
PsExec	Утилита командной строки Windows. Инструмент от Microsoft, который позволяет удалённо запускать процессы с использованием учётных данных любого пользователя. Функционал программы схож с программой удалённого доступа, но вместо того, чтобы управлять удаленным компьютером с помощью мыши, команды отправляются на компьютер через командную строку.
RAT	Троян удаленного доступа – утилита для несанкционированного доступа к системе удаленного пользователя с корыстными целями.
RegAsm	Утилита командной строки Windows, которая позволяет регистрировать .NET-сборки.
Regsvr32	Утилита командной строки Windows, которая позволяет регистрировать или отменять регистрацию элементов управления OLE (технология связывания и внедрения объектов в другие объекты и документы)
RPC	Класс технологий, позволяющих программам вызывать функции или процедуры в другом адресном пространстве. Обычно реализация RPC-технологии включает два компонента: сетевой протокол для обмена в режиме клиент-сервер и язык сериализации объектов.

Термин	Расшифровка термина
Rpcrt4.dll	Библиотека динамической компоновки, которая предоставляет API удаленного вызова процедур (RPC), используемый приложениями Windows для связи по сети и через Интернет.
Rundll32	Хост-процесс Windows. Компонент операционных систем семейства Microsoft Windows, запускающий программы, находящиеся в динамически подключаемых библиотеках.
Screenshot	Изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора или другого визуального устройства вывода.
Setupapi.dll	Библиотека динамической компоновки, которая предоставляет два набора функций: — общие функции установки; — функции установки устройств. Программное обеспечение для установки устройств может использовать эти функции для выполнения настраиваемых операций в установщиках классов, соустановщиках и приложениях установки устройств.
SHA-1	Алгоритм криптографического хеширования. Описан в RFC 3174. Для входного сообщения произвольной длины алгоритм генерирует 160-битное хеш-значение, называемое также дайджестом сообщения, которое обычно отображается как шестнадцатеричное число длиной в 40 цифр.
SHA-256	Алгоритм хеширования. Криптографическая хеш-функция, разработанная Агентством национальной безопасности США.
Shell32.dll	Библиотека динамической компоновки, которая отвечает за отображение иконок в различных диалоговых окнах операционной системы Windows.
Shlwapi.dll	Библиотека динамической компоновки, которая содержит функции для путей UNC и URL, записей реестра и настроек цвета.
Sigma	Унифицированный формат описания правил детектирования событий.
SOC	Центр обеспечения безопасности.
SSDeep	Программа для расчета нечетких хешей.
SSL	Криптографический протокол, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
Svchost.exe	Хост процесс Windows, главный процесс для служб, загружаемых из динамических библиотек.
Task Sheduler	Компонент Microsoft Windows, который предоставляет возможность запланировать запуск программ или скриптов в определённые моменты времени или через заданные временные интервалы.
TCB	Применительно к EDR – флаг, который указывает, что исполняемый файл, который отмечен этим флагом, является максимально доверенным для ОС.
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.

Термин	Расшифровка термина
Threat Hunting	Охота на киберугрозы – это активная деятельность по киберзащите. Процесс упреждающего и итеративного поиска в сетях для обнаружения и изоляции сложных угроз, которые обходят существующие решения безопасности.
TLSH	Библиотека для матчинга нечетких хешей, разработанная компанией Trend Micro.
Trustlets	Программы, запускаемые как IUM-процессы (Isolated User Mode) в VSM (Virtual Secure Mode)
TTP	Тактики, техники и процедуры, используемые злоумышленниками для осуществления атак
User32.dll	Библиотека динамической компоновки, содержащая функции Windows API, связанные с пользовательским интерфейсом Windows (обработка окон, основные функции пользовательского интерфейса и т. д.)
Userenv.dll	Библиотека динамической компоновки, которая содержит функции интерфейса прикладного программирования (API) для создания профилей пользователей и управления ими.
Usp10.dll	Библиотека динамической компоновки, которая содержит набор функций интерфейса прикладного программирования (API), позволяющие клиенту макета текста форматировать сложные сценарии.
UTC	Стандарт, по которому общество регулирует часы и время. Отличается на целое количество секунд от атомного времени и на дробное количество секунд от всемирного времени UT1.
UUID	Стандарт идентификации, используемый в создании программного обеспечения, основное назначение которого – позволить распределённым системам уникально идентифицировать информацию без центра координации.
Uxtheme.dll	Библиотека динамической компоновки, отвечающая за изменение графических тем системы.
Verclsid	Утилита Windows, которая позволяет верифицировать в ОС COM-объекты. Может использоваться злоумышленниками для скрытного выполнения вредоносного кода.
Version.dll	Библиотека динамической компоновки, содержащая функции интерфейса прикладного программирования (API), используемые приложениями для проверки версии Windows.
Virus Total	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ. Кроме бесплатной существует корпоративная платная версия.
Vssadmin	Утилита Windows, которая позволяет администрировать в командной строке службы теневого копирования (резервирования) томов.
Wbadmin	Утилита Windows, которая позволяет в командной строке выполнять резервное копирование и восстановление операционной системы, томов, файлов и приложений.
White Team	Судьи/организаторы киберучений, контролирующие их ход.
Whoami	Утилита Windows, позволяющая получить информацию о пользователе, вошедшем в локальную систему, а также его группе и привилегиях.
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса.

Термин	Расшифровка термина
Winmm.dll	Библиотека динамической компоновки для Windows Multimedia API, который содержит низкоуровневый звук и функции джойстика.
Winspool.drv	DLL-библиотека, содержащая API-методы, которые используется GDI (интерфейс графических устройств) и приложениями для взаимодействия с сервисом печати.
WMI	Инструментарий управления Windows. Одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.
Wmic	Утилита, которая предоставляет интерфейс командной строки для инструментария управления Windows (WMI).
WmiPrvSE	Системный процесс Windows, который позволяет программам, установленным на компьютере, получать различную информацию об ОС.
Ws2_32.dll	Библиотека динамической компоновки, содержащая API-интерфейс Windows Sockets, используемый большинством интернет-приложений и сетевых приложений для обработки сетевых подключений.
YARA	Инструмент для матчинга текстовой информации, направлен на помощь исследователям вредоносных программ в выявлении и классификации образцов вредоносных программ.

Цитирование документа допускается только со ссылкой на настоящее руководство. Руководство не может быть полностью или частично воспроизведено, тиражировано или распространено без разрешения АО «РТ-ИБ».