

RT Protect TI

Руководство аналитика

Версия 1.0.35 от 19 июня 2026

Разработано компанией АО «РТ-Информационная безопасность»



1. Общие положения	4
1.1 Идентификация документа	4
1.2 Аннотация документа	4
1.3 Термины и определения	4
1.4 Условные обозначения	6
2. Общие сведения	7
2.1 Назначение и архитектура программы	7
3. Организационно-распорядительные меры	8
3.1 Общие сведения	8
3.2 Комплектность поставки	8
3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения	8
4. Особенности функционирования программы	9
4.1 Требования к среде функционирования	9
5. Интерфейс программы	10
5.1 Окно авторизации и общие сведения	10
5.2 Горизонтальная панель управления	12
5.2.1. Меню «Пользователь»	14
5.3 Администрирование	17
5.3.1. Организации	17
5.3.2. Источники данных	19
5.3.3. Теги	35
5.4 Аналитика	44
5.4.1. Активность	44
5.4.2. Заключение аналитика	51
5.4.3. Анализаторы	58
5.4.4. Граф связей	67

5.4.5. Yara-правила	69
5.4.6. Распространяемая аналитика	75
5.4.7. Угрозы и злоумышленники	82
5.4.8. Вредоносное ПО	83
5.4.9. Инструменты	85
5.4.10. Матрица MITRE ATT&CK	86
5.4.11. Лента угроз	87
5.4.12. Уязвимости	90
5.4.13. ИИ агент	100
5.5 Аналитика EDR	102
5.5.1. Индикаторы атак	102
5.5.2. Индикаторы компрометации	125
5.5.3. Журналы.....	130
5.5.4. Yara-правила (файлы)	133
5.5.5. YARA-правила (память)	137
5.6 Исключения EDR.....	140
5.6.1. Исключения для программ.....	141
5.6.2. Исключения для файлов	147
5.6.3. Сетевые исключения	153
5.6.4. Исключения индикаторов атак	157
6. Действия после сбоя и ошибки.....	162
6.1 Общие сведения	162
7. Перечень сокращений	163
8. Заключение.....	164

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect TI» Руководство Аналитика
Версия документа	Версия 1.0.35 (актуальна для версии продукта 3.4.0)
Идентификация программы	Сервис по предоставлению аналитики «RT Protect TI»
Идентификация разработчика	АО «РТ-Информационная безопасность»

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей с ролью «Аналитик» (в рамках организации владельца платформы) с работой сервиса по предоставлению данных по киберугрозам «RT Protect TI» (далее по тексту программа) и содержит общие сведения о программе, описание возможностей работы с программой, а также процессов функционирования программы.

1.3 Термины и определения

В настоящем документе используются термины и определения согласно ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» согласно таблице 2.

Таблица 2 – Термины и определения

Термин	Описание
Аналитик	Уполномоченный пользователь, ответственный за эксплуатацию программы
JSON	Текстовый формат обмена данными, основанный на JavaScript
JSON-объект	Неупорядоченный набор пар ключ/значение. Объект начинается с открывающей фигурной скобки { и заканчивается закрывающей фигурной скобкой}. Каждое имя сопровождается двоеточием, пары ключ/значение разделяются запятой
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux

Термин	Описание
Malware Bazaar	Проект сайта abuse.ch, целью которого является обмен образцами вредоносного ПО с сообществом информационной безопасности, поставщиками антивирусных программ и поставщиками информации об угрозах
Sophos	Производитель средств информационной безопасности для настольных компьютеров, серверов, мобильных устройств, почтовых систем и сетевых шлюзов
SSDEEP	Алгоритм нечеткого хеширования
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами. В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ
Web-сервер	Сервер, принимающий HTTP-запросы от клиентов, чаще всего веб-браузеров, и выдающий HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем

1.4 Условные обозначения

Условные обозначения, применяемые в документе, представлены в таблице 3.

Таблица 3 – 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 RT Protect TI

2. Общие сведения

2.1 Назначение и архитектура программы

RT Protect TI – это программное решение, которое позволяет собирать, обрабатывать, накапливать и распространять данные о киберугрозах (Threat Intelligence), то есть выполняет функции TI-платформы. Решение предоставляет аналитикам информационной безопасности возможность работать с актуальными сведениями об угрозах для эффективных расследований инцидентов и упреждения вредоносной активности.

Программа функционирует под управлением ОС Linux Ubuntu 20.04.5 LTS.

Для распространения сервиса применяется две модели:

- on-premise (покупка дистрибутива и установка на мощностях клиента);
- on-cloud (установка и развертывание сервиса осуществляется на мощностях предприятия-разработчика сервиса уполномоченными сотрудниками, доступ к сервису как услуга).

Программа предназначена для обработки информации, не являющейся секретной.

Программа имеет многофункциональный пользовательский интерфейс и подразумевает наличие следующих ролей пользователя:

Пользователь – может загружать для анализа на сервисе различные артефакты, просматривать отчеты по проверке артефактов, просматривать графики проверки артефактов с распределением по времени.

Администратор – выполняет установку и корректную настройку программы в соответствии с настоящим руководством, регистрирует новых пользователей, подключенных к сервису, регистрирует новые организации, подключенные к сервису, подключает новые источники данных, предоставляющие информацию, и осуществляет другие функции;

Аналитик – пользователь, ответственный за анализ поступающих от программы данных. Аналитик принимает решения по дальнейшей реакции на обнаруженные угрозы, заполняет и редактирует аналитические наборы, может загружать артефакты для их последующего анализа и просмотра отчетов по его результатам.

3. Организационно-распорядительные меры

3.1 Общие сведения

Программа поставляется заказчику на основании договора о поставке, заключенного между заказчиком и правообладателем.

Программа и документация на нее хранятся на сервере предприятия-изготовителя.

Программа поставляется заказчику согласно комплектности поставки.

3.2 Комплектность поставки

Комплектность поставки представлена в таблице 4.

Таблица 4 – Комплектность поставки

Обозначение	Наименование	Кол.	Примечание
	Сервис по предоставлению аналитики Модуль администрирования «RT Protect TI»	1	
	Комплект документов согласно списку: — «Руководство Администратора RT Protect TI» — «Руководство Аналитика RT Protect TI» — «Руководство Пользователя RT Protect TI»	1	

3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения

Процедуры и меры безопасности при распространении программы к месту назначения решают следующие задачи:

- обеспечивают идентификацию и целостность программы во время пересылки;
- обеспечивают обнаружение несанкционированных модификаций программы;
- препятствуют попыткам подмены программы от имени разработчика.

4. Особенности функционирования программы

4.1 Требования к среде функционирования

Программа работает на 64-х разрядной платформе семейства Linux (Ubuntu 20.04.5 LTS).

Аппаратная платформа сервера обеспечивает возможность выполнения функциональных требований, предъявляемых к серверу, с учетом технологии его построения, критериев производительности и отказоустойчивости.

Программа пригодна для функционирования на аппаратных платформах, указанных в таблице 5.

Таблица 5 – Программно-аппаратное обеспечение

Характеристики	Платформа	
	Минимальные требования	Рекомендуемые требования
Процессор	Не менее 12 ядер частотой минимум 2,4 ГГц	Не менее 20 ядер частотой минимум 2,4 ГГц
Оперативная память	32 Гб	64 Гб
Жесткий диск	SSD: 2 Тб	SSD: 2 Тб

Программа поддерживает работу в браузерах, представленных в таблице 6.

Таблица 6 – Список поддерживаемых браузеров

№ п/п	Тип браузера	Минимальная рекомендуемая версия
1	Google Chrome	Версия не ниже 92.0.4515.107
2	Firefox Browser	Версия не ниже 83.0

5. Интерфейс программы

5.1 Окно авторизации и общие сведения

Вход в программу производится из поддерживаемой версии браузера. Для открытия окна авторизации необходимо в строке браузера ввести имя сервера или его IP-адрес. После ввода в строке браузера корректных данных откроется окно авторизации (рис. 1).

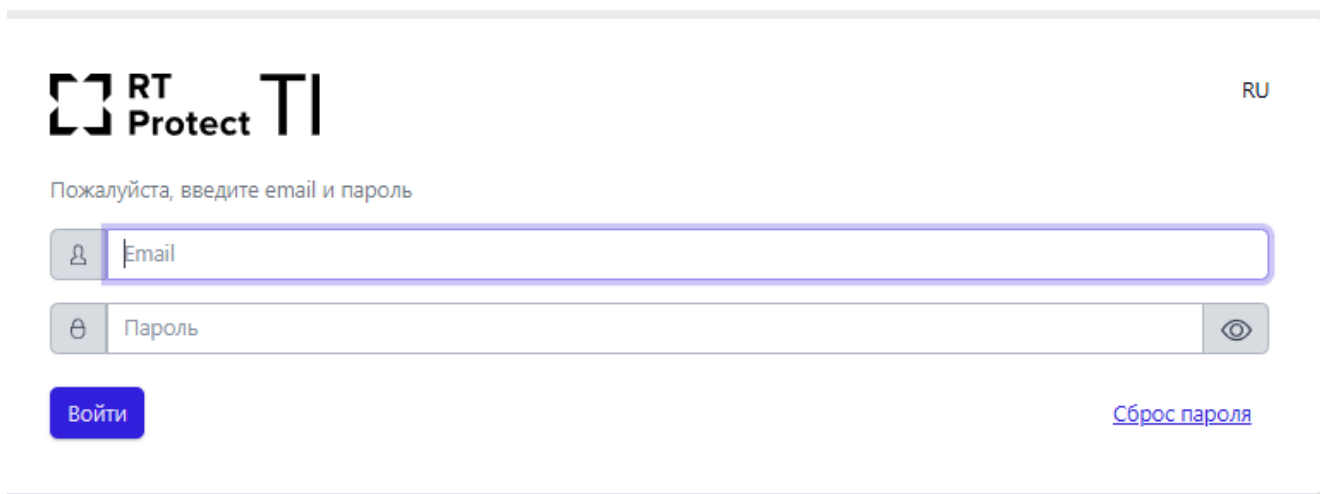


Рисунок 1 – Окно авторизации

При нажатии по иконке **Сброс пароля**, откроется окно, в котором потребуется ввести действующую почту, на которую будет отправлена ссылка для сброса пароля. После перехода по данной ссылке открывается окно для сброса пароля, представленное на рисунке 2.

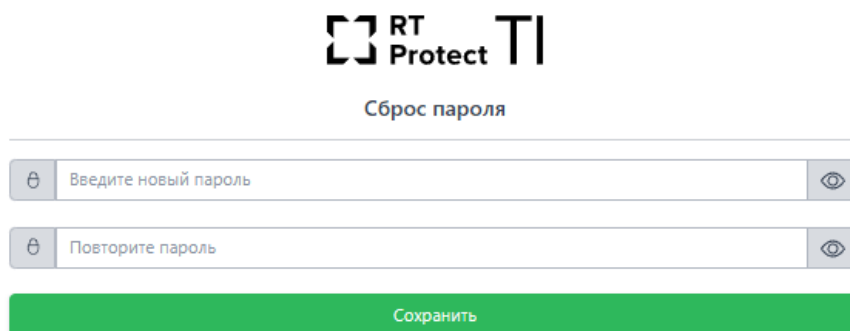


Рисунок 2 – Окно ввода параметром для сброса пароля

После ввода нового пароля потребуется вновь авторизоваться, для этого необходимо ввести в окне авторизации имеющийся логин (email) и новый пароль.

После ввода в окне авторизации пароля и логина для пользователя с ролью «Аналитик» открывается Главная страница (рис. 3).

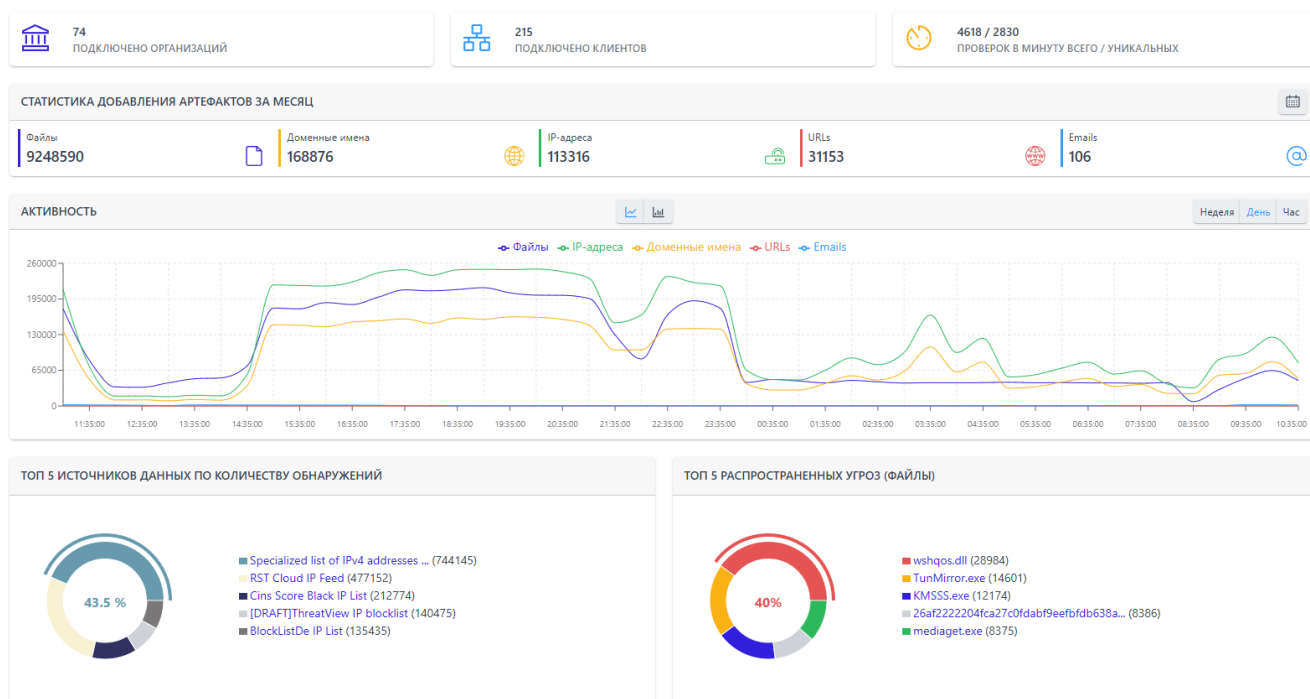


Рисунок 3 – Главная страница

Если в течение 5 минут пользователь выполнил 5 неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор (подробнее см. подраздел 5.3).

В левой части основного окна программы (см. рис. 3) находится вертикальная панель управления, доступная аналитику. С помощью панели управления пользователь может переходить по разделам программы для изменения настроек и просмотра информации по разделам. При выборе определенного раздела в правой части окна будет представлена информация выбранного раздела и основной инструментарий для работы пользователя программы.

В нижней части страницы находится информация о товарном знаке компании –



Справа от текущей версии программы отображается надпись о том, где «RT Protect TI» разработана – **Сделано в России**.

5.2 Горизонтальная панель управления

В верхней части окна находится горизонтальная панель управления (рис. 4).

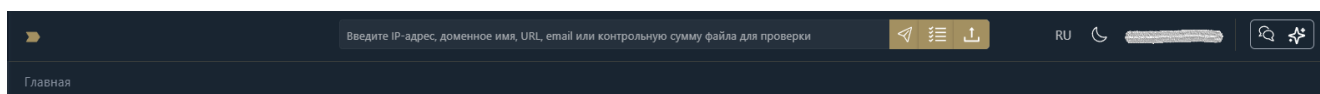


Рисунок 4 – Горизонтальная панель управления

При нажатии по иконке  в нижней части горизонтальной панели отображается, на какой странице с уровнем вложенности находится пользователь, например, [Главная / Источники данных / Abuse MalwareBazaar](#).

При наведении указателя мыши на каждый уровень и нажатии по нему ЛКМ можно перейти на страницу с данным указателем.

При нажатии по иконке  все страницы будут представлены в темной теме. Для возврата светлой темы необходимо повторно нажать на иконку.

При нажатии ЛКМ по иконке  появляется область, представленная на рисунке 5.

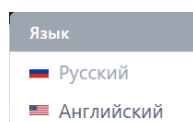


Рисунок 5 – Выбор языка

В данной области можно выбрать язык, на котором будет отображаться информация на всех страницах модуля администрирования.

При нажатии по иконке , открывается область чата, где пользователи могут оставлять сообщения и комментарии, отвечать на сообщения, оставленные другими пользователями, а также редактировать и удалять собственные комментарии.

При нажатии по иконке , открывается окно для работы с ИИ агентом (подробнее см. в пункте 5.4.13).

В области представленной на рисунке 6 можно отправить артефакт, либо список артефактов на проверку.



Рисунок 6 – Область быстрой отправки артефактов на проверку

В области **Проверка артефактов** администратор может получить вердикт для IP-адреса, домена, EMAIL, URL-адреса или хеш-суммы. Для этого необходимо ввести данные соответствующего артефакта в строку и нажать по иконке **Отправить** ().

Откроется отчет TI-платформы (подробнее см. в пункте 5.4.1).

В области **Проверка артефактов** администратор также может проверить целый список артефактов, нажав по иконке  , после чего откроется окно для загрузки списка артефактов, представленное на рисунке 7.

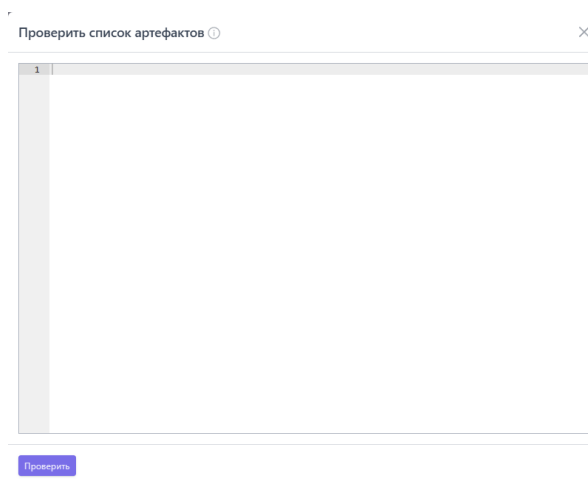


Рисунок 7 – Окно для добавления списка артефактов для проверки

В данном окне артефакт добавляется по одному в каждой строчке (строчки нумеруются). Проверка артефактов списком ограничена количеством в 1000 строк. После написания артефактов требуется нажать по иконке «Проверить».

Проверенный артефакт будет отображаться на странице **Активность** с вердиктом от TI-платформы (если артефакт уже присутствовал в базе). Можно создать заключение аналитика для одного или нескольких артефактов (создание заключения для группы артефактов).

Также в области проверки артефактов с помощью кнопки **Загрузить файл** () можно проверить файлы на компьютере, с которого осуществлен доступ к TI-серверу. После нажатия кнопки  откроется проводник, в котором можно выбрать файл, нуждающийся в проверке. Далее файл загружается на TI-платформу, а после завершения его загрузки выводится отчет с вердиктом.

5.2.1. Меню «Пользователь»

При нажатии ЛКМ на имени пользователя (логин) в правой верхней части основного окна программы открывается меню работы с учетной записью, в котором представлены подменю **Профиль пользователя**, иконка для загрузки документации и кнопка **Выход** для выхода из программы с текущего устройства (рис. 8).

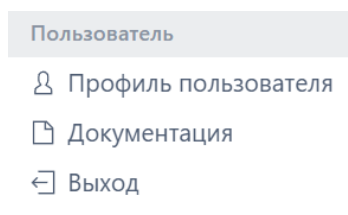


Рисунок 8 – Меню «Пользователь»

При нажатии по иконке **Документация** будет загружено руководство в формате pdf согласно роли, под которой был осуществлен вход, при этом руководства будут отличаться для ролей пользователей с выставленным признаком владельца и не владельца платформы.

Подменю **Профиль пользователя** представлено на рисунке 9.

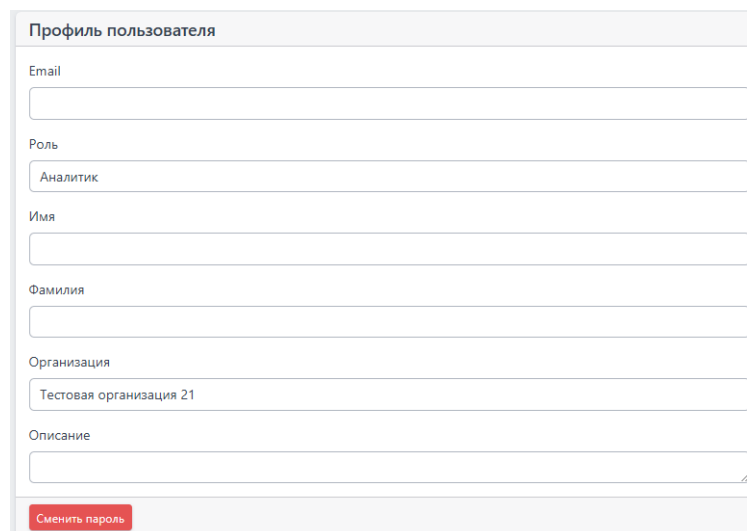


Рисунок 9 – Подменю «Профиль пользователя»

В данном окне информация о профиле пользователя представлена в виде следующих полей:

- адрес электронной почты для своей учетной записи;
- роль, назначенная пользователю администратором (**Администратор, Пользователь, Аналитик**);
- имя и фамилия пользователя;
- организация (информация об организации, в которой работает пользователь);
- поле с описанием профиля пользователя.

Изменять пароль возможно с помощью кнопки **Сменить пароль**. При нажатии кнопки **Сменить пароль** открывается окно для смены пароля (рис. 10).

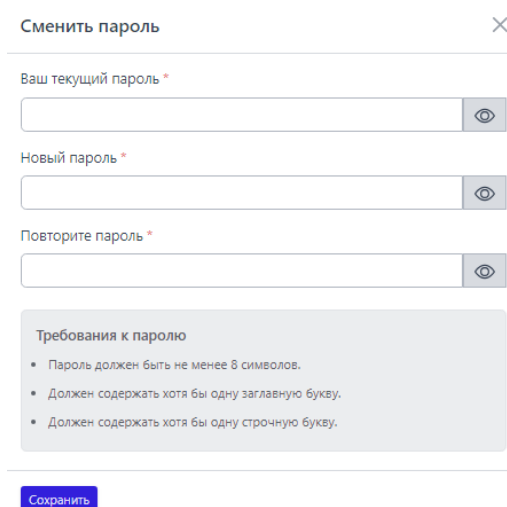


Рисунок 10 – Окно смены пароля

Введенный пароль должен соответствовать требованиям, указанным в нижней части окна. Для смены пароля необходимо ввести старый и новый пароль с подтверждением в соответствующие поля и нажать кнопку

Сохранить

При нажатии по иконке  /  имеется возможность показать/скрыть пароль.

5.3 Администрирование

В области **Администрирование** основной панели программы для учетной записи с ролью «Аналитик» содержатся следующие разделы:

- Организации;
- Источники данных;
- Теги.

На странице **Организации** аналитик может просматривать информацию об организациях, подключенных к сервису.

На странице **Источники данных** аналитик может выполнять следующие действия:

- просматривать источники данных о киберугрозах;
- добавлять новые источники данных о киберугрозах;
- загружать список с данными в CSV-формате на компьютер, с которого осуществлен доступ к серверу

TI.

На странице **Теги** аналитик может создавать группы тегов и группы псевдонимов для удобства маркирования источников данных.

5.3.1. Организации

Страница раздела **Организации** предназначена для ознакомления аналитиком со списком организаций, подключенных к сервису.

Общий вид страницы представлен на рисунке 11.

Организации							Сбросить фильтры
Название		Страна		Сектор		Признак активности	
Введите значение		Не задана		Не задан		Не задано	
Дата создания / изменения		Список		Календарь			
Все время							
« 1 2 3 4 ... »		Показывать по: 10				Найдено: 70, показано с 1 по 10	
☐	Название	Страна	Сектор	Количество обнаружений за месяц	Дата создания / Автор	Дата обновления / Пользователь	
☒	 тестовая 3			9	20.11.2025, 14:08:37	06.03.2026, 15:58:28	
☒	 тестовая 2			0	20.11.2025, 14:07:23		
☒	 тестовая 1			0	20.11.2025, 14:07:03		
☒	 vp-test			0	16.11.2025, 18:36:37		
☒	 ORG_testbud	Федеративные Штаты Микронезии	Сельское хозяйство	0	14.11.2025, 13:12:34	18.12.2025, 12:51:47	
☒	 test3(ME)			0	23.10.2025, 16:51:23		
☒	 test2(n_M)			0	23.10.2025, 16:50:43	23.10.2025, 16:51:42	
☒	 test_1(n_M_E)			0	23.10.2025, 16:49:37	23.10.2025, 16:50:05	
☒	 Test			0	14.10.2025, 13:20:55		
☒	 тестовая	Россия	Коммерческий сектор	0	13.10.2025, 16:27:36		
« 1 2 3 4 ... »		Показывать по: 10				Найдено: 70, показано с 1 по 10	

Рисунок 11 – Общий вид страницы «Организации»

Для фильтрации информации на странице предусмотрена система фильтров, представленная в следующем списке:

- Название;
- Страна;
- Сектор;
- Признак активности;
- Дата создания/Изменения.

Для пользователя с ролью аналитик недоступны возможности по добавлению и редактированию информации об организациях.

Иконка рядом с названием показывает, что организация, подключенная к админке на данный момент, имеет активное подключение  либо не активна .

Нажав в столбце **Название** по имени организации, аналитик переходит на страницу с информацией об организации.

На странице отдельной организации имеется возможность скачать отчет по найденным в организации артефактам сформированный сервисом RT Protect TI в формате pdf (иконка ) , либо отчет сформированный с помощью встроенного модуля использующего искусственный интеллект (иконка ).

5.3.2. Источники данных

Раздел **Источники данных** предназначен для добавления файлов с данными об артефактах, распространяемых различными вендорами на возмездной и безвозмездной основе. Источник данных может содержать как данные о киберугрозах (индикаторы компрометации), которые в зависимости от настройки TI-платформа будет классифицировать как вредоносные (подозрительные), так и белые списки артефактов, которые TI-платформа будет классифицировать как безопасные.

Для возможности добавления файла внешнего источника на TI-платформу файл должен соответствовать следующим условиям:

- загрузка файла должна осуществляться по фиксированной ссылке;
- файл должен загружаться по ссылке непосредственно либо должен загружаться архив поддерживаемого формата, в котором находится единственный файл;
- файл должен быть одного из поддерживаемых форматов (CSV, JSON, либо текстовый файл произвольного формата).

Общий вид окна раздела **Источники данных** представлен на рисунке 12.

Источники данных

Название: Введите значение | Класс артефакта: Не задан | Теги: Не заданы | Приоритет (не менее): Не задан

Статус: Не задано | Дата создания / изменения: Все время | Типы источников: Не задан

Показывать по: 10

	Название	Обнаружений за месяц	Элементов	Актуальных	STIX	Статус	Приоритет	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☐	Payloads Collected by URL Haus	0	0	0	0		0 0 0 0 0	13.03.2026, 14:24:03	13.03.2026, 15:56:48	
☐	for_test11	92	1807	1807	0		0 0 0 0 0	12.03.2026, 16:12:04	12.03.2026, 18:36:43	
☐	URL Haus (Online)	0	14060	14060	0		0 0 0 0 0	12.03.2026, 12:32:29	12.03.2026, 12:37:25	
☐	URL Haus	0	21585	21585	0		0 0 0 0 0	12.03.2026, 11:51:42	12.03.2026, 11:59:18	
☐	test_feed_IP_Qa	43	100	100	0		0 0 0 0 0	18.03.2026, 17:14:19	Пользователь не найден	
☐	SECURELIST_test_QA	0	9	9	2		0 0 0 0 0	05.03.2026, 17:52:47	Создан автоматически	
☐	Blog Malware Bytes_forrest_other_org	0	0	0	1		0 0 0 0 0	05.03.2026, 17:48:39	Создан автоматически	
☐	test_SSL (не установлен чек-бокс)	20	60	60	0		0 0 0 0 0	05.03.2026, 15:08:29	06.03.2026, 18:12:42	
☐	test_SSL (установлен чек-бокс)	0	0	0	0		0 0 0 0 0	05.03.2026, 15:08:18	Пользователь не найден	
☐	ip-test-feed-1	0	0	0	0		0 0 0 0 0	04.03.2026, 16:46:32	04.03.2026, 16:47:07	

Найдено: 174, показано с 1 по 10

Добавить источник | Аналитика источников

Рисунок 12 – Окно раздела «Источники данных»

Таблица со списками источников данных имеет следующие поля:

- **Название** (отображается название базы данных);
- Количество обнаружений за месяц;
- Элементов;
- Актуальных;
- STIX;
- **Статус** (отображается информация о статусе обновления базы);
- **Приоритет** (минимальный, низкий, ниже среднего, средний, выше среднего, высокий);
- Дата создания/Автор;
- Дата последнего изменения/Пользователь;
- **Управление** (отображаются элементы управления: активировать/деактивировать источник данных,

редактировать источник, удалить источник, синхронизация источника данных, подключенного к сервису, с базой источника извне.

Для фильтрации информации в таблице имеется система фильтров, которая представлена следующими фильтрами:

- **Название** (название базы данных);

- **Класс артефакта** (безопасный, вредоносный, подозрительный);
- **Тэги** (ключевые слова, которые задаются при редактировании/добавлении источника и нужны для дополнительного удобства категорирования и классификации источников);
- **Приоритет** (минимальный, низкий, ниже среднего, средний, выше среднего, высокий);
- Статус;
- **Тип источника** (JSON, CSV, STIX, Провайдер, Отчет, любой формат);
- Дата создания/Изменения;

В столбце **Статус**, в строчке напротив источника, который загружается с ошибкой, имеется иконка с предупреждением . При наведении на данную иконку указателя мыши появляется всплывающее окно, представленное на рисунке 13.

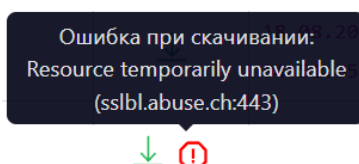


Рисунок 13 – Сообщение об ошибке при скачивании обновления источника

В столбце **Статус** может присутствовать иконка, показывающая количество нераспознанных артефактов , то есть артефактов в источнике данных, которые имеют некорректную информацию.

Список таких артефактов можно просмотреть, перейдя на страницу источника данных и раскрыв область **Нераспознанные артефакты**.

В поле Автор создания источника данных может присутствовать запись «Создан автоматически», это означает что источник данных формируется автоматически из подключенного провайдера данных.

При нажатии на странице **Источники данных** по иконке  откроется страница, представленная на рисунке 14.

Аналитика источников

Тип артефакта

Не задан

Процент пересечения

Введите значение

%

Источники данных

Не задан

Источники данных	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1 RST Cloud IP Feed	-	0	0	< 1 %	0	1.6 %	0	0	0	0	< 1 %	< 1 %	0	0	4.9 %	0	0	0	< 1 %	0	0
2 Abuse MalwareBazar	0	-	< 1 %	0	0	0	< 1 %	0	95.3 %	< 1 %	< 1 %	< 1 %	0	20.6 %	0	< 1 %	0	0	< 1 %	< 1 %	0
3 LOKINEW	0	2.3 %	-	0	0	0	0	0	2.3 %	< 1 %	0	0	0	2.5 %	0	< 1 %	0	0	0	0	0
4 AbuseIPDB Top IP Addresses	33.8 %	0	0	-	0	1.4 %	0	0	0	0	0	0	0	0	5.4 %	0	0	0	0	0	0
5 Email-Domains Block List	0	0	0	0	-	0	0	0	0	0	0	0	< 1 %	0	0	0	0	0	0	0	0
6 Global CSV	100%	0	0	< 1 %	0	-	0	0	0	0	0	0	0	0	93.6 %	0	0	0	0	0	0
7 PMI_Test_1.1_18	0	100%	0	0	0	0	-	0	100%	0	0	0	25.0 %	100%	0	0	0	0	0	0	0
8 RST Cloud URL Feed	0	0	0	0	0	0	0	-	0	0	< 1 %	< 1 %	0	0	0	0	0	0	< 1 %	0	0
9 Abuse	0	100%	< 1 %	0	0	0	< 1 %	0	-	< 1 %	< 1 %	< 1 %	0	16.8 %	0	< 1 %	0	0	< 1 %	< 1 %	0
10 Global SET	0	11.7 %	< 1 %	0	0	0	0	0	9.8 %	-	0	0	0	28.2 %	0	< 1 %	0	0	0	0	< 1 %
11 Source_from_file_test_ii	24.4 %	< 1 %	0	0	0	0	0	63.6 %	< 1 %	0	-	100%	16.7 %	< 1 %	0	0	0	0	100%	0	0
12 FinCERT	24.4 %	< 1 %	0	0	0	0	0	63.6 %	< 1 %	0	100%	-	16.7 %	< 1 %	0	0	0	0	100%	0	0
13 RST Cloud Domain Feed	0	0	0	0	< 1 %	0	< 1 %	0	0	0	< 1 %	< 1 %	-	0	0	0	< 1 %	0	< 1 %	0	0

Рисунок 14 – Страница Аналитика источников

На данной странице в табличной форме представлена матрица пересечения источников данных, которая может быть использована аналитиком для понимания приоритетности источников данных. Таблица изменяется при применении фильтров, представленных выше таблицы.

В таблице показаны источники данных и процент пересечения данных, входящих в источники. Например, у источника данных в строке 7 (PMI_Test_1.1_18) имеется 100% пересечение данных, входящих в источник 9 (Abuse).

При нажатии в поле пересечений ЛКМ откроется окно с информацией по пересечениям с источниками по типам артефактов в источнике (рисунок 15).

Пересечения						
	Всего					
RST Cloud IP Feed	3403665	0	3403665	0	0	0
FinCert	247187	239867	4579	1524	1135	82
Пересечения	3921	0	3921	0	0	0
93.22% 0.11% 6.67%						

Рисунок 15 – Информация по пересечениям данных аналитики в источнике

При нажатии по названию источника на странице Источники данных, например, [Abuse MalwareBazaar](#) откроется окно с информацией по источнику, представленное на рисунке 16.

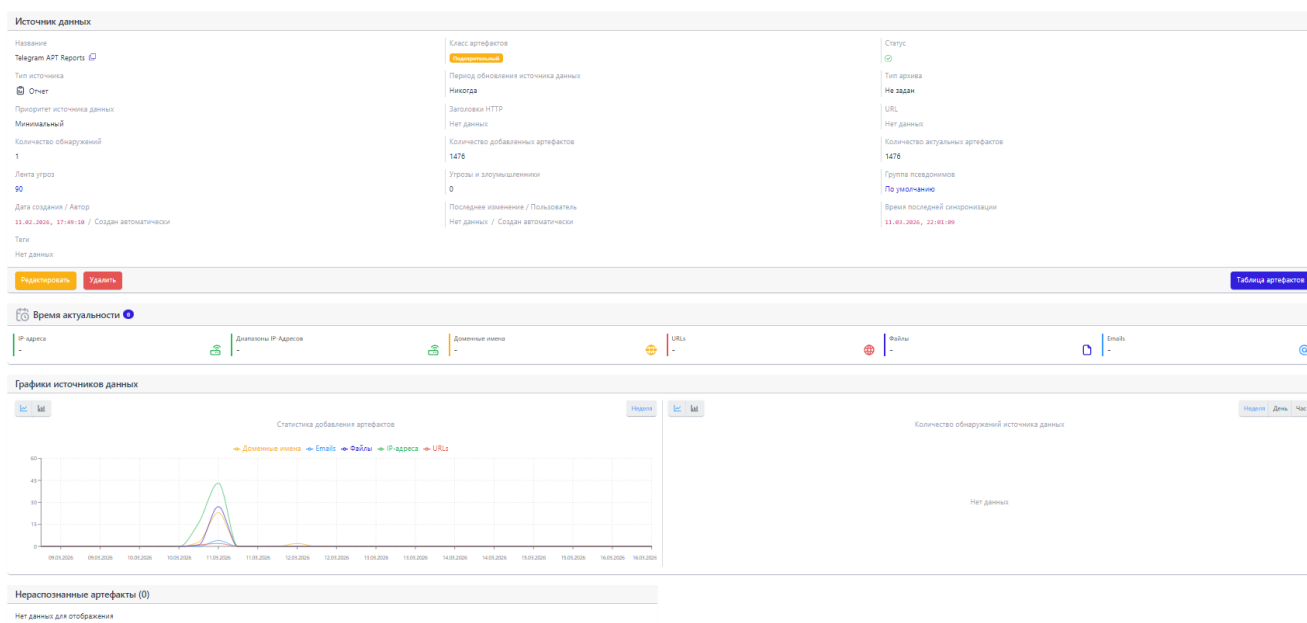


Рисунок 16 – Окно информации по источнику данных

В данном окне представлены следующие области:

- источник данных (выводится информация о добавленном источнике);
- время актуальности (указывается общее время актуальности данных из источника);
- Нераспознанные артефакты;
- Графики источников данных (Статистика добавления артефактов, количество обнаружений источника данных).

При нажатии по иконке  открывается окно для редактирования информации по источнику данных, представленное на рисунке 17.

Редактировать источник

Основные настройки | Настройка парсинга (JSON)

Имя *
Abuse IP DB

Приоритет источника данных *
Средний

Группа псевдонимов
По умолчанию

Теги
Не задан

Класс артефактов *
Вредоносный

Время актуальности *
Общее время актуальности элемента источника данных *
0

IP-адреса
Введите значение

Диапазоны IP-Адресов
Введите значение

Доменные имена
Введите значение

URLs
Введите значение

Файлы
Введите значение

Emails
Введите значение

Тип источника *
JSON

Тип аризма
Не задан

Источник
Выбор источника из загруженных

URL *
https://api.abuseipdb.com/api/v2/blacklist

Период обновления источника данных *
Никогда

Добавить заголовок HTTP
Ключ
Значение

Загрузить часть файла | Проверить настройки | Сохранить

Рисунок 17 – Окно редактирования источника данных

В данном окне имеется возможность редактировать основные настройки либо настройки парсинга источника данных, после чего требуется нажать по иконке **Сохранить**.

При нажатии по иконке **Таблица артефактов** на странице источника данных, открывается окно с таблицей, показывающей список артефактов, представленных по этому источнику данных (рисунок 18).

Артефакты Abuse IP DB

Артефакт
Введите значение

Дата обнаружения
начальная дата → конечная дата

Дата синхронизации
начальная дата → конечная дата

Актуальность
Не задана

Активация
Не задана

Теги
Не заданы

Файлы | IP-адреса | Диапазоны IP-Адресов | Доменные имена | URLs | Emails

Показывать по: 50

Найдено: 10000, показано с 1 по 50

Артефакт	Время обнаружения	Время последней синхронизации	Другие источники	Управление
☐ 329.128.122.76 Неактуальный	11.03.2026, 15:54:33	11.03.2026, 15:54:35	RST Cloud IP Feed ThreatView IP blacklist Attackers IP RUTGRES BlockListDe IP List	☐
☐ 195.185.75.133 Неактуальный	11.03.2026, 15:54:33	11.03.2026, 15:54:35	RST Cloud IP Feed Cins Score Black IP List ThreatView IP blacklist BlockListDe IP List	☐
☐ 181.82.128.185 Неактуальный	11.03.2026, 15:54:33	11.03.2026, 15:54:35	RST Cloud IP Feed ThreatView IP blacklist BlockListDe IP List	☐
☐ 159.82.286.171 Неактуальный	11.03.2026, 15:54:33	11.03.2026, 15:54:35	RST Cloud IP Feed ThreatView IP blacklist Attackers IP RUTGRES BlockListDe IP List Specialized list of IPv4 addresses belonging to common VPN providers and datacenters	☐

Рисунок 18 – Окно Таблица артефактов по источнику данных

В этом окне для фильтрации информации имеется система фильтров согласно следующему списку:

- Артефакт;
- **Дата обнаружения** (начальная и конечная даты);
- **Дата синхронизации** (начальная и конечная даты);
- **Актуальность** (не задан, актуальный, не актуальный);
- **Активация** (не задан, активен, не активен);
- Теги.

В области **Управление** с помощью иконки  можно исключить из анализа отдельный артефакт из источника.

Также в списке артефактов источника можно исключить/включить несколько артефактов из анализа с помощью иконок  / .

Артефакт в таблице является активной ссылкой, при нажатии по которой происходит переход на страницу отчета по артефакту.

Графики на странице **Источник данных** могут быть представлены в линейном или столбчатом виде.

Для изменения вида графика имеются следующие иконки:

-  — линейное представление графика статистики;
-  — столбчатое представление графика статистики.

Для добавления нового источника, на странице Источники данных, требуется нажать по иконке

 **Добавить источник**

, после чего будет открыто окно добавления источника, представленное на рисунке 19.

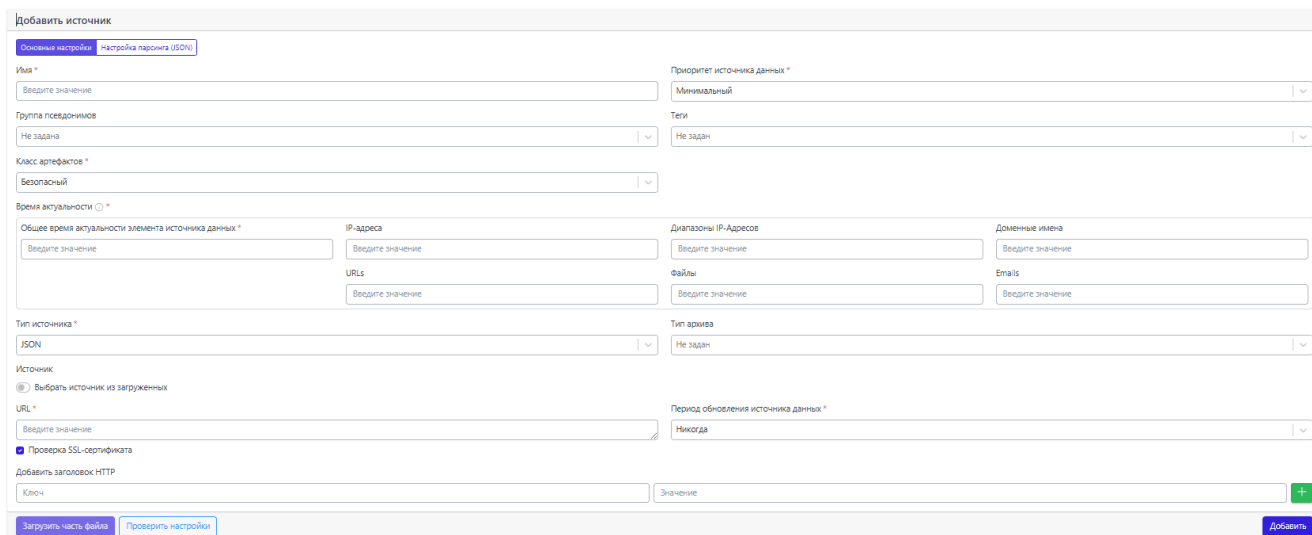


Рисунок 19 – Окно добавления источника данных

Параметры, требуемые для настройки источников данных в этом окне, разделены на 2 группы:

- 1) Основные настройки;
- 2) Настройки парсинга.

Основные настройки

Имя источника.

Приоритет источника данных – задает степень доверия к источнику данных по сравнению с другими источниками. Если артефакт находится одновременно в двух источниках данных, по которым настроен различный класс артефактов, вердикт по артефакту будет выдаваться на основании источника с самым высоким приоритетом. Если артефакт находится одновременно в двух источниках данных, по которым настроен различный класс артефактов, при этом приоритет обоих источников одинаков, приоритетным будет выбираться источник белого списка (класс артефактов безопасный).

При настройке данного параметра имеется возможность задания следующих приоритетов (Минимальный, Низкий, Ниже среднего, Средний, Выше среднего, Высокий).

Тэги (ключевые слова для удобства категорирования и классификации).

Группа псевдонимов.

Класс артефактов – задает вердикт, который будет выноситься артефактам, обнаруженным в данном источнике данных, для источника белого списка класс артефактов должен быть безопасный, для источника данных об угрозах класс артефактов должен быть вредоносный либо подозрительный.

Время актуальности в днях отчета по артефакту из источника (можно выставить общее время актуальности для источника, а также, время для каждого типа артефакта).

Тип источника (JSON, CSV, STIX, любой формат).

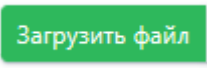
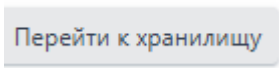
Тип архива (формат архива, загружаемого по ссылке, в котором содержится целевой файл с данными), тип архива не указывается, если файл скачивается не в архиве.

Переключатель «Выбрать источник из загруженных» позволяет загрузить файл с источником данных вручную, без использования внешних URL.

При таком режиме работы поля для выбора URL и HTTP-заголовков становятся недоступны.

В данном режиме работы можно выставить период обновления источника данных согласно следующих предустановленных параметров (никогда, час, 6 часов, 12 часов, день, 3 дня).

Для выбора источника данных из имеющихся загруженных источников следует сделать активной кнопку выбора **Выбрать источник из загруженных**, переведя ползунок кнопкой мыши вправо (рисунок 20), при

этом становятся активны иконки  – Загрузить файл,  – Перейти к хранилищу.

Источник
 Выбрать источник из загруженных

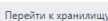
 

Рисунок 20 – Выбор источника из загруженных

При нажатии по иконке **Загрузить файл** происходит переход на страницу **Загрузки** на компьютере, с которого был осуществлен вход в модуль администрирования TI, для выбора уже имеющегося ранее загруженного файла с источником данных.

При нажатии по иконке **Перейти к хранилищу** происходит переход на страницу внутреннего хранилища файлов с источниками (рисунок 21).

Хранилище источников			
Показывать по: 50		Найдено: 9, показано с 1 по 9	
Название	Размер	Дата создания / Автор	Управление
test-kn-244.json	125 Б	10.01.2024, 13:00:19 rt@mail.ru	
file.csv	299.5 KB	12.12.2023, 16:30:44 test1@test.ru	
file_1.csv	268.15 KB	12.12.2023, 16:24:35 test1@test.ru	
file_1.csv	268.15 KB	12.12.2023, 16:19:09 test1@test.ru	
file.csv	299.5 KB	12.12.2023, 16:18:58 test1@test.ru	
test-kn-d.csv	96 Б	27.10.2023, 12:56:55 rt@mail.ru	
1.csv	134 Б	27.10.2023, 12:56:45 rt@mail.ru	
ProcessExplorer.zip	3.35 MB	13.10.2023, 16:00:38 rt@mail.ru	
Без названия (1).zip	126.16 MB	11.10.2023, 14:37:15 rt@mail.ru	
Показывать по: 50		Найдено: 9, показано с 1 по 9	

Рисунок 21 – Страница «Хранилище источников»

URL – фиксированная ссылка, по которой сервер может загрузить файл с данными.

Заголовки http – набор заголовков, которые будут передаваться серверу в запросе на скачивание целевого файла, могут содержать токены доступа и прочую информацию, которая требуется целевому серверу для возврата файла.

Период обновления источника данных – задает периодичность загрузки и синхронизации данных из источника с имеющимися на сервере данными, имеется возможность выбора следующих периодов обновления (никогда, день, 3 дня, неделя, месяц).

Тип источника – указывает формат целевого файла (JSON, CSV, любой формат). На основании выбранного формата отображаются дополнительные настройки парсинга.

JSON:

Путь до списка объектов с артефактами, путь до артефактов в рамках элемента списка.

CSV:

Порядковый номер колонки, в которой содержится артефакт – формат CSV подразумевает наличие на каждой строке записи с несколькими колонками. Требуется указать номер колонки (начиная с 0), в котором содержится целевой артефакт.

STIX (настройка парсинга невозможна).

Любой формат:

Регулярное выражение для разбора каждого элемента – при парсинге произвольного формата требуется указать регулярное выражение для поиска требуемых данных на каждой строке целевого файла.

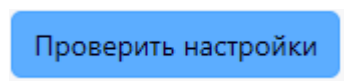
Выражение должно содержать как минимум одну группу, заключенную в круглые скобки, в которой будет содержаться артефакт.

В поле «Добавить заголовок HTTP» можно заполнить соответственно ключ и значение заголовка. Эти заголовки могут требоваться вендорам, предоставляющим файл с данными (например, на платной основе).

При указании галочки скрыть заголовок  значение заголовка не будет доступно для дальнейшего просмотра и редактирования.

Корректную настройку данных параметров можно проверить, нажав кнопку **Загрузить часть файла**. Если все настроено верно, на форме редактирования должны корректно отобразиться первые несколько строк целевого файла с данными.

Для проверки корректности настроек при добавлении источника имеется иконка



Настройки получения данных из файла (парсинга)

Под парсингом понимается разбор файла источника данных для получения артефактов, обрабатываемых TI-платформой.

Поле настройки получения данных из файла (парсинга) в зависимости от выставленного ранее типа источника имеет разные настройки и представлено на рисунках 22 - 24.

Добавить источник

Основные настройки | **Настройка парсинга (JSON)**

☐ JSONL - на каждой строке файла располагается JSON-объект

Путь до списка объектов с артефактами:

Путь до артефактов в рамках элемента списка:

Настройки дополнительных полей ⓘ

|

Рисунок 22 – Настройка парсинга файлов в формате JSON

Добавить источник

Основные настройки | **Настройка парсинга (CSV)**

Порядковый номер колонки, в которой содержится артефакт ⓘ *

0

Настройки дополнительных полей ⓘ

Введите значение | ▼ Номер колонки +

Загрузить часть файла | Проверить настройки | Добавить

Рисунок 23 – Настройка парсинга файлов в формате CSV

Добавить источник

Основные настройки | **Настройка парсинга (Любой формат)**

Регулярное выражение для разбора каждого элемента *

Введите значение

Символ разделения между элементами ⓘ

Введите значение

Номер группы, содержащий артефакт *

0

Настройки дополнительных полей ⓘ

Введите значение | ▼ Номер группы +

Загрузить часть файла | Проверить настройки | Добавить

Рисунок 24 – Настройка парсинга файлов любого формата

Настройка парсинга файлов в формате JSON

Путь до списка объектов с артефактами – если не установлен флаг JSONL, требуется указать путь до JSON-списка, содержащего объекты с артефактами в формате "property.property". Если JSON-список является корневым объектом, поле нужно оставить пустым.

Путь до артефактов в рамках элемента списка – требуется указать путь до элемента в формате "property.property", в котором содержится строка с целевым артефактом в рамках одного элемента списка. Если это корневой элемент, поле можно оставить пустым.

Для настройки дополнительных полей следует нажать кнопку «Добавить поле». При ее нажатии будут добавлены для поля ввода, для наименования поля и в зависимости от типа файла колонка, группа или JSON-свойство для получения значения поля в рамках одного артефакта. В строке «Наименование поля» можно указать как произвольные значения, так и выбрать значения из предложенных сервером: **Надежность данных** и **Дата обнаружения**.

Настройка парсинга файлов в формате CSV

При настройке парсинга файлов в формате CSV в основном поле следует указать **Порядковый номер колонки, в которой содержится артефакт** (номера колонок начинаются с 0). Настройка дополнительных полей аналогична настройке, описанной выше.

Настройка парсинга файлов любого формата

В поле **Регулярное выражение для разбора каждого элемента** можно написать выражение, по которому будет произведен разбор элемента.

Символ разделения между элементами – должен указываться, если вместо разбора файла построчно требуется разделить его содержимое по другому разделителю. По умолчанию для разделения между элементами используется новая строка.

Номер группы, содержащий артефакт – содержит номер группы в регулярном выражении, содержащий артефакт.

После добавления информации об источнике данных можно проверить правильность заполнения полей, нажав по иконке **Проверить настройки**.

Если параметры указаны некорректно, либо имеются незаполненные поля, выводятся соответствующие сообщения, например, как на рисунке 25.

The screenshot shows a web interface titled "Добавить источник" (Add Source). It has two tabs: "Основные настройки" (Basic settings) and "Настройка парсинга (Любой формат)" (Parsing settings (Any format)). The "Parsing settings" tab is active. It contains three main sections:

- Регулярное выражение для разбора каждого элемента *** (Regular expression for parsing each element *): A text input field with the placeholder "Введите значение" (Enter value) and a red border. Below it is a red error message: "Необходимо заполнить данное поле" (This field must be filled).
- Символ разделения между элементами** (Separator between elements): A text input field with the placeholder "Введите значение" (Enter value) and a red border.
- Номер группы, содержащий артефакт *** (Group number containing the artifact *): A text input field with the value "0" and a red border.

Below these sections is a section for **Настройки дополнительных полей** (Additional field settings), which includes a dropdown menu with the placeholder "Введите значение" (Enter value) and a text input field with the value "Номер группы" (Group number). At the bottom of the dialog are three buttons: "Загрузить часть файла" (Load part of the file), "Проверить настройки" (Check settings), and "Добавить" (Add).

Рисунок 25 – Сообщение об ошибках при добавлении/редактировании информации об источнике

При нажатии по иконке **Загрузить часть файла** в отдельном окне ниже данной иконки будет показана часть файла, предоставленного источником данных (рисунок 26).

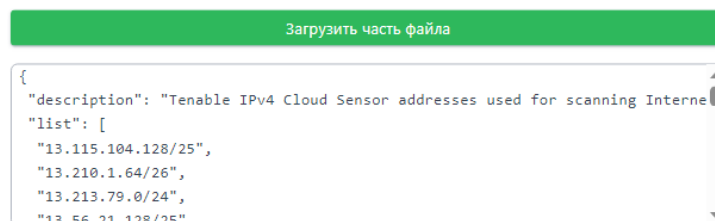


Рисунок 26 – Часть файла, предоставленного источником данных

Пример настройки источника данных на основе источника Malware Bazaar

Рассмотрим процедуру конфигурации источника данных на примере ресурса Malwarebazaar. На ресурсе в разделе **export** (<https://bazaar.abuse.ch/export/>) находится прямая ссылка на zip-файл со всеми данными – <https://bazaar.abuse.ch/export/csv/full/> (см. рисунок 27).

Note

Recent datasets ("recent additions") include hashes for the last 48 hours and are being generated every **5 minutes**. Please do not fetch them more often than that. Full data dumps include all hashes and are only being generated once per hour. Please do not fetch them more often than once per hour.

CSV files

The following data exports exists in CSV format:

- Recent additions ([download](#))
- Full data dump ([download](#) - zip compressed)

Рисунок 27 – Информация со страницы ссылки на источник

В описании содержится информация, что данный файл обновляется каждый час. В этом случае оптимальным периодом обновления файла в TI будет 1 день. Имея прямую ссылку, мы можем приступить к настройке источника данных.

Заполняем поле **Имя**, в поле **URL** указываем ссылку на файл, в выпадающем списке **Тип архива** выбираем значение **ZIP-архив**.

После заполнения этих полей мы можем нажать на кнопку **Загрузить часть файла** и проверить правильность введенных полей.

Далее заполняем остальные поля на вкладке **Основные настройки**:

- Период обновления источника данных устанавливаем «День»;
- Приоритет источника данных выбираем согласно уровню доверия относительно других источников данных (можно оставить «Минимальный»);

— Класс артефактов выбираем «Вредоносный» либо «Подозрительный» в зависимости от уровня доверия к содержимому файла;

— Время актуальности устанавливаем больше, чем заданный период обновления (1 день), чтобы элементы сохраняли признак актуальности в случае, когда очередная синхронизация не была завершена успешно; вводим в поле 5 дней.

— Формат файла выбираем CSV, исходя из содержимого файла.

Переходим на вкладку **Настройка парсинга**. Из загруженной части файла мы видим заголовки всех csv-колонок, доступных в файле.

"first_seen_utc", "sha256_hash", "md5_hash", "sha1_hash", "reporter", "file_name", "file_type_guess", "mime_type", "signature", "clamav", "vtpersent", "imphash", "ssdeep", "tlsh"

Артефактом в данном случае для нас будет являться SHA-256 от файла, которая находится в колонке sha256_hash.

Данная колонка находится под порядковым номером один, если вести отсчет от нуля. Вводим «1» в поле **Порядковый номер колонки, в которой содержится артефакт**.

Мы можем добавить информацию из всех остальных колонок csv-файла при помощи раздела **Настройки дополнительных полей** в правой части формы. Например, добавим время обнаружения артефакта. Для этого нажимаем на кнопку **Добавить поле**. На форме отображается два поля для ввода имени поля и номера колонки.

При нажатии на поле ввода **Наименование поля** отобразится выпадающий список, отображающий предустановленные на TI-платформе дополнительные поля. Выбираем из списка **Дата обнаружения**, т.к. это поле соответствует по смыслу тому полю, которое мы хотим добавить. В строку **Номер колонки** вводим порядковый номер колонки, если считать от нуля – 0.

Добавим также дополнительное поле из колонки file_name. Нажимаем на кнопку **Добавить поле**, чтобы на форме отобразились поля для ввода настроек для еще одной колонки. В поле **Наименование поля** не выбираем значение из выпадающего списка, а вводим своё. Записываем в строку ввода **Имя файла**. В поле **Номер колонки** вводим порядковый номер целевой колонки – 5.

После завершения настройки основного поля, содержащего артефакт, и всех желаемых дополнительных полей мы можем проверить корректность введенных нами настроек парсинга, нажав кнопку **Проверить настройки**.

Через некоторое время на форме отобразится окно, содержащее несколько полученных из файла записей об артефактах.

Нам требуется проверить корректность отображения следующих элементов:

- Поле **Артефакт** у элементов заполнено хешами SHA-256 файлов и отображается красным или желтым цветом (в зависимости от установленного в источнике данных класса артефактов).
- Поле **Дата обнаружения** заполнено значением, полученным из файла (время должно отличаться у каждого элемента).
- Поле **Имя файла** содержит имя каждого файла, а не иные данные.

Чтобы убедиться в корректности настроек, достаточно проверить 1-2 элемента (см. рисунок 28).

Артефакт	366C3E4F90B97F849AE44A2D0F6C6D78B9DAB71582E3FBECA225180B39D58983	Артефакт	04EE06F5A05400D75674FAE38ED7D2938468D096CEE29F2C896AA8C610F8E5BC
Время детектирования	14.03.2024, 11:47:48	Время детектирования	14.03.2024, 11:47:48
Надежность данных (от 0 до 100)	100	Надежность данных (от 0 до 100)	100
detectDate	2024-03-14 07:30:21	detectDate	2024-03-14 07:28:36
Имя файла	[External] Purchase Order from Telkomse.exe	Имя файла	file

Рисунок 28 – Проверка корректности настроек

Если настройка всех полей произведена корректно, нажимаем на кнопку **Добавить**. Источник данных будет сохранен и доступен для просмотра и редактирования в табличной форме. Синхронизация данных из источника будет произведена сразу после сохранения.

5.3.3. Теги

Теги в разделе **Администрирование** предназначены для удобства маркировки и ранжирования источников данных, а также для назначения своих тегов (псевдонимов) источникам данных, которые уже маркированы собственными тегами.

Общий вид страницы **Теги** представлен на рисунке 29.

☐	Название ¹	Префикс ¹	Описание	Количество	Дата создания / Автор ¹	Дата изменения / Автор	Управление
☐	111	euzy	111	1	04.12.2025, 14:59:58		✎ ✖
☐	vp-test-22	/	123	4	22.11.2025, 14:13:02	24.11.2025, 16:12:37	✎ ✖
☐	qa	qa	test	14	13.10.2025, 12:28:09		✎ ✖
☐	11	1	1	1	22.09.2025, 16:52:36	22.09.2025, 16:52:43	✎ ✖
☐	test_group	test	Тестовая группа тегов	2	19.06.2025, 18:56:36		✎ ✖
☐	TEST_QA	QA	для теста (удалить)	6	06.05.2025, 15:48:45	25.11.2025, 12:01:57	✎ ✖
☐	Fraud	fraud	Fraud	7	17.02.2025, 17:07:43	31.03.2025, 17:42:08	✎ ✖
☐	Network activity	network_activity	Network activity	18	17.02.2025, 17:05:08		✎ ✖
☐	Malware type	malware_type	Malware type	48	17.02.2025, 17:48:52		✎ ✖

Рисунок 29 – Страница Теги

Общий вид страницы имеет вид таблицы с полями, зависящими от вкладки, выбранной в верхней части страницы (**Группы тегов/Группы псевдонимов**).

Фильтрация на страницах **Группы тегов/Группы псевдонимов** осуществляется с помощью следующих фильтров:

- Название;
- Дата создания/изменения.

Таблица с полями для выбранной вкладки (вкладка помечена серым цветом), например, **Группы тегов** представлена полями согласно следующему списку:

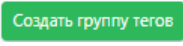
- Кнопка выбора ☐ / ☒ ;
- Название (название группы тегов);
- Префикс;
- Дата создания/Автор;

- Дата изменения /Автор;
- Описание;
- Количество (количество элементов в группе);
- Управление (редактирование группы , удаление группы ).

Для удаления группы тегов необходимо в поле **Управление** нажать по иконке удаления группы.

Для удаления нескольких групп тегов следует пометить необходимые группы кнопкой выбора и нажать по иконке .

На странице имеются иконки для экспорта  в формате JSON информации о тегах, и для импорта тега .

Для создания новой группы тегов требуется нажать по иконке , после чего откроется окно создания группы тегов, представленное на рисунке 30.

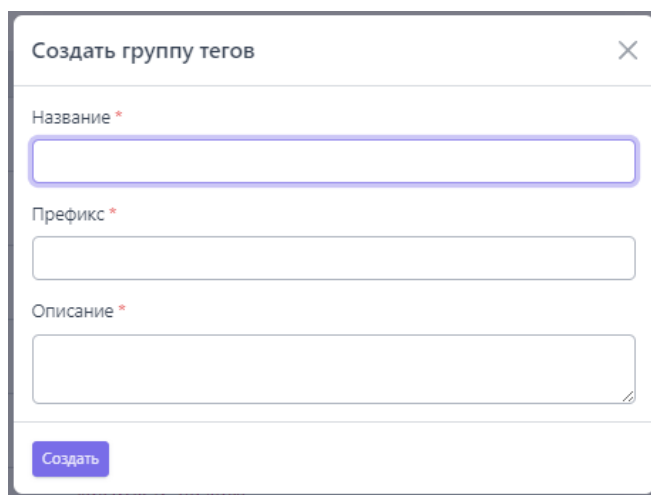


Рисунок 30 – Окно создания группы тегов

Для создания группы тегов, в данном окне требуется заполнить поля **Название**, **Префикс**, **Описание** и нажать по иконке **Создать**, после чего новая группа тегов появится в списке групп.

Для редактирования группы тегов следует в области **Управление** нажать по иконке , после чего появится окно редактирования группы, представленное на рисунке 31.

— Управление (редактировать тег , удалить тег ).

Для фильтрации информации на странице, имеется система фильтров, представленная в следующем списке:

- Название;
- Дата создания/изменения.

Для редактирования тега следует в области **Управление** нажать по иконке , после чего появится окно редактирования тега, представленное на рисунке 33.

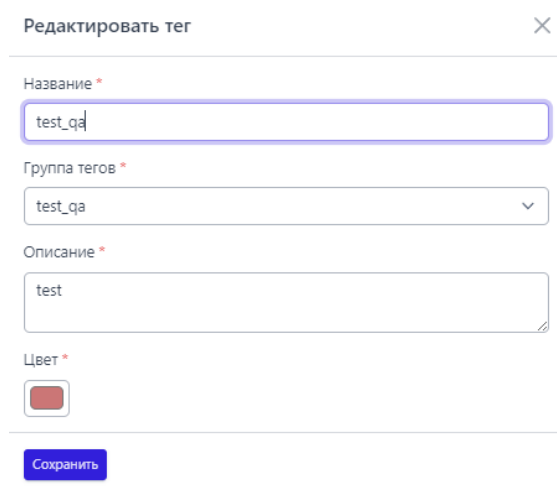
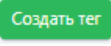


Рисунок 33 – Окно редактирования информации о теге

Для создания нового тега в данной группе следует нажать по иконке  **Создать тег**, после чего откроется окно создания тега, представленное на рисунке 34.

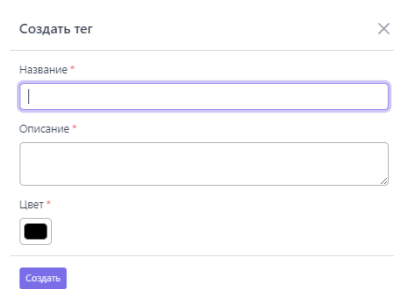


Рисунок 34 – Окно создания тега

В данном окне для создания тега следует заполнить все поля и нажать по иконке **Создать**.

Общий вид страницы **Теги** вкладки **Группы псевдонимов** представлен на рисунке 35.

Теги

Группы тегов | Группы псевдонимов

Название: Дата создания / изменения: ☒ Список ☐ Календарь

Введите значение: Все время

Показывать по: 50

☐	Название	Описание	Количество	Дата создания / Автор	Дата изменения / Автор	Управление
☐	zscxsc	zscxsc	0	25.11.2025, 12:22:55		
☐	z scxsc	zscxsc	0	25.11.2025, 12:22:55		
☐	vp-test	123	0	22.11.2025, 17:18:30	22.11.2025, 17:27:32	
☐	567u56u	u56u	0	22.09.2025, 16:53:54		
☐	По умолчанию	тест	0	24.06.2025, 15:20:22		
☐	test_for_PMI	Для тестирования работы псевдонимов	0	19.06.2025, 11:11:39		
☐	test_group1_1	для теста (удалить)	1	14.05.2025, 17:56:55	16.05.2025, 17:56:53	
☐	По умолчанию		3	24.03.2025, 18:23:28		
☐	test_group_1	Для теста	2	24.03.2025, 17:58:45	16.05.2025, 17:56:47	
☐	RST Cloud_1	RST Cloud	47	17.02.2025, 17:59:10	28.05.2025, 13:47:59	

Найдено: 10, показано с 1 по 10

Показывать по: 50

Рисунок 35 – Окно вкладки Группы псевдонимов

Таблица с полями для выбранной вкладки **Группы псевдонимов** представлена полями согласно следующему списку:

- Кнопка выбора ☐ / ☒ ;
- Название (название группы псевдонимов);
- Описание;
- Количество (количество элементов в группе);
- Дата создания/Автор;
- Дата изменения /Автор;
- Управление (редактирование группы , удаление группы).

Для удаления группы псевдонимов необходимо в поле **Управление** нажать по иконке удаления группы.

Для удаления нескольких групп псевдонимов следует пометить необходимые группы кнопкой выбора и нажать по иконке

Для создания новой группы псевдонимов требуется нажать по иконке , после чего откроется окно создания группы, представленное на рисунке 36.

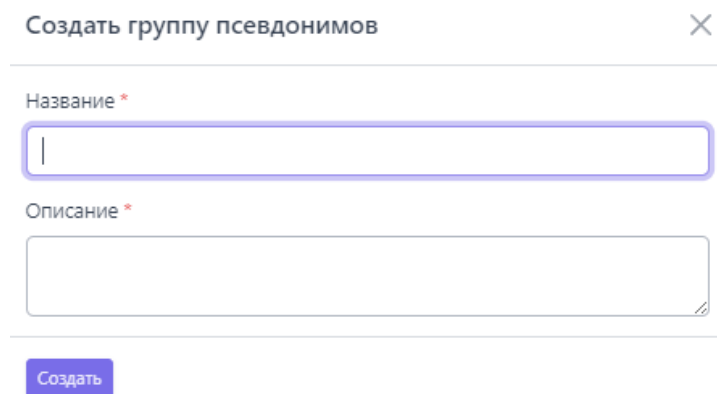


Рисунок 36 – Окно создания группы псевдонимов

Для создания группы псевдонимов в данном окне требуется заполнить поля **Название**, **Описание** и нажать по иконке **Создать**, после чего новая группа псевдонимов появится в списке групп.

Для редактирования группы псевдонимов следует в области **Управление** нажать по иконке , после чего появится окно редактирования группы, представленное на рисунке 37.

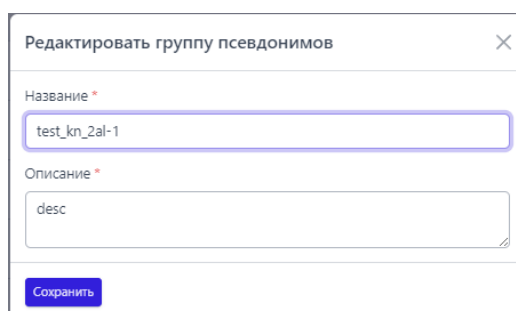


Рисунок 37 – Окно редактирования группы псевдонимов

Название группы псевдонимов на странице **Теги** вкладки **Группы псевдонимов** является активной ссылкой, при нажатии по которой открывается окно с псевдонимами данной группы (рисунок 38).

Группа псевдонимов - RST Cloud_1 Сбросить фильтры

Название: Дата создания / изменения: Список Календарь

Введите значение: Все время

Показывать по: 10

☐	Название	Тег	Дата создания / Автор	Дата изменения / Автор	Управление
☐	dock	fraud:fraud	07.05.2025, 17:36:07		
☐	hex	malware_type:worm	07.05.2025, 11:50:57		
☐	elf	fraud:phishing	07.05.2025, 11:37:20		
☐	tag1QAtest	fraud:spam	21.04.2025, 16:01:40		
☐	64bits	fraud:scareware	14.04.2025, 11:53:13		
☐	tag3	fraud:spam	09.04.2025, 17:20:38		
☐	pedill	fraud:spam	07.04.2025, 17:21:17		
☐	assembly	fraud:spam	07.04.2025, 17:18:45		
☐	wiper	malware_type:wiper	17.02.2025, 18:06:12		
☐	vulndriver	malware_type:vulndriver	17.02.2025, 18:06:05		

Найдено: 47, показано с 1 по 10

Создать псевдоним Удалить выбранные

Рисунок 38 – Окно Псевдонимы в группе псевдонимов

В данном окне информация о псевдонимах, входящих в группу, представлена в виде таблицы со следующими полями:

- Кнопка выбора ☐;
- Название;
- Тег;
- Дата создания/Автор;
- Дата изменения/Автор;
- Управление (редактировать псевдоним , удалить псевдоним).

Для фильтрации информации на странице, имеется система фильтров, представленная в следующем списке:

- Название;
- Дата создания/изменения.

Для редактирования псевдонима следует в области **Управление** нажать по иконке , после чего появится окно редактирования псевдонима, представленное на рисунке 39.

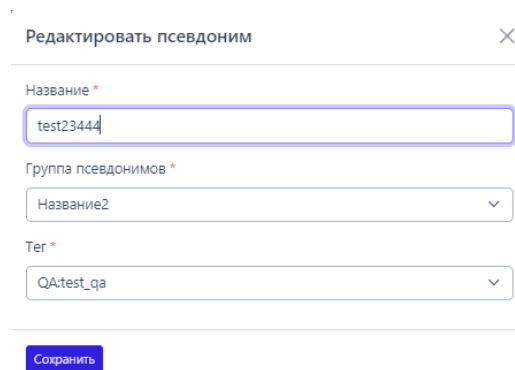


Рисунок 39 – Окно редактирования информации о псевдониме

Для создания нового тега в данной группе следует нажать по иконке , после чего откроется окно создания псевдонима, представленное на рисунке 40.

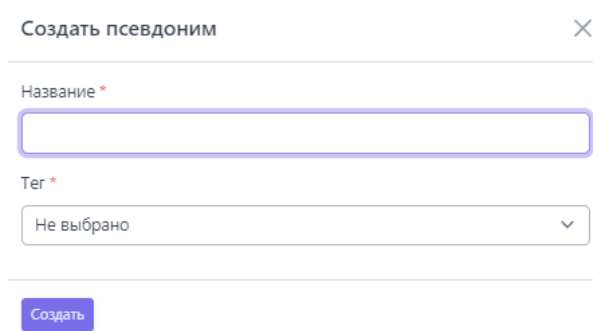


Рисунок 40 – Окно создания псевдонима

В данном окне для создания тега следует заполнить все поля и нажать по иконке **Создать**.

Механизм тегов в RT Protect TI

В механизме тегов в RT Protect TI теги из собственной библиотеки тегов могут назначаться следующим сущностям:

- 1) Непосредственно артефакту. Назначение и удаление происходит только вручную.
- 2) Источнику данных. Назначение и удаление происходят через настройки источника данных, только вручную.
- 3) Элементу источника данных. Назначение происходит только автоматически через систему псевдонимов. Описание работы системы псевдонимов см. ниже.
- 4) Анализатору. Назначение происходит при создании анализатора. Возможно редактирование тегов для уже созданных анализаторов.

В элементе источника данных также присутствует поле "Нераспознанные теги". Данное поле является чисто техническим и служит для удобства определения строк, для которых в системе не настроены псевдонимы.

В случае создания нового псевдонима нераспознанные теги с этим псевдонимом превращаются в теги, назначенные в пункте 3.

Описание работы системы псевдонимов

Псевдоним позволяет настроить сопоставление между какой-либо строкой, являющейся тегом в файле источника данных, и тегом в собственной библиотеке тегов.

Для того, чтобы заработало сопоставление тегов для элемента источников данных необходимо:

- наличие поля с тегами в самом файле источника данных. Пока что поддерживаются поля строкового массива в JSON, либо строки в JSON.

- наличие псевдонимов для встречающихся в файле источника данных вариантов тегов.

В случае, если в файле источника данных встречается строка или набор строк с тегами, для них ищутся соответствующие псевдонимы из собственной коллекции псевдонимов. Если псевдоним найден, то привязанный к нему тег записывается в поле из пункта 3 выше. Если псевдоним не найден, то строка попадает в поле "нераспознанные теги" для данного элемента источника данных. Распознанные ранее теги в дальнейшем не удаляются в случае изменения псевдонимов/изменения данных в самом источнике.

Фронтенд

На фронтенде теги из пунктов 1-3 отображаются в нескольких местах в различной комбинации, из-за чего может возникать путаница.

На странице артефакта отображаются теги, назначенные артефакту (п. 1), назначенные всем связанным источникам данных (п. 2) и элементу каждого источника данных (п. 3.). При этом редактируется только та часть тегов, которая назначена самому артефакту.

На вкладке "Внешние источники" артефакта отображаются теги, назначенные самому источнику (п. 2), и автоматически назначенные элементу источника данных (п. 3). Отдельным полем отображаются нераспознанные теги.

5.4 Аналитика

5.4.1. Активность

В разделе **Активность** в табличной форме представлена информация о последних угрозах, которые обнаружены в инфраструктуре, подключенной к сервису аналитики.

В верхней части страницы **Активность** имеются следующие активные вкладки **Артефакты**, **Источники данных**, **Организации и клиенты**.

При переходе по каждой вкладке на странице **Активность** отображается информация, соответствующая данной вкладке, при этом вкладка, на которую был произведен переход, отмечается серым цветом.

Вид страницы **Активность** в зависимости от того, по какой вкладке был произведен вход, показан на рисунках 41 - 43.

Название артефакта	Предидущий вердикт / Время	Количество обнаружений	Время последнего обнаружения
216.24.57.4	Неизвестный 21.04.2025, 09:02:53	113	21.04.2025, 13:37:27
5d7999214b0a13ef5d086ad70678ab8daef17926c24ac024d867849bc81d	Безопасный 24.03.2025, 15:23:24	11758	21.04.2025, 13:10:21
185.125.190.20	Безопасный 25.04.2024, 15:37:59	131	21.04.2025, 12:12:14
6279696c1d73024618508e9125886a26709decc05946f3729802e4bdfdb030b0	Вредоносный 21.04.2025, 11:31:18	11	21.04.2025, 11:31:18
phv5ss.com	Неизвестный 21.04.2025, 12:43:48	1	21.04.2025, 11:04:37
22873d9d5706476785e7f3c1208b5d5f56838cc0a8a2015d2b11598cc80b4	Вредоносный 10.03.2025, 10:02:46	271	21.04.2025, 10:07:13
9d4cf1e3629f92667fcd7e3f1094a7fc3cb16134994640853d7f0830af843	Неизвестный 18.04.2025, 12:28:40	2201	19.04.2025, 07:54:18
59438921c6a4a02439854c4552791bf4a0b7c12e9b0b0b040e77251521f1	Неизвестный 18.04.2025, 12:28:25	2230	19.04.2025, 07:54:18
85fe088eab7fc535c3e18c1bd76a2f3e6217f9c91a25834774588881c3f90de	Неизвестный 15.04.2025, 05:12:14	1950	18.04.2025, 16:51:52
umnyitrobel.ru		68	18.04.2025, 13:23:09

Рисунок 41 – Страница Активность вкладка Артефакты

Активность

Артефакты Организация и клиенты Источники данных

Тип артефакта: Не задан Вердикт: Вредный X Рациональный X Период регистрации (на сервере): 1 неделя

Дополнительные фильтры: Источники данных: Включить режим агрегации

График обнаружений

Название артефакта	Предыдущий вердикт / Время	Количество обнаружений	Время последнего обнаружения
216-24-67-8 RST Cloud IP Feed	Неизвестный 21.04.2025, 09:02:10	111	21.04.2025, 11:37:27
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Global SET	Безопасный 24.03.2025, 15:21:24	330	21.04.2025, 11:38:25
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Global test	Безопасный 24.03.2025, 15:21:24	326	21.04.2025, 11:38:25
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 test	Безопасный 24.03.2025, 15:21:24	332	21.04.2025, 11:38:25
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 TESTAB2	Вредоносный 21.04.2025, 11:31:58	5	21.04.2025, 11:31:58
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Abuse: MailServerBazar	Вредоносный 21.04.2025, 11:31:58	5	21.04.2025, 11:31:58
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 RST Cloud Hash Feed	Вредоносный 21.04.2025, 11:31:58	11	21.04.2025, 11:31:58
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 TestIAR	Вредоносный 21.04.2025, 11:31:58	5	21.04.2025, 11:31:58
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 RST Cloud Domain Feed	Неизвестный 21.04.2025, 12:07:40	1	21.04.2025, 11:04:17
3287395728647876c270b3c30836c6c4948a201542ab1598c6dc0c TESTABpart12	Вредоносный 11.03.2025, 10:01:46	17	21.04.2025, 10:07:13

Рисунок 42 – Страница Активность вкладки Источники данных

Активность

Артефакты Организация и клиенты Источники данных

Тип артефакта: Не задан Вердикт: Вредный X Рациональный X Период регистрации (на сервере): 1 неделя

Дополнительные фильтры: Организация: Не задан Клиенты: Не задан

График обнаружений

Степень обнаружений по клиентам: 41

Степень обнаружений по организации: 41

Legend: ● IP-адрес (16) ● IP-информация (17) ● Mail (20) (20) ● IP-информация (16) ● Тестовый сервер (20) (20) ● IP-информация (17)

Название артефакта	Предыдущий вердикт / Время	Количество обнаружений	Время последнего обнаружения
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Неизвестный 21.04.2025, 09:02:10	5	21.04.2025, 11:37:27
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Безопасный 24.03.2025, 15:21:24	2086	21.04.2025, 11:38:25
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Безопасный 24.03.2025, 15:21:24	29	21.04.2025, 11:38:25
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Безопасный 21.04.2025, 11:31:58	11	21.04.2025, 11:31:58
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Неизвестный 21.04.2025, 11:31:58	1	21.04.2025, 11:04:17
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Вредоносный 21.04.2025, 10:01:46	212	21.04.2025, 10:07:13
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 RT-информация (Безопасность (Тестовый сервер (20K))	Неизвестный 10.04.2025, 11:03:05	2176	10.04.2025, 07:11:08
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 RT-информация (Безопасность (Тестовый сервер (20K))	Неизвестный 10.04.2025, 11:03:05	2226	10.04.2025, 07:11:08
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Неизвестный 11.03.2025, 01:13:14	1807	10.04.2025, 10:11:08
827692146ba318756086a5a79a79a06ac17326c24cc0240c79693b16 Mail-информация (Email (20K (20K))	Неизвестный 11.03.2025, 01:13:14	17	10.04.2025, 11:38:25

Рисунок 43 – Страница Активность вкладки Организации и клиенты

Таблица имеет следующие поля:

- **Название артефакта** (в данном столбце в зависимости от типа артефакта отображается различная информация: контрольная сумма файла-угрозы в формате SHA-256, IP-адреса, доменные имена, URL);
- **Предыдущий вердикт/Время** (предыдущий вердикт по артефакту, а также дата и время внесения вердикта);

- **Количество обнаружений** (отображается общее количество обнаружений по данному артефакту);
- **Время последнего обнаружения** (отображается время последнего обнаружения файла с угрозой).

Для удобства и наглядного отображения вердикта по артефакту в столбце **Название артефакта** информация отображается разным цветом шрифта:

- [630ae106a99ae7da5d8dd33e7704b27701f65](#) – вредоносный артефакт (шрифт красного цвета);
- [02f0c498bb4e5f62722ab5e8a63f5b3779db88ef](#) – безопасный артефакт (шрифт зеленого цвета);
- [B73753C4C69A03F9A3E09F121B6599D77B1A48E0247F9B71856572555E1FE12B](#) – неизвестный артефакт (шрифт серого цвета);
- [61F897ED69646E0509F6802F82D7C5E88C3E3B93C4CA86942E24D203AA878863](#) – подозрительный артефакт (шрифт оранжевого цвета).

В столбце **Название артефакта** слева от артефакта имеется иконка , показывающая в процентах общий вердикт для данного артефакта. В примере, приведенном выше, иконка показывает, что артефакт является вредоносным на 86.25 процента.

В столбце **Название артефакта** справа от информации, характеризующей артефакт (контрольной суммы файла, IP-адреса, или доменного имени), имеется иконка , нажав ЛКМ по которой, можно скачать данную информацию в буфер обмена.

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы, представленное на рисунке 44.

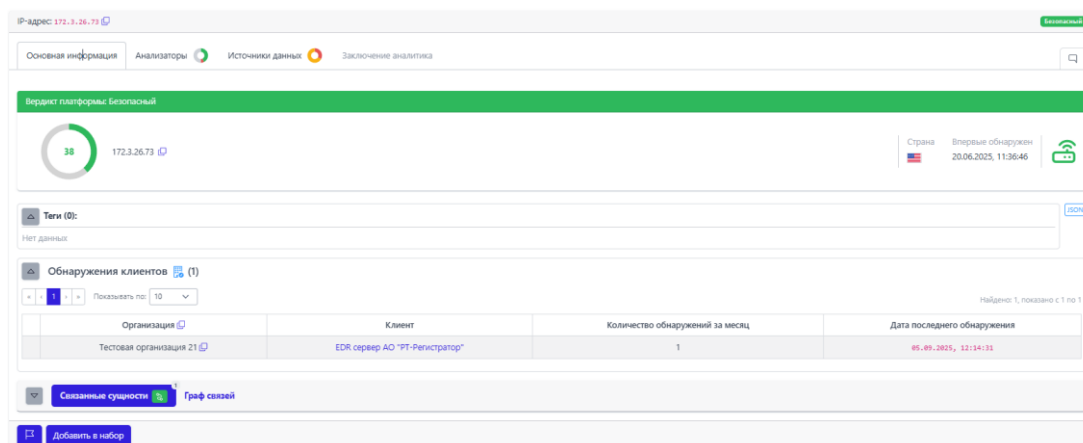


Рисунок 44 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

- 1) Область краткой информации об угрозе;
- 2) Область вкладок (Основная информация, Анализаторы, Источники данных, Заключение аналитика);
- 3) Область основной информации отчета об угрозе;
- 4) Область расширенной аналитики (Теги, Обнаружения клиентов, Связанные сущности);

В области краткой информации отображена информация об анализируемой угрозе в зависимости от типа артефакта (контрольная сумма проанализированного файла в формате SHA-256, IP-адрес, доменное имя, URL и вердикт TI-портала по данной угрозе).

В области **Анализаторы** показан список анализаторов.

При наведении указателя мыши на иконку  , рядом с названием вкладки, открывается окно показывающее статусы отчетов полученных для данного артефакта (рисунок 45).

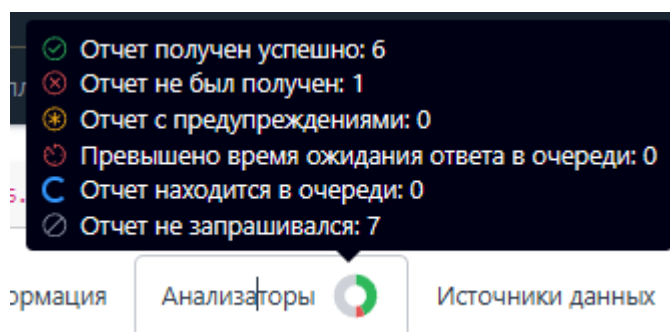


Рисунок 45 – Статусы отчетов по артефакту

При наведении указателя мыши на Название анализатора и нажатия ЛКМ, открывается отчет от анализатора по артефакту.

В области **Источники данных** отображаются отчеты от источников данных по артефакту.

В области названия вкладки **Источники данных** имеется иконка  , при наведении на которую указателя мыши открывается окно с указанием вердиктов по артефакту полученных от источников данных (рисунок 46).

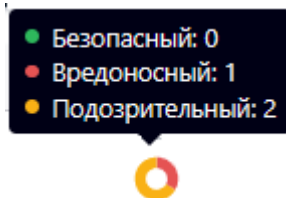


Рисунок 46 – Вердикты по артефакту

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 47.

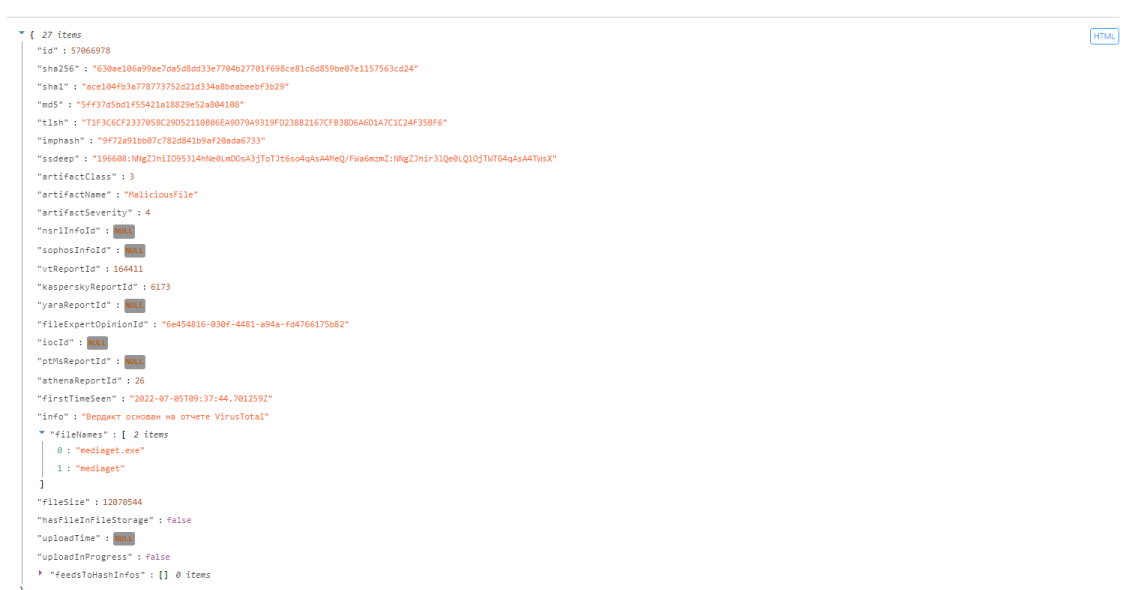
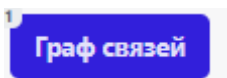


Рисунок 47 – Информация отчета об артефакте в формате JSON

При нажатии по иконке  в поле **Обнаружения клиентов**, показывается таблица в которой отображается список клиентов организации и количество обнаружений артефакта за месяц.

При нажатии по иконке  в поле **Связанные сущности** открывается таблица в которой показаны сущности связанные с рассматриваемым артефактом.

В области связанные сущности имеется иконка  нажав по которой ЛКМ можно привязать к артефакту различные сущности (другие артефакты, уязвимости, организации, отчеты и другое).



При нажатии по иконке , открывается область отображающая граф связей для данного артефакта.

На странице отчета по артефакту имеется иконка для создания заявки на корректировку вердикта по



артефакту и иконка для добавления артефакта в набор

Добавить в набор

Для того чтобы добавить артефакт в набор, нужно указать тип набора и название набора.

Для фильтрации информации на странице **Активность** вкладка **Артефакты** предусмотрена система основных фильтров, представленная в следующем списке:

- **Тип артефакта** (файл, IP-адрес, доменное имя, URL);
- **Вердикт** (неизвестный, безопасный, вредоносный, подозрительный);
- **Период регистрации (на сервере)** может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца) либо в виде календаря (начальная и конечная даты);
- Теги.

Также имеется система дополнительных фильтров, которая по умолчанию скрыта. Для открытия поля



с дополнительными фильтрами требуется нажать по иконке в области **Дополнительные фильтры**.

Имеются следующие дополнительные фильтры:

- Артефакт;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Предыдущий вердикт;
- Время последнего изменения вердикта;
- Вердикт.

На странице **Активность** вкладки **Клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 48).



Рисунок 48 – Область графического отображения информации по обнаруженным угрозам вкладки «Артефакты»

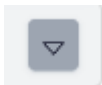
В данной области для наглядности представления информации имеются графики, отображающие следующие статистические данные:

- статистика обнаружений по типам;
- Статистика обнаружений по вердиктам.

Для фильтрации информации на странице **Активность** вкладки **Клиенты** предусмотрена система фильтров, представленная в следующем списке:

- **Тип артефакта** (файл, IP-адрес, доменное имя, URL);
- **Вердикт** (неизвестный, безопасный, вредоносный, подозрительный);
- **Период регистрации (на сервере)** может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца), либо в виде календаря (начальная и конечная даты);
- Клиенты.

Также имеется система дополнительных фильтров, которая по умолчанию скрыта. Для открытия поля

с дополнительными фильтрами требуется нажать по иконке  в области **Дополнительные фильтры**.

Имеются следующие дополнительные фильтры:

- Артефакт;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Предыдущий вердикт;
- Время последнего изменения вердикта;
- Вердикт.

5.4.2. Заключение аналитика

Общие сведения

В разделе **Заключение аналитика** в табличной форме представлена информация о зарегистрированных на портале заключениях аналитика.

Заключение аналитика – это своего рода основополагающий вердикт об артефакте, который выносится аналитиком на основании анализа вердиктов, полученных от источников данных.

Проанализировав на странице **Активность** отчеты по проверке артефактов от различных вендоров, аналитик результирует общий вердикт по артефакту и, если требуется, выносит свой вердикт об опасности артефакта.

Также аналитик может поставить время актуальности, т.е. время, в течение которого вердикт по артефакту, указанный им, будет актуальным.

Общий вид страницы **Заключения аналитика** зависит от выбранной вкладки (подсвечена серым цветом).

Общий вид страницы **Заклучения аналитика** вкладки **Заклучения аналитика** представлен на рисунке

49.

Артефакт	Вердикт	Количество обнаружений	Комментарий	Время актуальности	Дата создания / Автор	Дата обновления / Пользователь	Действия
1895f3137aefcf96c82b0c0d9a6cf0d6a8b03116233b276312a414c39758209f	Подозрительный	1	для теста 3	День	04.08.2025, 15:07:09		
68486378a9804888f3a4f4590a826c23e3f0488e	Подозрительный	1	для теста 2	День	04.08.2025, 15:07:27		
53262089459f426382f41d2735818f1	Подозрительный	1	для теста 1	День	04.08.2025, 15:07:07		
31464a6a667fc9b1d01311b233294ca	Подозрительный	0	для теста QA	День	01.08.2025, 16:44:13		
62f685f3a5e6d286c186c8b87b8d89f39a3d559	Подозрительный	0	для теста QA	День	01.08.2025, 16:43:17		
25ea9de82dc33b18d9751580b0b2f39376058a6f6c486475a272d78fe33a	Подозрительный	0	для теста QA	День	01.08.2025, 16:42:41		
18.11.12.17	Вредоносный	0	t_test	День	01.08.2025, 14:38:06	01.08.2025, 14:39:13	
18.11.12.16	Вредоносный	0	t_test	День	01.08.2025, 14:38:06	01.08.2025, 14:39:13	
18.11.12.15	Вредоносный	0	t_test	День	01.08.2025, 14:38:06	01.08.2025, 14:39:13	
18.11.12.14	Вредоносный	0	t_test	День	01.08.2025, 14:38:06	01.08.2025, 14:39:13	

Рисунок 49 – Страница **Заклучения аналитика**

В таблице имеются следующие поля:

- Артефакт (в столбце отображается артефакт, для которого имеется заключение аналитика);
- Вердикт (в столбце отображается вердикт для артефакта);
- Количество обнаружений;
- Комментарий;
- Время актуальности (отображается время, показывающее, сколько будет актуален вердикт (заключение аналитика) по данному артефакту;
- Дата создания/Автор;
- Дата обновления/Пользователь;
- Действия (редактирование, удаление заключения аналитика).

Для фильтрации информации на странице имеется система фильтров, представленная согласно следующему списку:

- Вердикт (не задано, безопасный, вредоносный, подозрительный);

- Время актуальности (не задано, день, неделя, месяц, три месяца, бесконечно);
- Тип артефакта (файл, ip-адрес, доменное имя, URL, Email);
- Комментарий;
- Автор/пользователь;
- Временной период.



В столбце **Артефакт** слева от артефакта имеется иконка , показывающая в процентах вердикт анализатора для данного артефакта. В примере, приведенном выше, иконка показывает, что артефакт является вредоносным на 86.25 процента.

В столбцах **Артефакт** и **Вердикт** для наглядности представления записи выделены различными цветами согласно следующему списку:

- [630ae106a99ae7da5d8dd33e7704b27701f65](#) – вредоносный артефакт (шрифт красного цвета);
- [02f0c498bb4e5f62722ab5e8a63f5b3779db88ef](#) – безопасный артефакт (шрифт зеленого цвета);
- [61f897ED69646E0509F6802FB2D7C5E88C3E3B93C4CA86942E24D203AA878863](#) – подозрительный артефакт (шрифт оранжевого цвета).

В столбце **Артефакт** справа от информации, характеризующей артефакт (контрольной суммы файла, IP-адреса, или доменного имени), имеется иконка , нажав ЛКМ по которой, можно скачать данную информацию в буфер обмена.

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы по данному артефакту.

Для редактирования заключения аналитика необходимо в столбце **Действия** нажать по иконке , при этом открывается окно, представленное на рисунке 50.

Редактировать заключение аналитика

Артефакт *

Вердикт *

Комментарий *

Время актуальности *

Редактировать

Рисунок 50 – Окно редактирования заключения аналитика

В данном окне после редактирования информации по заключению требуется нажать по иконке **Редактировать** после чего окно редактирования исчезнет, и появится короткое всплывающее сообщение с надписью **Заключение обновлено**.

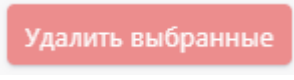
Для удаления заключения аналитика в столбце **Действия** требуется нажать по иконке , после чего появится окно, в котором следует подтвердить (либо отменить) действие удаления (рисунок 51).

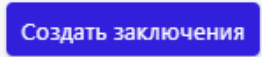
Подтверждение действия

Удаление заключения аналитика

Выполнить Отмена

Рисунок 51 – Окно подтверждения действия удаления заключения аналитика

Для удаления нескольких записей на странице необходимо отметить кнопкой выбора запись (либо несколько записей), которые необходимо удалить, после чего нажать по иконке . Для завершения операции следует в окне подтверждения подтвердить либо отменить запись.

Для создания нового заключения аналитика требуется нажать по иконке , после чего откроется окно создания заключения, представленное на рисунке 52.

Создать заключения

Артефакт ⓘ *

Признак создания графа "Звезда"

Вердикт *

Безопасный

Комментарий *

Время актуальности *

День

Перезаписать ранее добавленные заключения

Добавить

Рисунок 52 – Окно добавления заключения аналитика

В списке артефактов, для которых добавляется заключение аналитика, можно указать разные типы артефактов и после добавления заключения аналитика оно будет добавлено для каждого типа артефакта.

При установке галочки в поле «Перезаписать ранее добавленные заключения», заключение, написанное в данный момент изменится, если оно уже имелось для данного артефакта.

После заполнения полей следует нажать по иконке **Добавить**. После подтверждения действия по добавлению новое заключение аналитика будет отображаться в списке на странице **Заключения аналитика**.

Вкладка Заявки

На странице **Заключения аналитика** вкладка **Заявки** пользователь может принять или отклонить заявку на корректировку вердикта заключения аналитика по артефактам.

Общий вид страницы **Заключения аналитика** вкладки **Заявки** представлен на рисунке 53.

Заклучения аналитика

Сбросить фильтры

Заклучения аналитика

Заявки

Вердикт

Статус

Комментарий

Не задан

Активна

Введите значение

Артефакт

Временной период

Список Календарь

Введите значение

Всё время

10

Найдено: 58, показано с 1 по 10

☐	Артефакт	Тип артефакта	Статус	Вердикт	Комментарий	Дата создания / Автор	Дата обновления / Пользователь	Действия
☐	test@mail.com	@	Активна	Подозрительный	тест	06.10.2025, 12:02:46		
☐	https://habr.com/ru	globe	Активна	Подозрительный	для теста	06.10.2025, 12:02:19		
☐	vp-test-domain-or-is-some-value-not-check.tutu	globe	Активна	Безопасный	vp-test-check-verdict-claim-please	03.10.2025, 16:01:35 v.pavichuk@vr-protect.ru		
☐	0a72e68778018c0b1c453c1998a4a19a4eaf6659f4774cf68484990a83259581	document	Активна	Безопасный	бум	03.10.2025, 15:54:13		
☐	7840fc68717272095cc13e716a4fdaa	document	Активна	Безопасный	для теста	03.10.2025, 12:00:15		
☐	test@mail.com	@	Активна	Безопасный	для теста	03.10.2025, 12:00:15		
☐	https://habr.com/ru	globe	Активна	Безопасный	для теста	03.10.2025, 12:00:15		
☐	8.8.8.8	ip	Активна	Безопасный	для теста	03.10.2025, 12:00:14		
☐	abr.ru	globe	Активна	Безопасный	для теста 1	03.10.2025, 12:00:14		
☐	test@mail.com	@	Активна	Безопасный	для теста	28.09.2025, 18:14:16		

Рассмотреть заявки

Рисунок 53 – Страница Заклучения аналитика вкладки Заявки

Информация на странице представлена в виде таблицы со следующими полями:

- Кнопка выбора;
- Артефакт (отображается артефакт);
- Тип артефакта (с помощью иконок отображается тип артефакта);
- Статус (отображается статус заявки: Активна, Отклонена, Одобрена);
- Вердикт (отображается вердикт по артефакту);
- Комментарий (отображается комментарий);
- Дата создания/Автор (отображается дата создания заявки и ее автор);
- Дата обновления/Пользователь (отображается дата изменения заявки и пользователь, производивший изменения);
- Действия (отображается иконка для рассмотрения заявки).

Для фильтрации информации на странице используется система фильтров, представленная в следующем списке:

- Вердикт;
- Статус;

- Автор/Пользователь;
- Комментарий;
- Артефакт;
- Временной период.

Для артефактов со статусом заявки «Активна», в поле **Действие**, пользователь может нажать по иконке



для того, чтобы рассмотреть заявку.

Окно рассмотрения заявки на корректировку вердикта по артефакту представлено на рисунке 54.

Заявка на корректировку вердикта

Артефакт *

cbg.com

Вердикт *

Подозрительный

Комментарий *

для теста (удалить)

Время актуальности *

День

Принять

Отклонить

Рисунок 54 – Окно рассмотрения заявки на корректировку вердикта по артефакту

В данном окне пользователь может либо принять, либо отклонить заявку на корректировку вердикта.

После нажатия по соответствующей иконке статус заявки по артефакту в таблице изменится и в таблице заключения аналитика по данному артефакту будет выставлен вердикт, который указан в заявке, если заявка была принята, либо останется прежним, если заявка была отклонена.

Также действие по рассмотрению заявки можно выполнить, выбрав кнопкой выбора несколько активных заявок и нажав по иконке

Рассмотреть заявки

5.4.3. Анализаторы

Анализаторы представляют собой функционал для расширения возможностей анализа артефактов с помощью программы RT Protect TI.

Процедура создания анализаторов описывается в отдельном документе.

В общем случае можно сказать, что сущность анализаторов – это сложно структурированный созданный инструмент по анализу артефактов, на основе заданных при написании анализатора правил.

Общий вид страницы **Анализаторы** зависит от вкладки, которая активна на данный момент.

Общий вид страницы **Анализаторы** вкладки **Активные интеграции** представлен на рисунке 55.

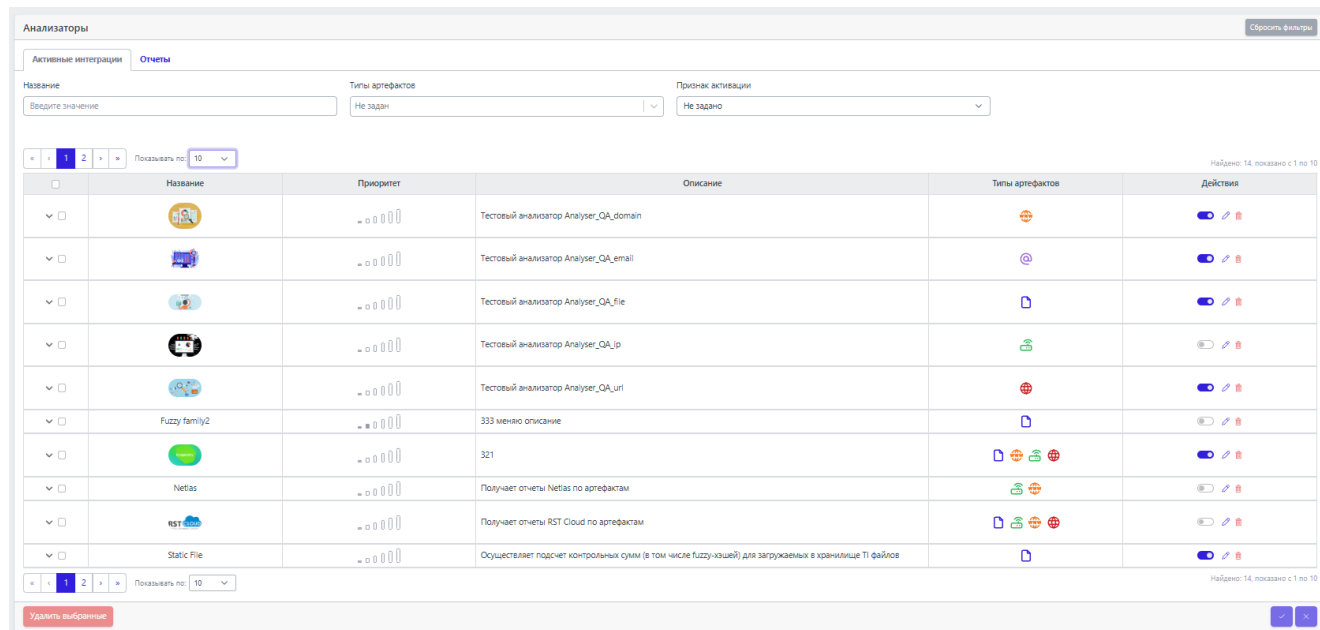


Рисунок 55 – Общий вид страницы Анализаторы вкладки Активные интеграции

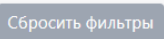
Информация на странице «Анализаторы» вкладки «Активные интеграции» представлена в виде таблицы со следующими полями:

- Иконка для раскрытия информации по анализатору ();
- Кнопка выбора (☐ / ☒);
- Название анализатора;
- Приоритет;
- Описание;
- Тип артефактов;
- Действия.

Для фильтрации информации на странице имеются следующие фильтры:

- Название;
- Признак активации (не задано, активировано, не активировано);
- Типы артефактов (Файл, IP-Адрес, доменное имя, URL, Email).

На странице «Анализаторы» имеются следующие иконки:

-  (при нажатии сбрасываются выставленные фильтры на странице);
-  (после нажатия кнопки выбора напротив анализатора, происходит удаление выбранного анализатора);
-  /  (активирует/деактивирует выбранные анализаторы, т.е. делает анализ артефактов по данному анализатору активным, или временно отключенным).

В поле «Типы артефактов» в виде иконок отображаются типы артефактов, проверяемые данным анализатором.

Имеются следующие типы артефактов:

-  (Почтовый адрес);
-  (Файл);
-  (Доменное имя);
-  (IP адрес);
- Диапазон IP адресов;
-  (Веб адрес).

В поле «Действия» с помощью иконок можно выполнить следующие действия:

-  /  (Активировать/Деактивировать анализ по выбранному анализатору);
-  (Редактировать информацию по анализатору);
-  (Удалить анализатор).

При выполнении действий по удалению анализатора, а также активации/деактивации анализатора, требуется подтвердить действие в всплывающих окнах, представленных на рисунках 56-58.

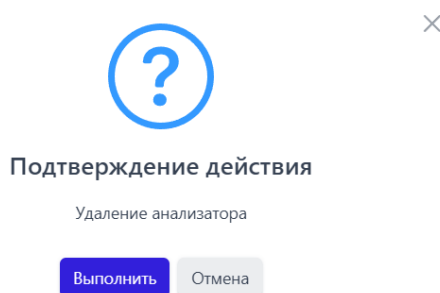


Рисунок 56 – Подтверждение действия удаления анализатора

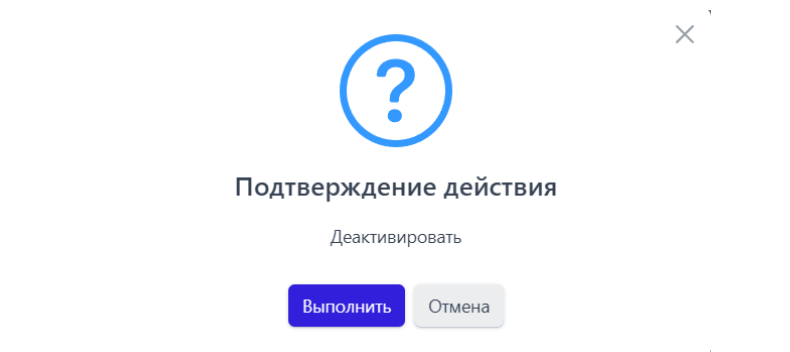


Рисунок 57 – Подтверждение действия деактивации анализатора

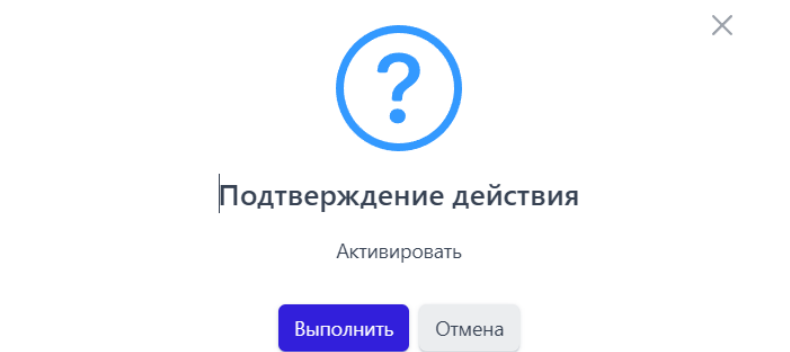


Рисунок 58 – Подтверждение действия активации анализатора

При нажатии по иконке редактирования анализатора, открывается окно, представленное на рисунке 59.

Редактировать анализатор

Название *

Analyser_QA_email

Приоритет *

Минимальный

Время актуальности получаемых отчетов (в днях) *

1

Группа псевдонимов тегов *

По умолчанию

Описание

Тестовый анализатор Analyser_QA_email

☒ Автоматически запрашивать отчет по артефакту при открытии

☒ Анализатор доступен только организациям-владельцам платформы

Загрузить иконку анализатора

Удалить иконку анализатора

Сохранить

Рисунок 59 – Окно редактирования информации по анализатору

В данном окне можно изменить следующие параметры работы анализатора:

- Название анализатора;
- Приоритет;
- Время актуальности получаемых отчетов в днях;
- Группу псевдонимов тегов;
- Описание анализатора;
- Загрузить или удалить иконку для анализатора;
- Автоматически запрашивать отчет по артефакту при открытии;
- Анализатор доступен только организациям-владельцам платформы.

После редактирования информации требуется нажать по иконке «Сохранить».

При нажатии по иконке, раскрывающей информацию по анализатору, открывается окно, представленное на рисунке 60.

	Analyser_test	09.04.2025, 14:05:02	17.04.2025, 12:14:26 homer@simpson.ru	   	Analyser test5	  
Поддерживаемые типы артефактов		Файл, Доменное имя, IP-адрес, URL, Email				
Максимальное время анализа артефакта (в минутах)		5				
Для работы анализатора требуется загруженный файл		Нет				
Время актуальности получаемых отчетов (в днях)		5				
Автоматически запрашивать отчет по артефакту при открытии		Да				
Название группы псевдонимов		По умолчанию				

Рисунок 60 – Информация по анализатору

Отчеты

В разделе **Анализаторы** вкладки **Отчеты** в табличной форме представлена информация о проверенных анализаторами артефактах.

Общий вид страницы представлен на рисунке 61.

Анализаторы

Активные интеракции

Отчеты

Анализатор

Типы артефактов

Дата создания

Актуальность

Признак ошибки

Не задан

Не задан

начальная дата

конечная дата

Не задано

Не задан

Вердикт анализатора

Минимум

Максимум

Сбросить

Применить

-100

100

1

2

3

4

...

Показать по 10

Артефакт

Анализатор

Статус

Вердикт анализатора

Время обращения

Действия

5b06f4c4b434c3a13b8c9ab7c3b0f73ab0914590b323e8611214703c7b78081

20.05.2025, 10:50:00

Открыть

5b06f4c4b434c3a13b8c9ab7c3b0f73ab0914590b323e8611214703c7b78081

20.05.2025, 10:50:00

Открыть

5b06f4c4b434c3a13b8c9ab7c3b0f73ab0914590b323e8611214703c7b78081

Не задан

Не задан

70

20.05.2025, 10:51:20

Открыть

3a0982a8b409dbcc8fa780f63115595f5e30764d9386453f6c452ae487087a1

20.05.2025, 10:50:00

Открыть

3a0982a8b409dbcc8fa780f63115595f5e30764d9386453f6c452ae487087a1

20.05.2025, 10:50:00

Открыть

912157e18808206642096c1a8f98793752b36c0b0f53a0d380779acc316021c

20.05.2025, 10:50:00

Открыть

912157e18808206642096c1a8f98793752b36c0b0f53a0d380779acc316021c

20.05.2025, 10:50:00

Открыть

3a0982a8b409dbcc8fa780f63115595f5e30764d9386453f6c452ae487087a1

20.05.2025, 09:50:44

Открыть

3a0982a8b409dbcc8fa780f63115595f5e30764d9386453f6c452ae487087a1

33 ошибки

100

20.05.2025, 09:50:57

Открыть

3a0982a8b409dbcc8fa780f63115595f5e30764d9386453f6c452ae487087a1

1511

10

20.05.2025, 09:50:22

Открыть

1

2

3

4

...

Показать по 10

Найдено: 4253, показаны с 1 по 10

Найдено: 4253, показаны с 1 по 10

Рисунок 61 – Окно раздела Анализаторы вкладки Отчеты

В таблице имеются следующие поля:

- **Артефакт** (в столбце отображается информация о проверенном артефакте в зависимости от типа артефакта (хеш сумма, IP-адрес, доменное имя, URL);
- **Анализатор** (в столбце отображается анализатор, которым был проверен артефакт);
- **Статус** (в столбце отображается информация о получении отчета (отчет получен успешно, отчет не был получен, отчет находится в очереди));
- **Вердикт анализатора** (отображается вердикт по артефакту, полученный от анализатора, например,  означает, что артефакт безопасен на 100 %);
- **Время обращения** (время, в которое был запрошен отчет);
- **Действия** (отображается иконка для просмотра информации по отчету анализатора).

Информация об артефакте отображается разными цветами:

- шрифт красного цвета (артефакт является вредоносным);
- шрифт зеленого цвета (артефакт является безопасным);
- шрифт серого цвета (неизвестный артефакт);
- шрифт оранжевого цвета (артефакт является подозрительным).

В столбце **Артефакты** слева от информации об артефакте имеется иконка , показывающая общий вердикт платформы, характеризующий артефакт, т.е. в данном примере артефакт вредоносный на 100%.

Над таблицей для фильтрации информации имеются следующие фильтры:

- **Анализатор** (Название анализатора);
- Тип артефакта;
- Дата создания;
- **Вердикт отчета** (Минимальное/Максимальное значения вердикта в границах от -100 (артефакт полностью безопасен), до 100 (артефакт полностью вредоносен);
- Артефакт;
- **Актуальность** (не задано, актуальный, не актуальный);
- **Признак ошибки** (не задано, не установлен, установлен).

Статус отчета от анализатора отображается следующими иконками:

—  отчет по артефакту получен с ошибками (краткое описание ошибок приведено во всплывающем окне при наведении на иконку);

—  отчет не получен, превышено время ожидания ответа в очереди;

—  отчет не был получен (при наведении на иконку выводится статус и код ошибки);

—  отчет получен успешно.

Для просмотра отчета по артефакту нужно нажать по иконке .

Страница отчета анализатора по артефакту представлена на рисунке 62.

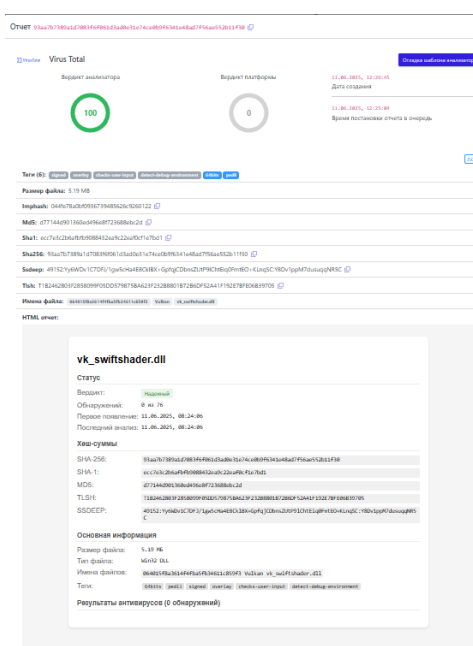


Рисунок 62 – Страница отчета по артефакту

В области **Теги** на странице отчета, полученного от анализатора, можно создать псевдоним для тега, который характерен для артефакта по данному анализатору. Нажав в поле **Теги** на имя тега, например, , откроется окно, представленное на рисунке 63.

В поле **HTML-отчет** представлено отображение HTML вида отчета по артефакту, пришедшее от анализатора.

Более подробная информация по написанию анализатора, редактированию вида HTML-отчета и работе с анализаторами описана в отдельном документе инструкции.

Отладка шаблона отчета может быть использована для предварительной визуализации в рамках разработки HTML-отчета анализатора.

5.4.4. Граф связей

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 65.

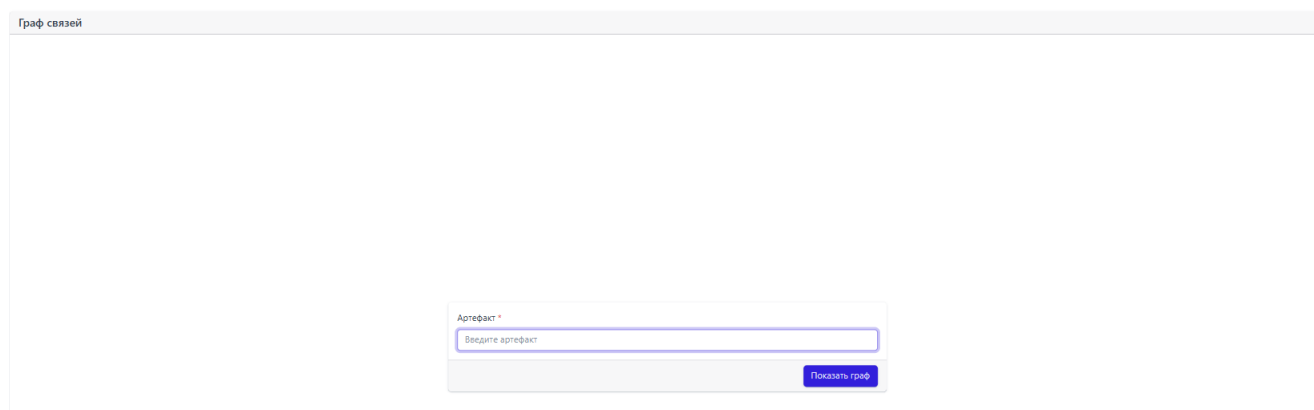


Рисунок 65 – Общий вид пустой страницы «Граф связей»

В поле артефакт следует указать артефакт, для которого необходимо построить граф.

Пример отображения графа после заполнения поля артефакта в виде IP-адреса представлен на рисунке 66.



Рисунок 66 – Отображение графа связей для артефакта типа ip-адрес

При наведении указателя мыши на элемент графа и нажатии ЛКМ открывается окно, представленное на рисунке 67.

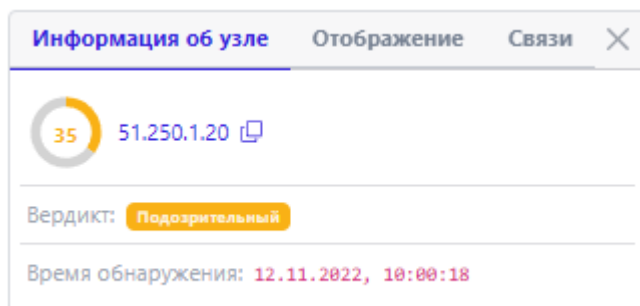


Рисунок 67 – Информация о элементе графа

В окне имеется информация об элементе графа.

При переходе во вкладку Отображение открывается информация о сущностях, связанных с данным элементом графа.

При нажатии по иконке  можно открыть на графе связи сущности с другим элементом графа.

При переходе во вкладку Связи открывается область где показаны связи с другими элементами графа.

На странице графа связей имеются следующие иконки:

- Изменение размера отображения графа (увеличение/ уменьшение)   ;
- Поиск  ;
-  (изменение глубины графа и отображения артефактов и типов связей).

При выборе значения глубины графа отличного от 1, связи выбранной ноды будут обновлены при клике на нее.

5.4.5. Yara-правила

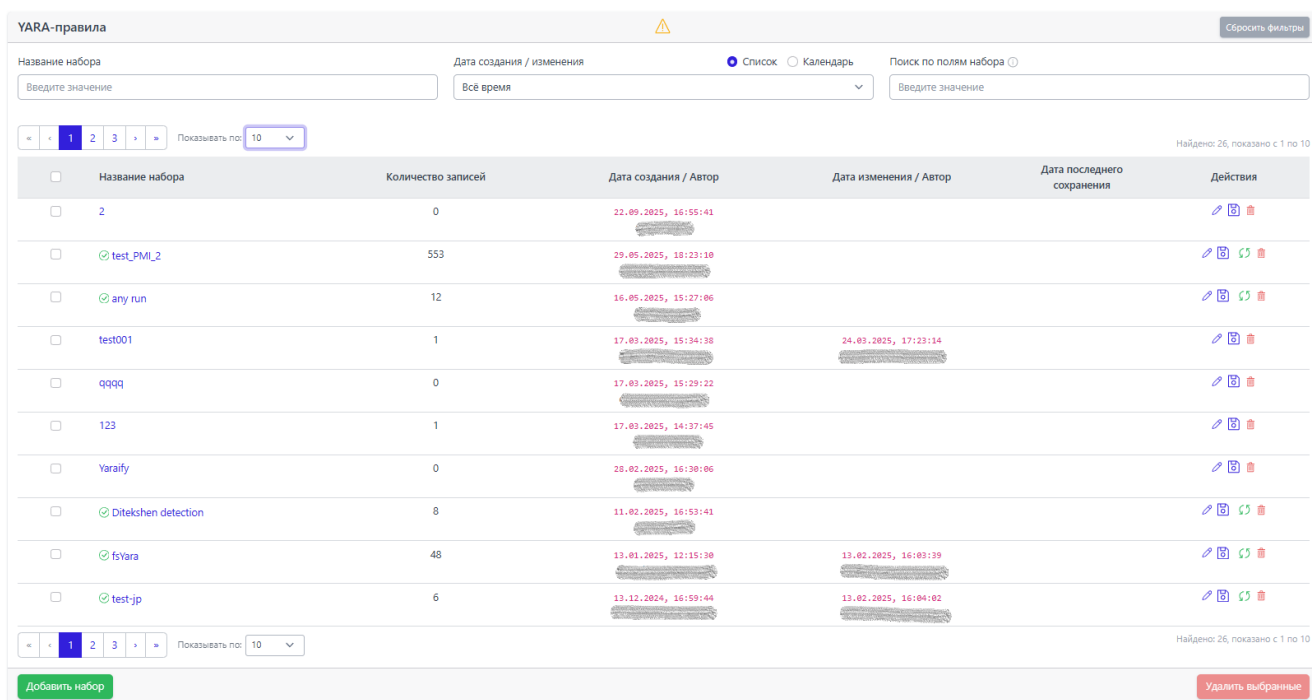
Общая информация

Правила, указанные в разделе **Yara-правила**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа вредоносных файловых сигнатур. Пользователи сервера аналитики могут создавать наборы с правилами, импортировать их из CSV-файлов, а также экспортировать в CSV-файл. Добавляемые YARA-файлы используются движком YARA внутри TI-платформы для проверки загружаемых через главную страницу или API файлов.

Наборы Yara-правил

Страница с наборами YARA-правил (рис. 68) открывается при выборе на панели слева раздела **Yara-правила** и включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- фильтры Название набора и Показывать по;
- таблица с наборами YARA-правил;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы.



Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
2	0	22.09.2025, 16:55:41			 
test_PMI_2	553	29.05.2025, 18:23:10			 
any run	12	16.05.2025, 15:27:06			 
test001	1	17.03.2025, 15:34:38	24.09.2025, 17:23:14		 
qqqq	0	17.03.2025, 15:29:22			 
123	1	17.03.2025, 14:37:45			 
Yaraify	0	28.02.2025, 16:30:06			 
Ditekshen detection	8	11.02.2025, 16:53:41			 
fsYara	48	13.01.2025, 12:15:30	13.02.2025, 16:03:39		 
test-jp	6	13.12.2024, 16:59:44	13.02.2025, 16:04:02		 

Рисунок 68 – Наборы Yara-правил

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Название набора;
- **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Дата создания/Изменения.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Создать набор** (см. рисунок 69) ввести название нового набора YARA-правил. Если требуется, чтобы набор экспортировался в YARA-правила системы RT Protect EDR, необходимо поставить галочку в соответствующей строчке ниже строки названия набора.

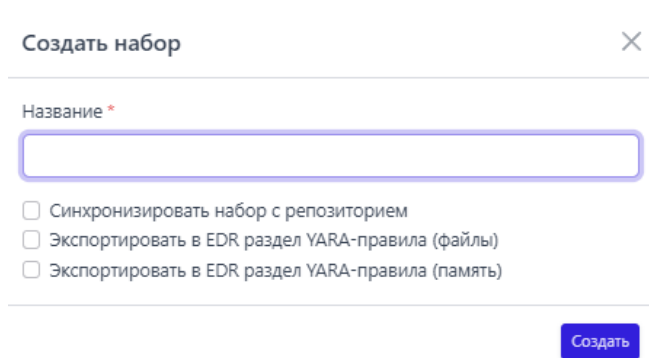


Рисунок 69 – Создать набор YARA-правил

Для завершения операции необходимо нажать кнопку **Создать**.

При этом в списке наборов на странице **YARA-правила**, набор, который будет экспортироваться в EDR, будет помечен иконками YARA-правил для файлов  и YARA-правил для памяти .

Для удаления набора необходимо нажать кнопку **Удалить** () или **Удалить выбранные наборы**.

При нажатии в поле **Действия** по иконке  открывается окно для редактирования информации о наборе, представленное на рисунке 70.

Редактировать набор

Название набора *

Yara-rules repo

Ссылка на репозиторий ⓘ *

<https://github.com/Yara-Rules/rules/tree/master>

☒ Признак рекурсивной синхронизации репозитория

Период обновления набора *

Месяц

☒ Синхронизировать набор с репозиторием

☐ Экспортировать в EDR раздел YARA-правила (файлы)

☐ Экспортировать в EDR раздел YARA-правила (память)

Сохранить

Рисунок 70 – Редактирование набора YARA-правил

В данном окне можно изменить название набора правил, изменить ссылку на репозиторий, откуда будут заимствоваться правила, а также, указав параметр **Признак рекурсивной синхронизации репозитория**, обозначить, что репозиторий будет обновляться именно из той папки, что стоит в конечном обозначении ссылки на репозиторий. Синхронизация набора с репозиторием будет производиться согласно периоду обновления набора, указанному в данном окне.

Принудительно синхронизировать набор и репозиторий в данный момент, можно, нажав в столбце

Управление по иконке  .

При нажатии по иконке  в поле действия можно сохранить набор в файл экспорта.

Страница «YARA-правила»

При нажатии ЛКМ на имени набора на странице YARA-правила, открывается страница **YARA-правила** для выбранного набора (рис. 71).

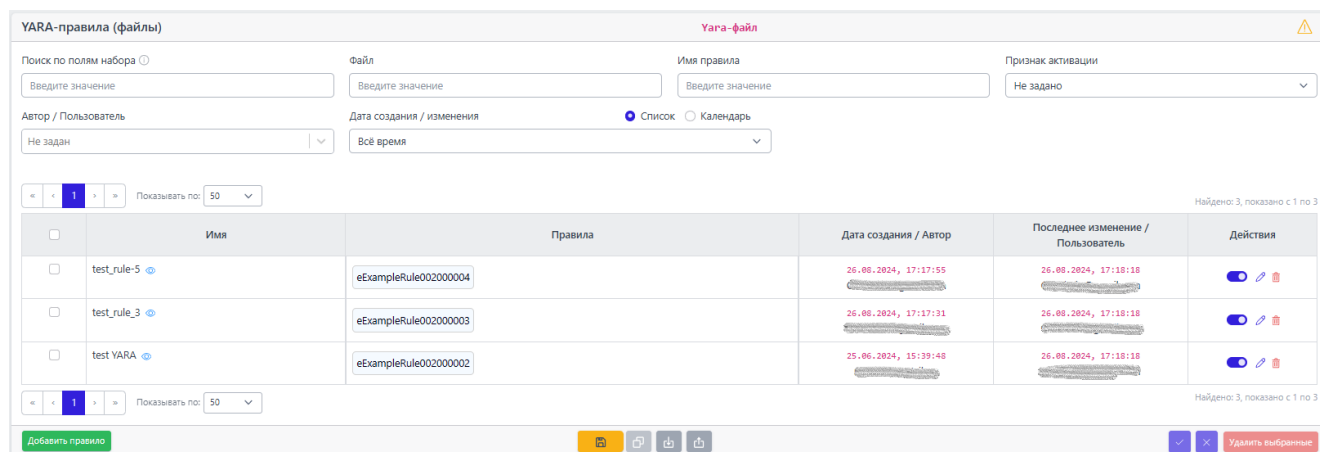


Рисунок 71 – YARA-правила

На странице **YARA-правила** можно выполнять следующие операции:

- просматривать правила из выбранного набора;
- добавлять новые правила в выбранный набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать правило;
- редактировать выбранное правило;
- удалить выбранное правило из набора;
- синхронизировать с репозиторием.

На странице с правилами фильтрация осуществляется с помощью следующих фильтров:

- **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: Значение,

Издатель ЭП, Правила, Комментарий);

- Файл;
- Имя правила;
- Признак активации;
- Автор/пользователь;
- Дата создания/Изменения.

Для добавления нового правила необходимо нажать кнопку **Добавить правило**, после чего откроется окно **Добавить правило** (рисунок 72), в котором необходимо прописать имя правила и условие в соответствии с синтаксисом YARA, либо добавить правило из внешнего источника, предварительно выбрав источник. Подробная информация о синтаксисе Yara содержится в [официальной документации Yara](#). Пример правила YARA приведен на рисунке 73.

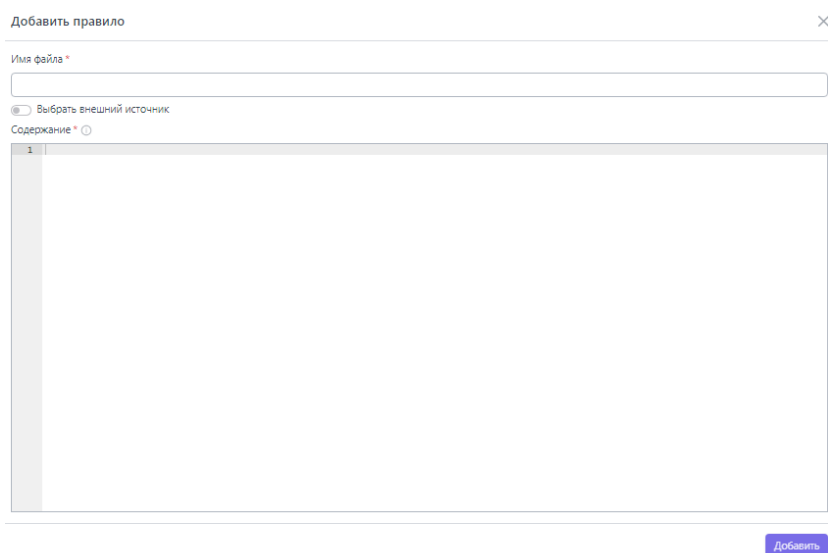


Рисунок 72 – Окно добавления правила

```
1 rule CobaltStrike__Resources_Artifact32_and_Resources_Dropper_v1_49_to_v3_14
2 {
3   meta:
4     desc="Cobalt Strike's resources/artifact32{.exe,.dll,big.exe,big.dll} and resources/dropper.exe signature for versions 1.49 to 3.14"
5     rsl = "40fc605a8b95bbd79a3bd7d9af73fbeebe3fada577c99e7a111f6168f6a0d37a"
6     author = "gssincl@google.com"
7
8   strings:
9     // Decoder function for the embedded payload
10    $payloadDecoder = { 88 [2] 89 ?? 03 [2] 8B [2] 03 [2] 0F B6 18 8B [2] 89 ?? C1 ?? 1F C1 ?? 1E 01 ?? 83 ?? 03 29 ?? 03 [2] 0F B6 00 31 ?? 88 ?? 8:
11
12   condition:
13     any of them
14 }
15
16 }
```

Рисунок 73 – Пример правила YARA

В окне добавления правила возможно добавить несколько правил, при этом каждое правило будет записано с новой строки.

Для добавления правила из внешнего источника требуется передвинуть ползунок  в положение , при этом откроется новое окно добавления правила, представленное на рисунке 74.

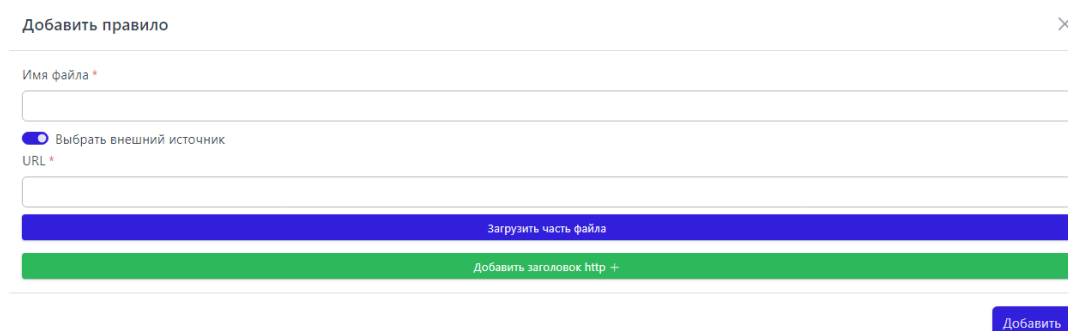


Рисунок 74 – Окно добавления правила из внешнего источника

Поля, помеченные символом , являются обязательными для заполнения.

Для корректного добавления правила в данном окне требуется указать URL внешнего источника.

В списке с YARA-правилами в наборе имеется иконка , показывающая, что данное правило синхронизировано с источником.

При нажатии по иконке  имеется возможность просмотреть правило.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата YARA** (). Набор будет сохранен в папке **Загрузки** в указанном формате. Для импорта правил из файла требуется нажать кнопку **Импортировать YARA-файл** (). Далее выбрать на компьютере файл, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать правило из выбранного набора, необходимо нажать кнопку  или . Действия требуют подтверждения в отдельном окне.

Для удаления правил из набора необходимо отметить флажками правила, которые требуется удалить и нажать кнопку **Удалить выбранные** или удалить правила по отдельности с помощью кнопки **Удалить** ().

Для редактирования правила следует нажать кнопку **Редактировать** () , после чего внести изменения в открывшемся окне с правилом. После внесения изменений в правило необходимо нажать кнопку **Сохранить**.

На странице с YARA-правилами имеется иконка  для синхронизации с репозиторием.

5.4.6. Распространяемая аналитика

Общие сведения

Распространяемая аналитика позволяет определить артефакты, в автоматическом режиме распространяемые на клиентов, взаимодействующих с TI, если они поддерживают соответствующий формат данных.

На странице раздела **Распространяемая аналитика** пользователь сервиса RT Protect TI, имеющий права Администратора/Аналитика, создает аналитические наборы, которые могут быть предоставлены пользователю, подключенному к платформе, при составлении договора на обслуживание и переданы ссылкой вместе с токеном, сгенерированным для нового клиента.

Наборы распространяемой аналитики

Страница раздела «Распространяемая аналитика» представлена на рисунке 75.

Распространяемая аналитика						
Название набора	Автор / Пользователь	Дата создания / изменения		Список Календарь		
Введите значение	Не задан	Всё время				
Найдено: 60, показано с 1 по 10						
☐	Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения
☐	teste	Доступен всем	0	15.05.2025, 13:45:41	15.05.2025, 16:28:48	15.05.2025, 16:28:48
☐	test7777	Доступен всем	160880	14.05.2025, 18:18:48		14.05.2025, 13:24:01
☐	sharedTest123	Доступен всем	324	23.04.2025, 16:28:28	12.05.2025, 14:38:28	14.05.2025, 13:24:25
☐	for_test	Доступен всем	0	05.04.2025, 17:02:02		
☐	Набор для отправки по email	Доступен всем	135	21.03.2025, 15:42:22	05.05.2025, 13:22:13	14.05.2025, 18:36:08
☐	для отправки по Email (много-во)	Доступен всем	50	18.03.2025, 18:07:14	29.04.2025, 17:18:14	14.05.2025, 18:36:08
☐	для теста email_002	Доступен всем	100	03.03.2025, 17:19:03	25.03.2025, 15:18:17	15.05.2025, 13:04:21
☐	для теста email	Доступен всем	100	03.03.2025, 17:15:44		15.05.2025, 13:18:48
☐	new_set	Доступен всем	15	03.03.2025, 16:25:43	29.04.2025, 17:18:14	15.05.2025, 13:18:41
☐	test_email_001	Доступен всем	0	03.03.2025, 16:17:28	12.05.2025, 15:11:15	15.05.2025, 13:11:47
Найдено: 60, показано с 1 по 10						
Добавить набор						
Удалить выбранное						

Рисунок 75 – Страница раздела «Распространяемая аналитика»

Страница представлена в виде таблицы с наборами аналитических данных.

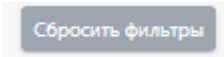
В таблице имеются следующие поля:

- Название набора;
- Доступен организациям;
- Количество записей;
- Дата создания/автор;
- Дата изменения/автор;

- Дата последнего сохранения;
- Действия.

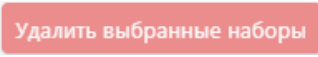
Для фильтрации информации в таблице имеются следующие фильтры:

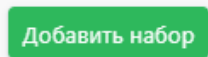
- Название набора;
- Автор/Пользователь;
- Дата создания/Изменения.

В верхней части страницы имеется иконка  для отмены примененных для фильтрации настроек.

Для навигации на странице имеется стандартный элемент пагинатор.

Действия, возможные над наборами:

-  (редактирование набора);
-  (принудительная синхронизация);
-  (скачивание набора или получение ссылки на скачивание набора);
-  (удаление набора);
-  (добавление нового набора);
-  (удалить выбранные наборы).

При нажатии по иконке  появится окно, представленное на рисунке 76.

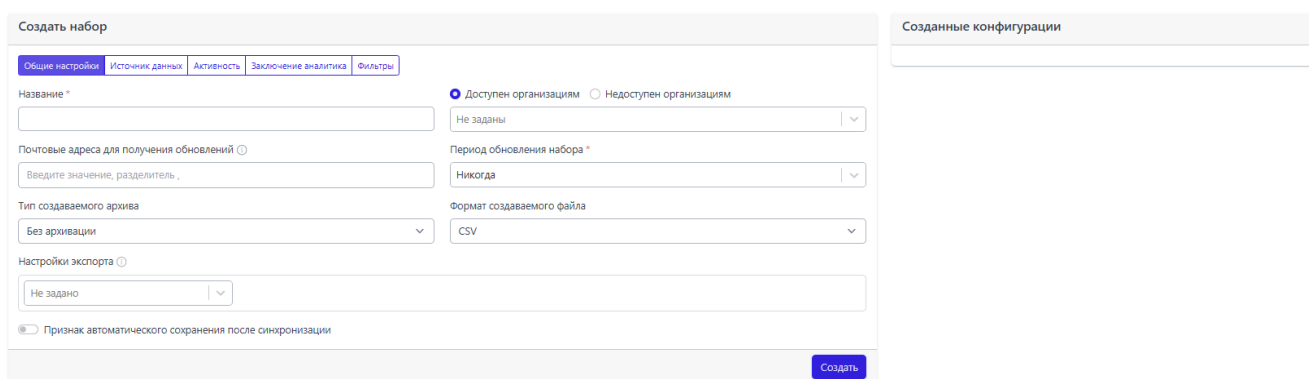


Рисунок 76 – Окно создания набора

В данном окне для создания набора требуется ввести в соответствующих полях следующие параметры:

- Название набора;
- Доступен организациям (в данном поле требуется указать организацию, для которой будет доступен данный набор с распространяемой аналитикой);
- Не доступен организациям (в данном поле требуется указать организацию, для которой будет недоступен данный набор с распространяемой аналитикой);
- Почтовый адрес для получения обновленных данных набора аналитики;
- Период обновления набора;
- Тип создаваемого архива;
- Формат создаваемого файла;
- Признак автоматического сохранения после синхронизации;
- Настройки экспорта (порядок вывода экспортируемых полей);
- Название набора и период обновления источника данных.

Далее следует произвести настройку данных в наборе. Для настройки данных имеются области, которые будут различаться в зависимости от выбранной вкладки, на которой представлены настройки.

Выбранная вкладка подсвечивается синим цветом. Поля с настройками по выбранной вкладке **Источники данных** представлены на рисунке 77.

Создать набор

Общие настройки | **Источники данных** | Активность | Заключение аналитика | Фильтры

Источник данных: Не задан

Сортировка: Не задан

Направление сортировки: Не задан

Тип артефакта: Не задан

Дата добавления: Все время

Количество: 0

Дата синхронизации: начальная дата → конечная дата

Актуальность: Не задан

Активация: Не задан

Надежность (Минимум): 0

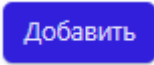
Добавить

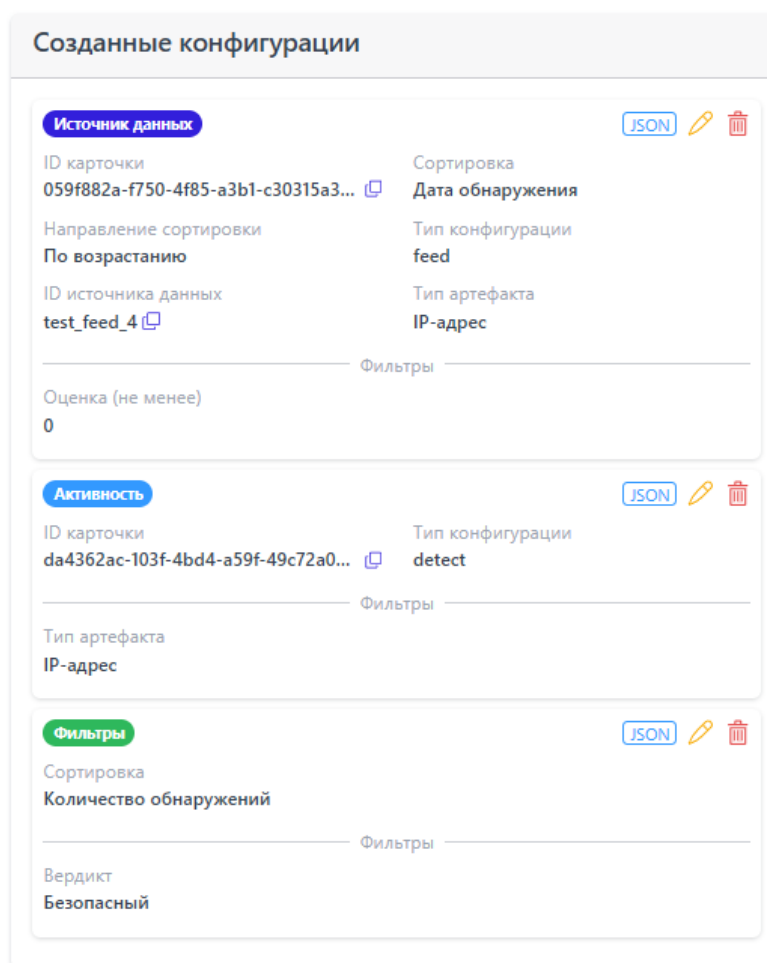
Создать

Рисунок 77 – Настройка полей выбранной вкладки «Источники данных»

В данной вкладке можно настроить следующие параметры:

- Источник данных (добавляется источник данных, для которого происходит настройка данных в наборе);
- Тип артефакта (указывается один или несколько типов артефактов согласно выпадающему списку);
- Актуальность (указывается, какие артефакты будут использоваться (актуальные, не актуальные));
- Сортировка (дата обнаружения, по убыванию/по возрастанию);
- Дата добавления (указывается начальная и конечная даты, когда был добавлен артефакт);
- Количество;
- Активация.

После выставления настроек требуется нажать по иконке , после чего появится поле с зафиксированными настройками конфигурации источника данных (рисунок 78).



Созданные конфигурации

Источник данных JSON  

ID карточки
059f882a-f750-4f85-a3b1-c30315a3... 

Направление сортировки
По возрастанию

ID источника данных
test_feed_4 

Сортировка
Дата обнаружения

Тип конфигурации
feed

Тип артефакта
IP-адрес

Фильтры

Оценка (не менее)
0

Активность JSON  

ID карточки
da4362ac-103f-4bd4-a59f-49c72a0... 

Тип конфигурации
detect

Фильтры

Тип артефакта
IP-адрес

Фильтры JSON  

Сортировка
Количество обнаружений

Фильтры

Вердикт
Безопасный

Рисунок 78 – Создание конфигурации набора распространяемой аналитики

В области настроенной конфигурации имеются кнопки, не зависящие от конфигурации и являющиеся общими для всех вкладок.

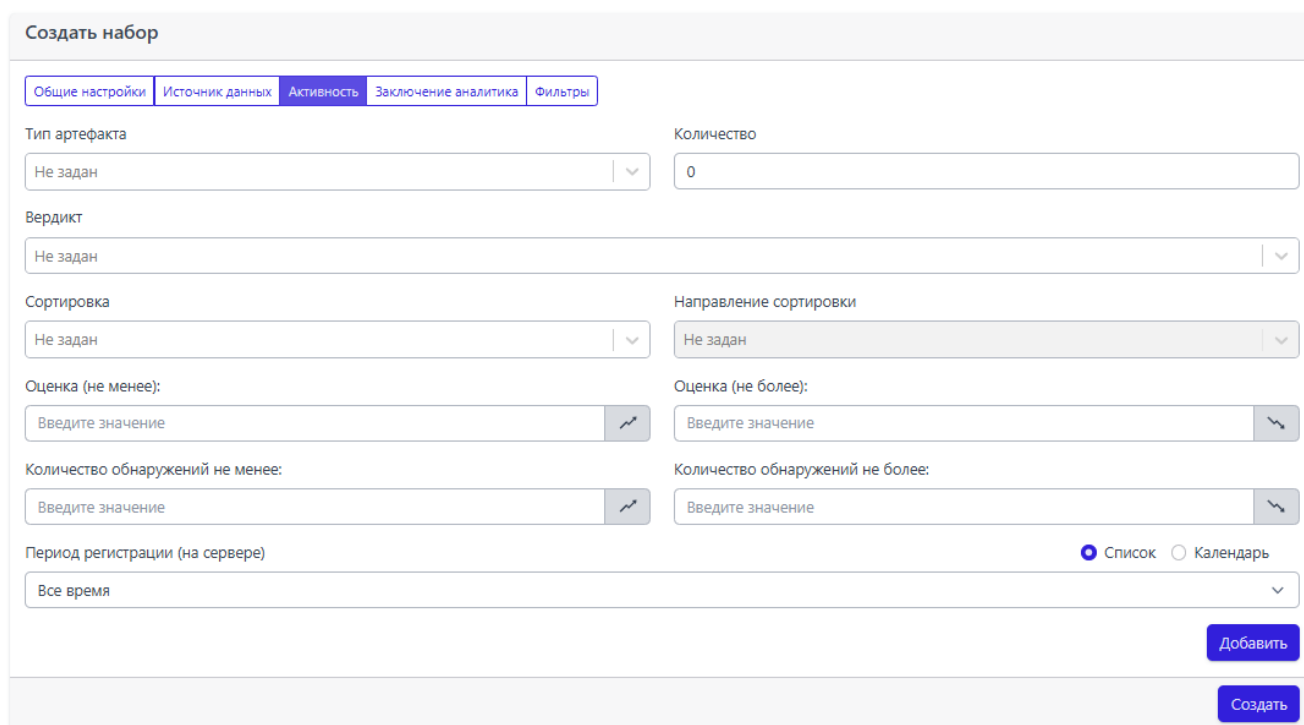
При нажатии по иконке  имеется возможность редактирования настроенной конфигурации.

При нажатии по иконке , имеется возможность просмотра настроенной конфигурации в соответствующем формате.

При нажатии по иконке  происходит удаление настроек параметров в конфигурации.

После редактирования настроек конфигурации для сохранения измененных настроек требуется нажать по иконке .

Поля настройки по выбранной вкладке **Активность** представлены на рисунке 79.



The screenshot shows a configuration window titled "Создать набор" (Create set). At the top, there are five tabs: "Общие настройки" (General settings), "Источник данных" (Data source), "Активность" (Activity), "Заключение аналитика" (Analytics conclusion), and "Фильтры" (Filters). The "Активность" tab is selected. The form contains several fields for configuring activity parameters:

- Тип артефакта** (Artifact type): A dropdown menu currently set to "Не задан" (Not specified).
- Количество** (Quantity): A text input field with the value "0".
- Вердикт** (Verdict): A dropdown menu currently set to "Не задан" (Not specified).
- Сортировка** (Sorting): A dropdown menu currently set to "Не задан" (Not specified).
- Направление сортировки** (Sorting direction): A dropdown menu currently set to "Не задан" (Not specified).
- Оценка (не менее):** (Rating (not less than)): Two identical text input fields, both containing "Введите значение" (Enter value).
- Количество обнаружений не менее:** (Number of detections not less than): Two identical text input fields, both containing "Введите значение" (Enter value).
- Период регистрации (на сервере)** (Registration period (on the server)): A dropdown menu set to "Все время" (All time). To its right are radio buttons for "Список" (List) and "Календарь" (Calendar), with "Список" selected.

At the bottom right of the form are two buttons: "Добавить" (Add) and "Создать" (Create).

Рисунок 79 – Настройка полей выбранной вкладки «Активность»

В области настроек параметров по данной вкладке имеется возможность настроить следующие параметры:

- Количество (количество получаемых элементов для каждого выбранного типа артефакта);
- Тип артефакта (Файл, IP-адрес; доменное имя; URL, EMAIL);

- Вердикт (Неизвестный, безопасный, вредоносный, подозрительный);
- Сортировка (по количеству обнаружений, по времени последнего обнаружения, по возрастанию/убыванию);
- количество обнаружений не менее;
- количество обнаружений не более;
- Период регистрации (на сервере) (начальная и конечная даты);
- Оценка (от -100 до 100).

Поля настройки по выбранной вкладке **Заключения аналитика** представлены на рисунке 80.

Рисунок 80 – Настройка полей выбранной вкладки «Заключение аналитика»

В области настроек параметров по данной вкладке имеется возможность настроить следующие параметры:

- Количество (количество записей артефактов по выбранному набору, отображающихся на странице **Заключение аналитика**);
- Тип артефакта (Файл, IP-адрес; доменное имя; URL, EMAIL);
- Вердикт (Неизвестный, безопасный, вредоносный, подозрительный);
- Сортировка (по количеству обнаружений, по времени последнего обнаружения, по возрастанию/убыванию);
- Время актуальности (день, неделя, месяц, 3 месяца, бесконечно);

- Время создания (начальная и конечная дата),
- Актуальность.

Поля настройки по выбранной вкладке **Фильтры** представлены на рисунке 81.

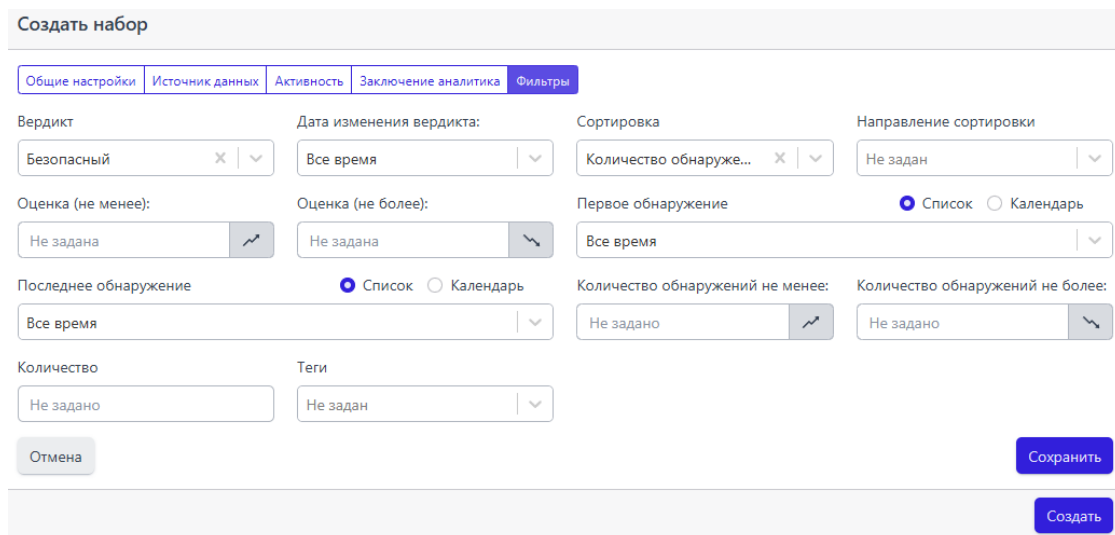


Рисунок 81 – Настройка полей выбранной вкладки «Фильтры»

В области настроек параметров по данной вкладке имеется возможность настроить следующие параметры:

- Вердикт;
- Дата изменения вердикта;
- Сортировка;
- Направление сортировки;
- Оценка (не менее);
- Оценка (не более);
- Первое обнаружение;
- Последнее обнаружение;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Количество;
- Теги.

5.4.7. Угрозы и злоумышленники

На данной странице отображаются данные по угрозам и злоумышленникам полученные от различных источников, например, данных MISP.

Источники данных возможно загрузить как с помощью сервера RT Protect TI, так и на этапе деплоя сервера добавим необходимую информацию в файл:

ti-deploy/config/default/feeds.json

Данный раздел может использоваться аналитиками и администраторами в качестве аналитической информации.

Общий вид страницы представлен на рисунке 82.

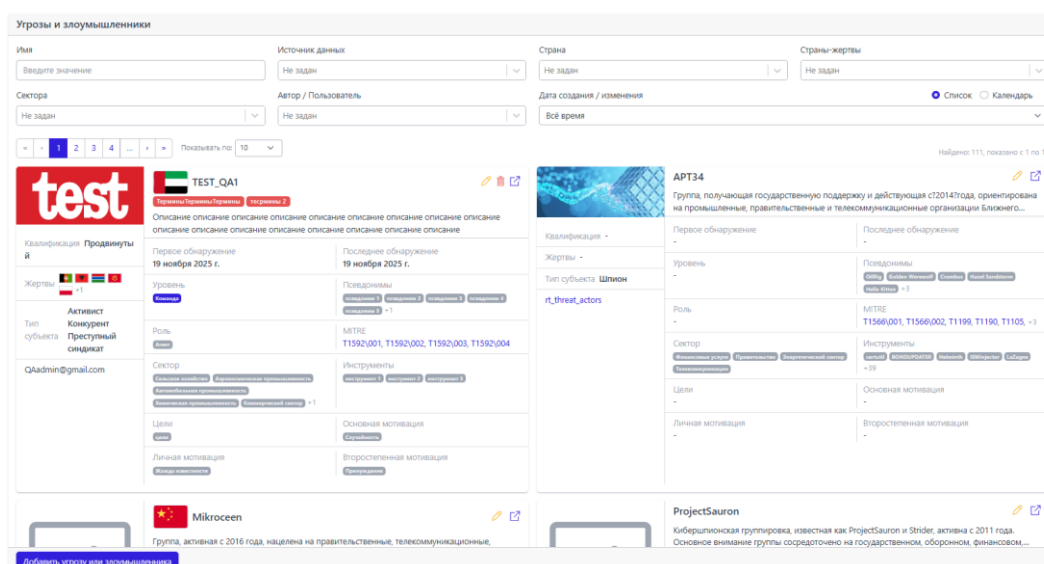


Рисунок 82 – Страница Угрозы и злоумышленники

На данной странице имеется возможность добавить информацию о злоумышленнике или угрозе нажав по иконке «Добавить угрозу или злоумышленника».

Имеется возможность редактировать информацию о злоумышленнике, удалить поле с описанием, либо перейти на страницу с описанием угрозы.

Так же можно просмотреть граф связей упоминаемых в статье артефактов.

5.4.8. Вредоносное ПО

На странице Вредоносное ПО в виде таблицы представлен перечень вредоносного ПО (рисунок 83).

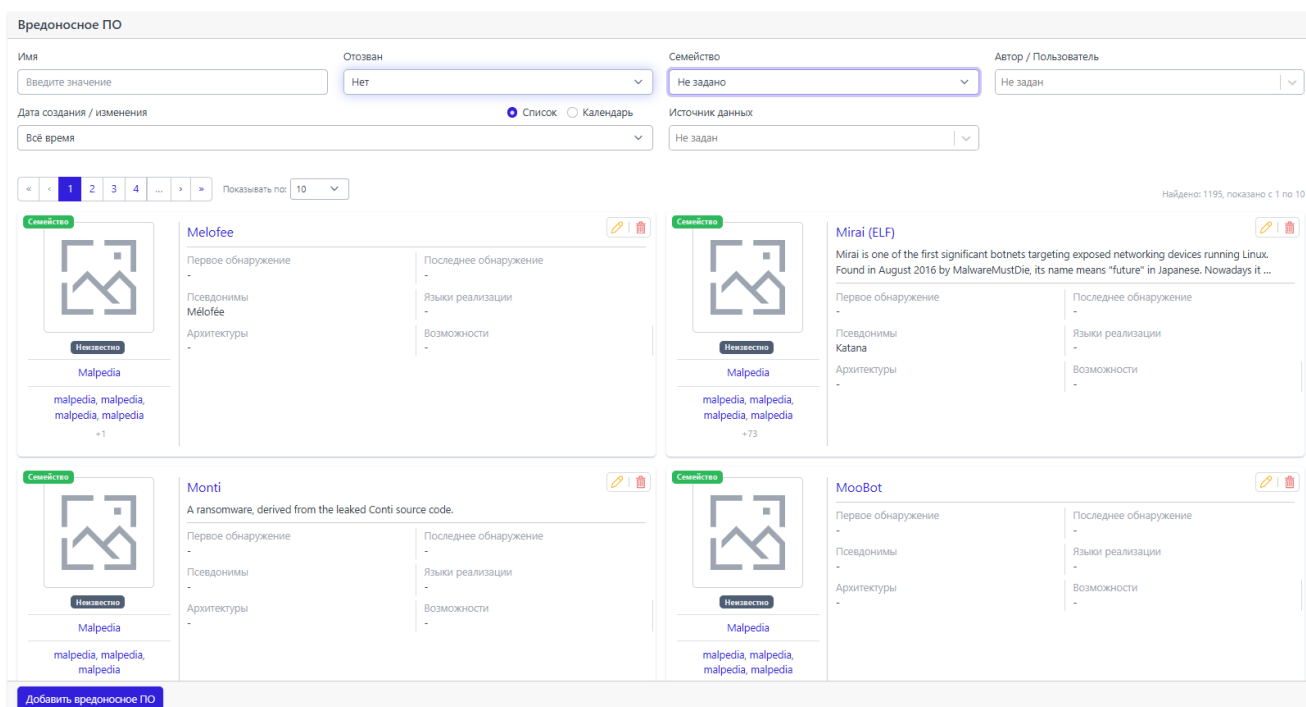


Рисунок 83 – Страница Вредоносное ПО

Информация о вредоносном ПО пополняется из источников данных типа STIX, а также, может быть добавлена вручную.

Для фильтрации информации на странице предусмотрена система фильтров, представленная в следующем списке:

- Имя;
- Отозван;
- Семейство (Не задано, Семейство, Экземпляр);
- Автор/Пользователь;
- Дата создания/Изменения (Все время, 15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца);
- Источник данных.

При нажатии по иконке имени вредоносного ПО (выделено синим шрифтом), открывается информация о вредоносном ПО, а также связанные сущности и граф связей.

Добавить вредоносное ПО

При нажатии по иконке , можно добавить информацию о новом вредоносном ПО.

После нажатия по иконке открывается страница добавления информации о ПО представленная на рисунке 84.

The screenshot shows a web form titled "Добавить вредоносное ПО" (Add Malware) with a close button (X) in the top right corner. The form contains several input fields and dropdown menus:

- Имя *** (Name): A text input field with placeholder "Введите значение".
- Тип вредоносного ПО *** (Malware Type): A dropdown menu with "Не задан" (Not specified) selected.
- Дата обнаружения *** (Discovery Date): A date picker input field with placeholder "Введите значение".
- Дата последнего обнаружения *** (Last Discovery Date): A date picker input field with placeholder "Введите значение".
- Псевдонимы** (Aliases): A text input field with placeholder "Введите значение, разделитель ;".
- Термины** (Terms): A text input field with placeholder "Введите значение, разделитель ;".
- Описание** (Description): A large text area with placeholder "Введите значение".
- Языки реализации** (Implementation Languages): A dropdown menu with "Не задана" (Not specified) selected.
- Архитектуры** (Architectures): A dropdown menu with "Не задана" (Not specified) selected.
- Возможности** (Capabilities): A dropdown menu with "Не задана" (Not specified) selected.
- Семейство** (Family): A checkbox.
- Отозван** (Revoked): A checkbox.
- Иконка** (Icon): A section with a "Выбрать файл" (Choose file) button and a preview area labeled "Иконка" with a red delete button.

At the bottom right of the form are two buttons: "Создать" (Create) in blue and "Отмена" (Cancel) in gray.

Рисунок 84 – Ручное добавление информации о вредоносном ПО

При установке галочки «Отозвать» дальнейший учет данного вредоносного инструмент исключается

В области дополнительной информации можно указать дату обнаружения, дату последнего обнаружения, языки реализации, Архитектуры, возможности.

При нажатии по иконке «Создать» информация о новом вредоносном ПО появится в общем списке.

5.4.9. Инструменты

На странице Инструменты показана информация по вредоносным инструментам, используемым злоумышленниками при проведении вредоносных действий.

Общий вид страницы представлен на рисунке 85.

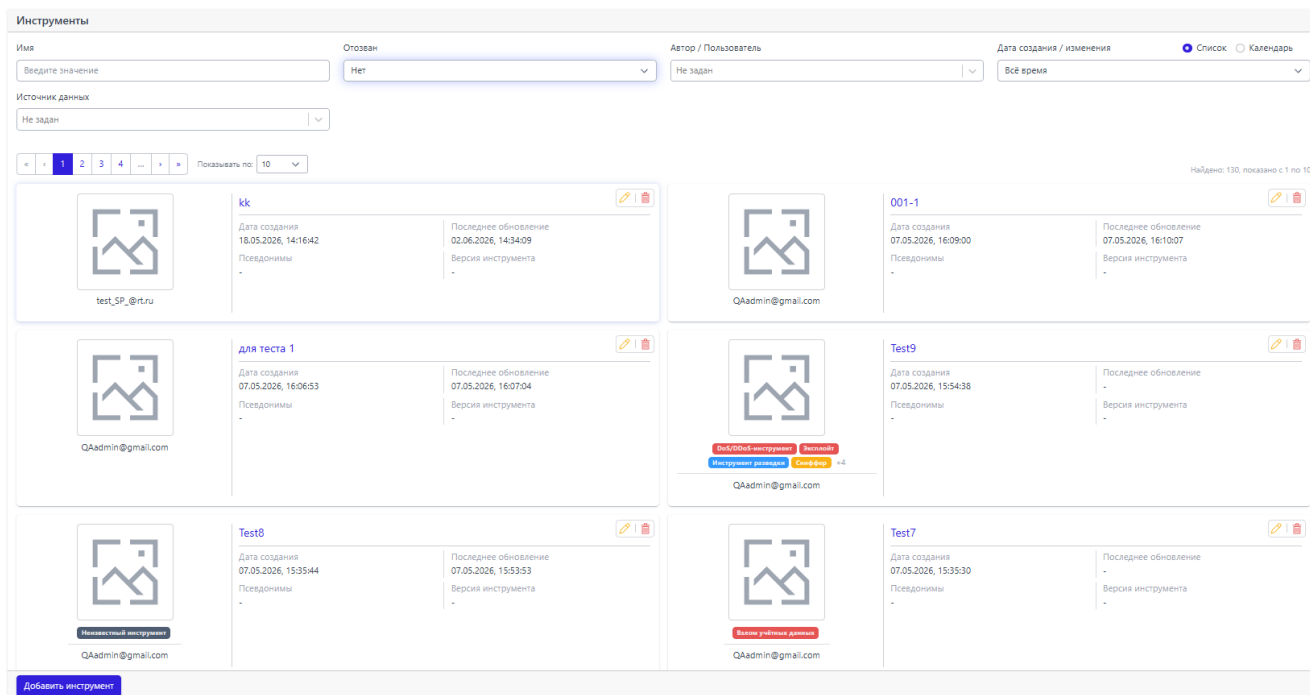


Рисунок 85 – Общий вид страницы «Инструменты»

Информация о вредоносных инструментах пополняется из источников данных типа STIX, а также, может быть добавлена вручную.

Для фильтрации информации имеется система фильтров, представленная в следующем списке:

- Имя;
- Отозван;
- Автор/Пользователь;
- Дата создания/изменения;
- Источник данных.

Для добавления информации о инструменте вручную, требуется по иконке , после чего в открывшемся окне добавить информацию и нажать по иконке «Создать», после чего инструмент появиться в общем списке.

При наведении указателя мыши на иконку с именем инструмента и нажатии ЛКМ, открывается окно с расширенной информацией, где есть так же возможность просмотреть связанные с инструментом сущности, и просмотреть граф связей.

5.4.10. Матрица MITRE ATT&CK

На рисунке 86 представлен общий вид страницы Матрица MITRE ATT&CK. На данной странице приведено описание техник Mitre описывающих различные вредоносные действия. Аналитик и администратор для удобства описания и понимания вредоносных техник упоминающихся в отчетах может обратиться к странице.

Поиск

Поиск по названию или ID техники...

Reconnaissance	12	Resource Development	9	Initial Access	11	Execution	24	Persistence	25	Privilege Escalation	14	Stealth	33
T1589 Gather Victim Identity L...	1	T1583 Acquire Infrastructure	1	T1078 Valid Accounts	1	T1047 Windows Management Inst...	1	T1034 Path Interception	1	T1034 Path Interception	1	T1006 Direct Volume Access	1
T1590 Gather Victim Network ...	1	T1584 Compromise Infrastruct...	1	T1091 Replication Through Remov...	1	T1053 Scheduled Task/Job	1	T1037 Boot or Logon Initializat...	1	T1037 Boot or Logon Initializat...	1	T1014 Rootkit	1
T1591 Gather Victim Org Infor...	1	T1585 Establish Accounts	1	T1133 External Remote Services	1	T1059 Command and Scriptin...	1	T1053 Scheduled Task/Job	1	T1053 Scheduled Task/Job	1	T1027 Obfuscated Files or Inf...	1
T1592 Gather Victim Host Info...	1	T1586 Compromise Accounts	1	T1189 Drive-by Compromise	1	T1061 Graphical User Interface	1	T1062 Hypervisor	1	T1055 Process Injection	1	T1036 Masquerading	1
T1593 Search Open Websites/...	1	T1587 Develop Capabilities	1	T1190 Exploit Public-Facing Applic...	1	T1064 Scripting	1	T1078 Valid Accounts	1	T1068 Exploitation for Privilege Es...	1	T1055 Process Injection	1
T1594 Search Victim-Owned Webs...	1	T1588 Obtain Capabilities	1	T1195 Supply Chain Comprom...	1	T1072 Software Deployment Tools	1	T1098 Account Manipulation	1	T1078 Valid Accounts	1	T1064 Scripting	1
T1595 Active Scanning	1	T1608 Stage Capabilities	1	T1199 Trusted Relationship	1	T1106 Native API	1	T1108 Redundant Access	1	T1098 Account Manipulation	1	T1070 Indicator Removal	1
T1596 Search Open Technical ...	1	T1650 Acquire Access	1	T1200 Hardware Additions	1	T1127 Trusted Developer Utilit...	1	T1112 Modify Registry	1	T1134 Access Token Manipulat...	1	T1078 Valid Accounts	1
T1597 Search Closed Sources	1	T1683 Generate Content	1	T1566 Phishing	1	T1129 Shared Modules	1	T1133 External Remote Services	1	T1484 Domain or Tenant Polic...	1	T1108 Redundant Access	1
T1598 Phishing for Information	1			T1659 Content Injection	1	T1153 Source	1	T1136 Create Account	1	T1543 Create or Modify Syste...	1	T1127 Trusted Developer Utilit...	1
T1681 Search Threat Vendor Data	1			T1669 Wi-Fi Networks	1	T1175 Component Object Model a...	1	T1137 Office Application Start...	1	T1546 Event Triggered Execut...	1	T1134 Access Token Manipulat...	1
T1682 Query Public AI Services	1					T1197 BITS Jobs	1	T1176 Software Extensions	1	T1547 Boot or Logon Autosta...	1	T1140 Deobfuscate/Decode Files ...	1
						T1203 Exploitation for Client Execu...	1	T1197 BITS Jobs	1	T1548 Abuse Elevation Control...	1	T1149 LC_MAIN Hijacking	1
						T1204 User Execution	1	T1205 Traffic Signaling	1	T1611 Escape to Host	1	T1197 BITS Jobs	1
						T1559 Inter-Process Communi...	1	T1505 Server Software Compo...	1			T1202 Indirect Command Execution	1
						T1569 System Services	1	T1525 Implant Internal Image	1			T1205 Traffic Signaling	1
						T1574 Hijack Execution Flow	1	T1542 Pre-OS Boot	1			T1211 Exploitation for Stealth	1
						T1609 Container Administration C...	1	T1543 Create or Modify Syste...	1			T1216 System Script Proxy Exe...	1
						T1610 Deploy Container	1	T1546 Event Triggered Execut...	1			T1218 System Binary Proxy Ex...	1
						T1648 Serverless Execution	1	T1547 Boot or Logon Autosta...	1			T1220 XSL Script Processing	1
						T1651 Cloud Administration Com...	1	T1554 Compromise Host Software...	1			T1221 Template Injection	1
						T1674 Input Injection	1	T1556 Modify Authentication ...	1			T1480 Execution Guardrails	1

Рисунок 86 – Общий вид страницы Матрица MITRE ATT&CK

5.4.11. Лента угроз

На данной странице представлены статьи, касающиеся информационной безопасности, в которых имеются упоминания об угрозах и вредоносных артефактах.

Информация на странице представлена в виде списка статей с кратким описанием.

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Название;
- Получена из ИИ;
- Артефакт;
- Уязвимость;
- Источник;
- Источник данных;
- Автор/Пользователь;
- Дата создания/Изменения;
- Тип отчета (не задано, отчет об угрозе, другое).

Общий вид страницы **Лента угроз** представлен на рисунке 87.

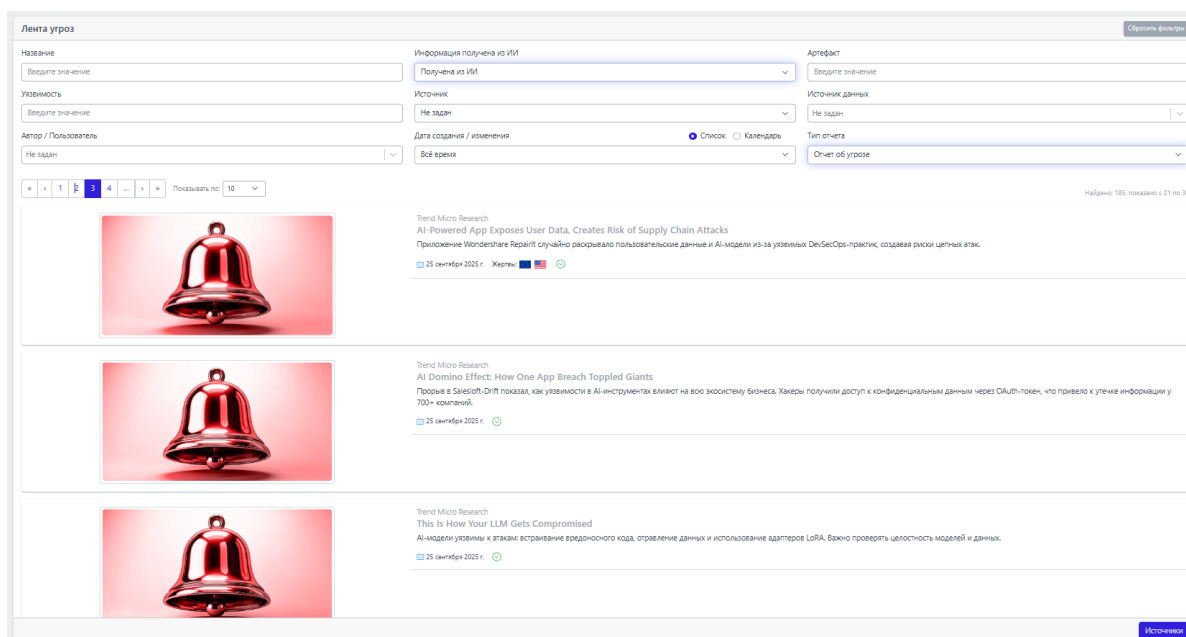


Рисунок 87 – Общий вид страницы Лента угроз

При нажатии по имени статьи ЛКМ откроется страница с более подробной информацией о статье и об артефактах, которые упоминаются в статье (рисунок 88).

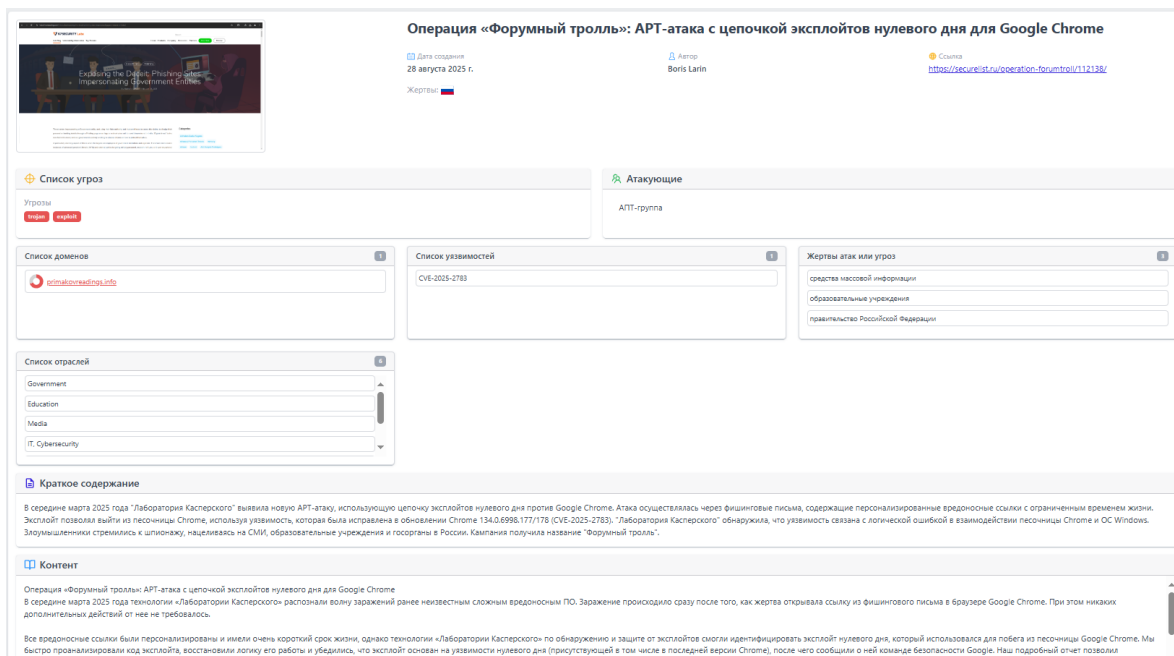


Рисунок 88 – Подробная информация о статье

На странице отображается информация из статьи, а также, угрозы упоминающиеся в статье, например, найденные вредоносные артефакты.

В нижней части окна отображается область с графом связей артефактов.

При нажатии по иконке  на странице «Лента угроз» происходит переход на страницу со списком источников из которых были получены представленные на странице статьи (рисунок 89).

Источники

Автор / Пользователь: Не задан | Дата создания / изменения: Все время | Сбросить фильтры

Показывать по: 10

☐	Название	URL	Источник данных	Дата создания / Автор	Действия
☐	Blog Teros Intelligence_TEST_QA	https://blog.terosintelligence.com/	Blog Teros Intelligence_TEST_QA	03.10.2025, 15:23:01 QAanalyst@gmail.com	
☐	Blog Malware Bytes_TEST_QA	https://www.malwarebytes.com/blog	Blog Malware Bytes_TEST_QA	03.10.2025, 15:23:01 QAanalyst@gmail.com	
☐	RED SECURITY News_QA	https://redsecurity.ru/news	RED SECURITY News_QA	03.10.2025, 15:26:33 QAdmin@gmail.com	
☐	RED SECURITY News	https://redsecurity.ru/news	RED SECURITY News	18.09.2025, 17:33:06 test@test.ru	
☐	Habr F6 Articles	https://habr.com/ru/companies/F6/articles/	Habr F6 Articles	18.09.2025, 17:33:06 test@test.ru	
☐	Expert Blog Solar 4RAYS	https://it-solar.ru/solar-4rays/blog/	Expert Blog Solar 4RAYS	18.09.2025, 17:33:06 test@test.ru	
☐	Blog PT ESC Threat Intelligence	https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/	Blog PT ESC Threat Intelligence	18.09.2025, 17:33:06 test@test.ru	
☐	SECURELIST Targeted Cyber Attacks	https://securelist.ru/threat-category/celebrity-kiberataki/	SECURELIST Targeted Cyber Attacks	18.09.2025, 17:33:06 test@test.ru	
☐	SECURELIST Financial Threats	https://securelist.ru/threat-category/finansovye-ugrozy/	SECURELIST Financial Threats	18.09.2025, 17:33:06 test@test.ru	
☐	SECURELIST Mobile Threats	https://securelist.ru/threat-category/mobile-ugrozy/	SECURELIST Mobile Threats	18.09.2025, 17:33:06 test@test.ru	

Выбрано: 0 из 10 | Найдено: 31, показано с 1 по 10

Поиск: | Сбросить фильтры

Рисунок 89 – Список источников

Информация на странице представлена в таблице со следующими полями:

- Кнопка выбора;
- Название;
- URL;
- Источник данных;
- Дата создания/Автор;
- Действия (Редактировать, проверить обновления, обновить целиком).

Для фильтрации информации предусмотрены следующие фильтры:

- Автор/пользователь;
- Дата создания/Изменения.

На странице представлены следующие иконки:

- ;
- (импортировать источники);
- (экспортировать выбранные источники).

При нажатии ЛКМ по названию источника происходит переход на страницу источника.

При нажатии в поле «Действия» по иконке редактирования источника открывается окно представленное на рисунке 90.

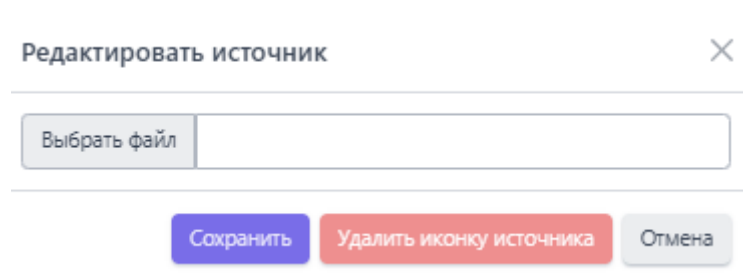


Рисунок 90 – Редактирование источника

В данном окне можно указать файл для обновления иконки источника.

На странице Источники в поле «Название» иконкой  показано что источник синхронизирован с данными полученными из источника данных взятого из статьи.

Иконка  показывает что синхронизация выполнена с ошибками, при этом при наведении указателя мыши на иконку. Во всплывающем окне приведен список ошибок синхронизации.

5.4.12. Уязвимости

Общие сведения

В данном разделе представлена информация по обнаруженным с помощью платформы RT Protect TI уязвимостям.

Отдельно представлены таблица с уязвимостями и таблица с программами, в которых обнаружены уязвимости.

Уязвимости идентифицированы в общепринятом формате CVE. Приведено описание уязвимости по БДУ ФСТЭК и базе данных от Национального института стандартов и технологий (NIST).

Типы уязвимостей представлены по CWE (Common Weakness Enumeration). Также имеются рекомендации по предотвращению и устранению уязвимостей и информация по описанию уязвимостей.

Оценка серьезности уязвимости представлена по классификации CVSS (Common Vulnerability Scoring System).

Уязвимости

Общий вид страницы «Уязвимости» представлен на рисунке 91.

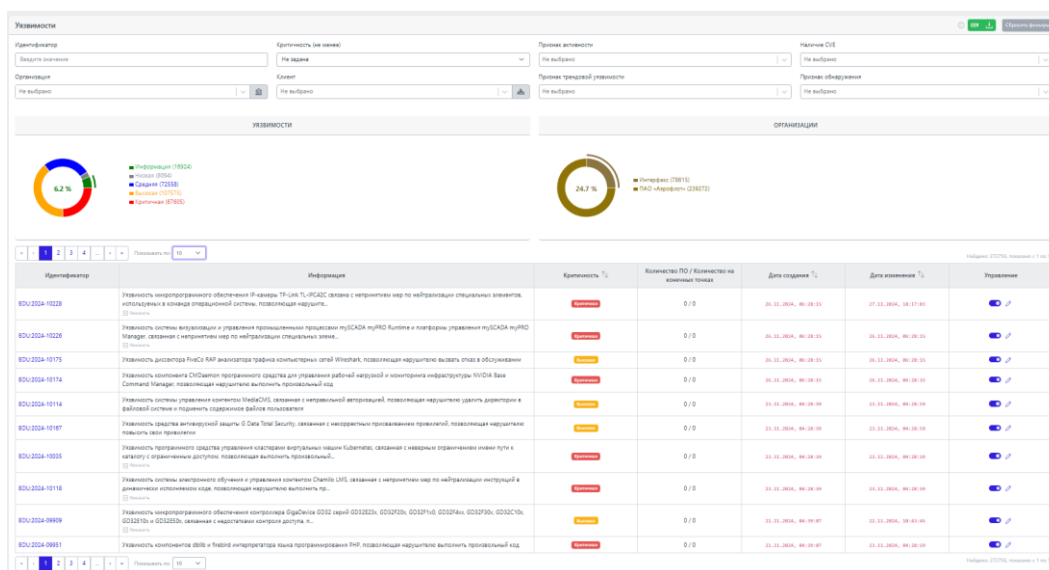


Рисунок 91 – Страница Уязвимости

На данной странице в виде таблицы представлена информация по найденным уязвимостям.

Таблица имеет следующие поля:

- Идентификатор (идентификация уязвимости по CVE);
- Информация (описание уязвимости);
- Критичность уязвимости;
- Количество ПО/Количество на конечных точках (в таблице отображается количество программ, в которых найдена данная уязвимость и количество конечных точек, на которых зарегистрировано ПО с данной уязвимостью);
- Дата создания;
- Дата изменения;
- Управление.

Для фильтрации информации в таблице имеются следующие фильтры:

- Идентификатор (в фильтре указывается идентификатор уязвимости в формате CVE);
- Критичность (не менее) (низкая, средняя, высокая, критичная);
- Признак активности (активирована, деактивирована);
- Наличие CVE (имеется, отсутствует);
- Признак трендовой уязвимости (обычная уязвимость, трендовая уязвимость).

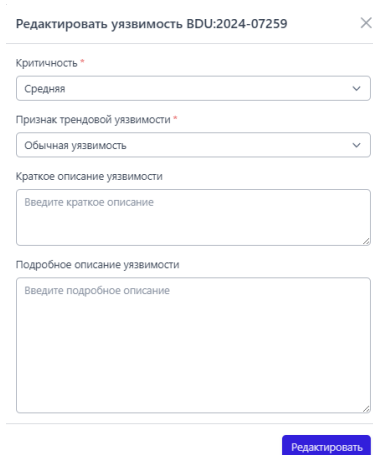
В столбце **Идентификатор** трендовая уязвимость отмечена иконкой . Признаком того, что уязвимость является трендовой можно выставить при редактировании уязвимости.

Признак выставляется аналитиком/администратором на основании анализа информации об уязвимости.

В столбце **Управление** можно деактивировать/активировать уязвимость, т.е. исключить из анализа программ.

Данное действие производится с помощью иконок  / . Деактивация/активация уязвимости производится аналитиком на основании анализа информации об уязвимости.

В столбце **Управление** при нажатии по иконке редактирования  открывается окно, представленное на рисунке 92



Редактировать уязвимость BDU:2024-07259

Критичность *

Средняя

Признак трендовой уязвимости *

Обычная уязвимость

Краткое описание уязвимости

Введите краткое описание

Подробное описание уязвимости

Введите подробное описание

Редактировать

Рисунок 92 – Окно редактирования информации по уязвимости

В данном окне можно изменить критичность уязвимости, выставить признак наличия трендовой уязвимости, а также добавить краткое и подробное описание уязвимости.

После добавления информации требуется нажать по иконке «Редактировать».

При нажатии в столбце **Идентификатор** по CVE-идентификатору уязвимости открывается информация об уязвимости, представленная на рисунке 93.

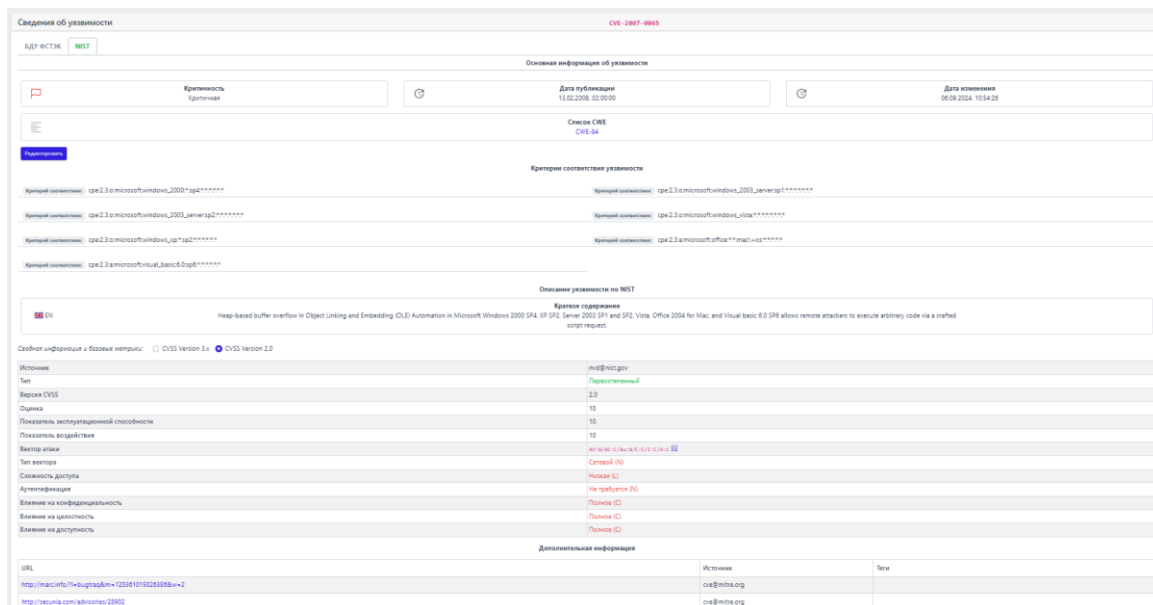


Рисунок 93 – Информация по уязвимости

На данной странице информация по уязвимости представлена в двух вкладках БДУ ФСТЭК и NIST.

Также по уязвимости можно просмотреть информацию по описанию CWE, перейдя по активной ссылке, подсвеченной синим цветом ([Список CWE: CWE-259](#)).

Данная ссылка находится в поле рядом с полем, где указывается дата публикации и изменения информации по уязвимости.

Редактирование информации по уязвимости можно также осуществить нажав по иконке [Редактировать](#), на странице «Сведения о уязвимости».

На странице «Уязвимости» имеется графическая область, в которой представлено распределение найденных уязвимостей по уровням критичности, а также, по организациям у которых в установленном ПО имеются уязвимости.

Данная область представлена на рисунке 94.

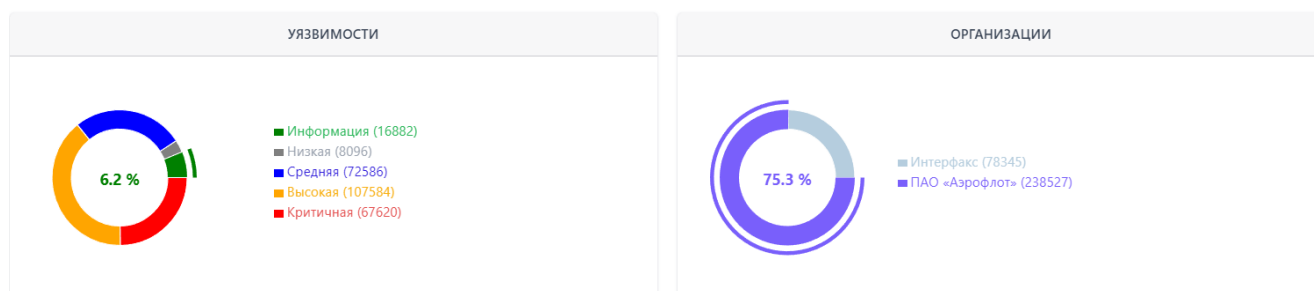


Рисунок 94 – Графическая область с отображением уязвимостей по уровням критичности и по организациям

В данной области записи с распределением по уровням критичности являются активными ссылками, при нажатии по которым в таблице с информацией по уязвимостям отображаются только уязвимости согласно выбранной критичности и выше. Например, при нажатии по уровню критичности «Высокая» в таблице будут отображаться только уязвимости с высоким и критичным уровнем.

Программы

Общий вид страницы Программы сервиса RT Protect TI возможно просмотреть в двух вариантах отображения.

Для переключения режима отображения используется иконка «Выбрать режим агрегации»  / .

В первом варианте, название программы и их модификации отображаются по группам в формате CPE (см. рис 95).

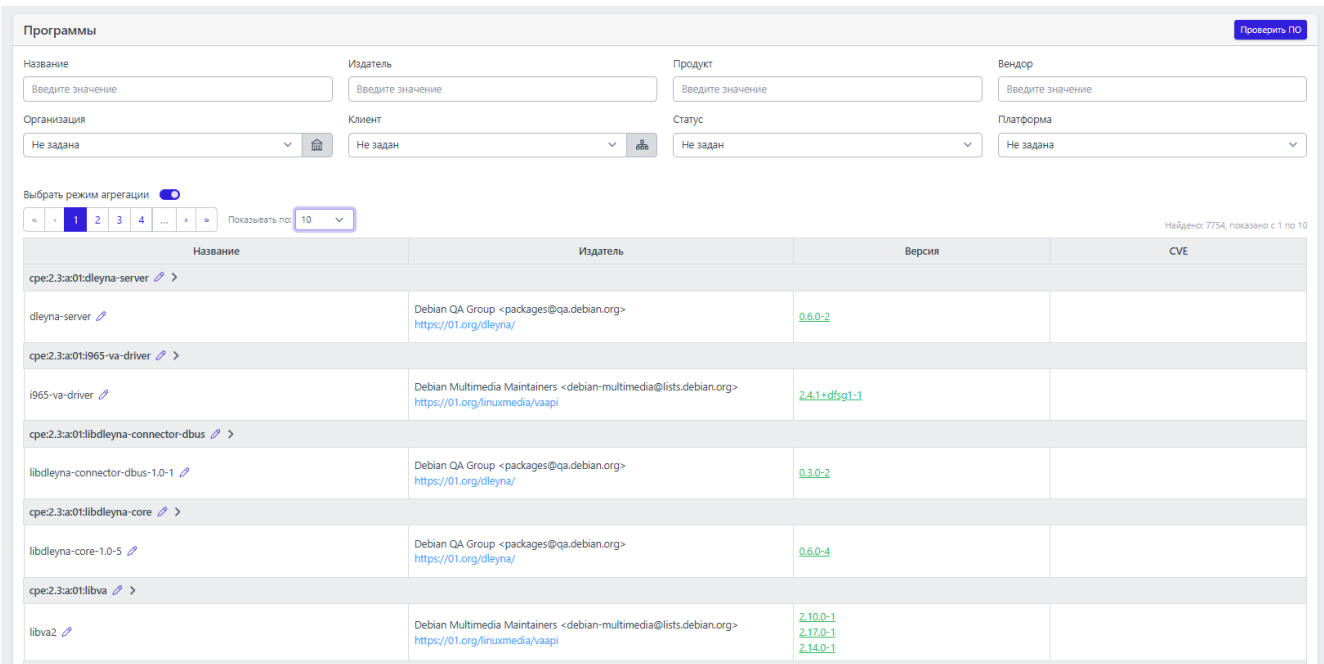


Рисунок 95 – Отображение страницы Программы
(название программы в формате CPE)

На странице в табличной форме представлена информация о программах, которые проанализированы на предмет уязвимостей.

Таблица имеет следующие поля:

- Название (указывается идентификация программы в формате CPE)
- Издатель;
- Версия (версия ПО);
- CVE (описание уязвимостей, найденных для программы в формате CVE с указанием критичности).

— CPE (описание программ по стандарту для машиночитаемого именования и идентификации всех видов программного обеспечения (софта) и устройств).

Во втором режиме отображения таблицы с проанализированными программами, при этом название программы отображается в обычном виде (рисунок 96).

Программы

Проверить ПО

Название

Введите значение

Издатель

Введите значение

Продукт

Введите значение

Вендор

Введите значение

Организация

Не задана

Клиент

Не задан

Статус

Не задан

Платформа

Не задана

Выбрать режим агрегации

Показывать по: 10

Найдено: 25517, показано с 11 по 20

Название	Издатель	Версия	CPE	Распространенность на конечных точках	Время сканирования	CVE
Среда выполнения Microsoft Edge WebView2 Runtime	Корпорация Майкрософт	130.0.2849.56	cpe:2.3:a:microsoft:edge:130.0.2849.56:*:*:*:*:*	16	30.10.2024, 12:34:14	CVE-2016-3296 CVE-2017-8521 CVE-2018-8452 CVE-2016-7243
Mozilla Firefox (x64 ru)	Mozilla	132.0	cpe:2.3:a:mozilla:firefox:132.0:*:*:*:*:*x64*	5	31.10.2024, 05:23:34	CVE-2023-1492 CVE-2011-3389 CVE-2022-4066 CVE-2007-1970
Rockstar Games Launcher	Rockstar Games	1.0.97.2200	cpe:2.3:a:rockstar:games:rockstar_games_launcher:1.0.97.2200:*:*:*:*:*	1	30.10.2024, 11:32:27	
Rockstar Games SDK	Rockstar Games	2.3.7.8	cpe:2.3:a:rockstar:games:rockstar_games:2.3.7.8:*:*:*:*:*	1	30.10.2024, 11:32:27	
Microsoft Visual Studio Code (User)	Microsoft Corporation	1.95.0	cpe:2.3:a:microsoft:visual_studio_code:1.95.0:*:*:*:*:*	1	30.10.2024, 10:32:29	CVE-2022-38020 CVE-2020-1192 CVE-2022-26921 CVE-2021-26437

Рисунок 96 – Отображение страницы программы (название программы в обычном формате)

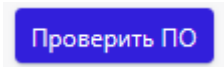
В таблице для удобного представления и быстрого анализа названия программ выделены различными цветами:

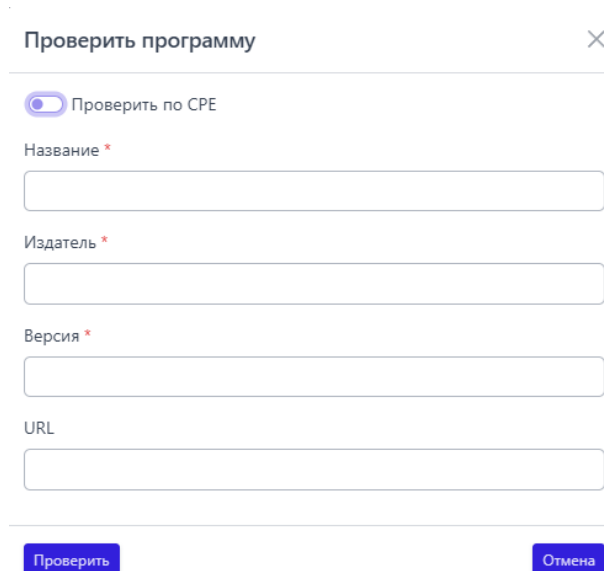
- Программы, в которых имеются уязвимости (шрифт красного цвета, например, **Microsoft Edge**);
 - Программы, в которых отсутствуют уязвимости (шрифт зеленого цвета, например, **Windows SDK**).
- Таблица имеет следующие поля:
- Название;
 - Издатель;
 - Версия;
 - CPE (описание программ по стандарту для машиночитаемого именования и идентификации всех видов программного обеспечения (софта) и устройств);
 - Распространенность на конечных точках;

- Время сканирования;
- CVE (описание уязвимостей, найденных для программы в формате CVE с указанием критичности).

Для фильтрации информации на странице **Программы** для обоих вариантов отображения используются следующие фильтры:

- Название (в области фильтра задается имя программы);
- Издатель;
- Продукт;
- Вендор;
- Организация;
- Клиент;
- Статус (не задан, уязвимости не найдены, уязвимости найдены, в процессе анализа, ошибка при формировании CVE, ошибка при сканировании);
- Платформа (Linux/Windows).

В правом верхнем углу страницы **Программы** имеется иконка , при нажатии по которой открывается окно для задания параметров для проверки новой программы, отсутствующей в списке (рисунок 97).



Проверить программу

☒ Проверить по CVE

Название *

Издатель *

Версия *

URL

Проверить Отмена

Рисунок 97 – Окно задания параметров проверяемой программы

В данном окне требуется задать параметры проверяемой программы и нажать по иконке **Проверить**.

Окно задания параметров для проверки программы при нажатии по иконке



Проверить по CPE

имеет вид, представленный на рисунке 98.

Рисунок 98 – Проверка программы, заданной в формате CPE

В данном окне после указания программы в формате CPE требуется нажать по иконке **Проверить**.

При нажатии по иконке с названием программы на странице **Программы** происходит переход на страницу сведений о программе, представленную на рисунке 99.

Сведения о программе

Среда выполнения Microsoft Edge WebView2...
ИЗДАТЕЛЬ: Майкрософт
ОПЕРАЦИОННАЯ СИСТЕМА: Майкрософт Windows 10 Корпоративная - 64...
Уязвимости найдены
СТАТУС ПРОВЕРКИ ПО НА УЯЗВИМОСТИ
130.0.2849.56
ВЕРСИЯ
30.10.2024, 12:34:12
ВРЕМЯ ОБНАРУЖЕНИЯ
30.10.2024, 12:34:12
ВРЕМЯ СКАНИРОВАНИЯ
Приложение
ТИП

Обнаруженные уязвимости

CVE	Соответствие	Дата создания	Дата обновления	CWE
CVE-2017-8504	Критерий соответствия: cpe2.3:microsoftedge-*****	15.06.2017, 04:29:03	29.10.2024, 04:31:31	CWE-200
CVE-2019-0650	Критерий соответствия: cpe2.3:microsoftedge-*****	06.03.2019, 02:29:01	29.10.2024, 04:54:16	CWE-119, CWE-787
CVE-2020-0823	Критерий соответствия: cpe2.3:microsoftedge-*****	12.03.2020, 19:15:17	29.10.2024, 04:54:19	CWE-119, CWE-787
CVE-2019-0612	Критерий соответствия: cpe2.3:microsoftedge-*****	09.04.2019, 02:29:00	29.10.2024, 04:54:16	CWE-269, NVD-CWE-NOINFO
CVE-2017-11792	Критерий соответствия: cpe2.3:microsoftedge-*****	18.10.2017, 03:00:00	29.10.2024, 04:54:14	CWE-119
CVE-2018-8618	Критерий соответствия: cpe2.3:microsoftedge-*****	12.11.2018, 03:00:00	29.10.2024, 04:54:15	CWE-119, CWE-787
CVE-2017-11893	Критерий соответствия: cpe2.3:microsoftedge-*****	13.12.2017, 00:29:01	29.10.2024, 04:32:36	CWE-119
CVE-2020-0826	Критерий соответствия: cpe2.3:microsoftedge-*****	12.03.2020, 19:15:17	29.10.2024, 04:54:19	CWE-119, CWE-787
CVE-2020-0828	Критерий соответствия: cpe2.3:microsoftedge-*****	12.03.2020, 19:15:17	29.10.2024, 04:54:19	CWE-119, CWE-787
CVE-2020-1242	Критерий соответствия: cpe2.3:microsoftedge-*****	09.06.2020, 23:15:16	29.10.2024, 04:54:20	CWE-200, NVD-CWE-NOINFO

Распространенность

Организация	ПАО «Аэрофлот»
Клиент	test (EDR DEV)
Распространенность на клиенте	16

Рисунок 99 – Сведения о программе

На данной странице сведения о программе представлены в следующих областях:

- Общие сведения о программе;
- Таблица с обнаруженными уязвимостями;
- Распространенность (показывается распространенность программы с уязвимостями у различных клиентов).

В верхней части страницы сведений о программе имеется иконка , при нажатии по которой ЛКМ будет отправлена команда на повторное сканирование экземпляра ПО.

В столбце CVE имеется иконка  для редактирования названия программы в CVE-формате.

Идентификатор уязвимости в CVE-формате является активной ссылкой, при нажатии по которой открывается страница с описанием уязвимости, представленная на рисунке 100.

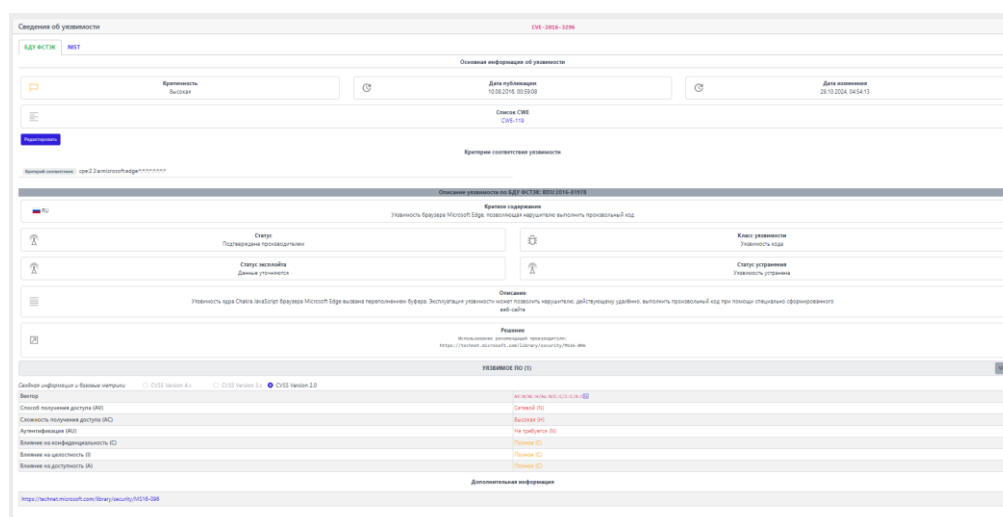
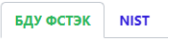


Рисунок 100 – Сведения об уязвимости

На данной странице сведения об уязвимости представлены от различных источников: БДУ ФСТЭК и NIST. Для отображения информации по уязвимости от источников требуется нажать по иконке .

Для редактирования информации об уязвимости требуется нажать по иконке , после чего откроется окно редактирования, представленное на рисунке 101.

Редактировать уязвимость BDU:2016-01978, CVE-2016-3296

Критичность *

Высокая

Признак трендовой уязвимости *

Обычная уязвимость

Краткое описание уязвимости

Введите краткое описание

Подробное описание уязвимости

Введите подробное описание

Редактировать

Рисунок 101 – Окно редактирования информации об уязвимости

На странице информации об уязвимости при нажатии по иконке **CWE-119** происходит переход на страницу с описанием уязвимости в CWE-формате.

5.4.13. ИИ агент

Для ускорения и облегчения работы пользователей в программе RT Protect TI в версии программы 3.3.0 появилась возможность использовать ИИ агента.

ИИ агент реализован в виде отдельного сервиса, разворачиваемого при деплое RT Protect TI.

С помощью конфигуратора при создании файла `config.yml` необходимого для разворачивания сервиса RT Protect TI, возможно отметить в разделе «Параметры работы с модулем TI Reports» флаг включения интеграции с сервисами AI, после чего указать URL на котором развернут сервис AI-агента и ключ доступа к сервису (URL и ключ при On-Premise установке запрашиваются заказчиком у поставщика).

ИИ агент доступен для всех пользователей RT Protect TI в рамках ролевой модели.

Запросы к агенту и получение ответов ограничены ролевой моделью пользователя под которой был осуществлен доступ к RT Protect TI.

Сервис ИИ агента для формирования запросов и ответов, касающихся работы в RT Protect TI использует API RT Protect TI.

Пользователем при формировании запросов к ИИ агенту создается сессия которая видна только для данного пользователя.

Одновременно можно создавать несколько сессий.

Общий вид страницы чата с ИИ агентом представлен на рисунке 102.

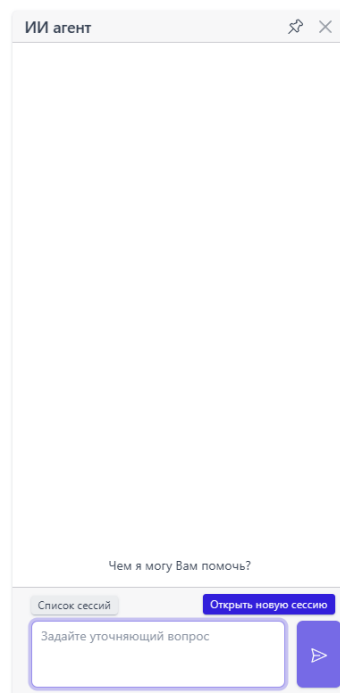


Рисунок 102 – Начало работы с ИИ агентом

Пример запроса к ИИ агенту и полученного ответа представлен на рисунке 103.

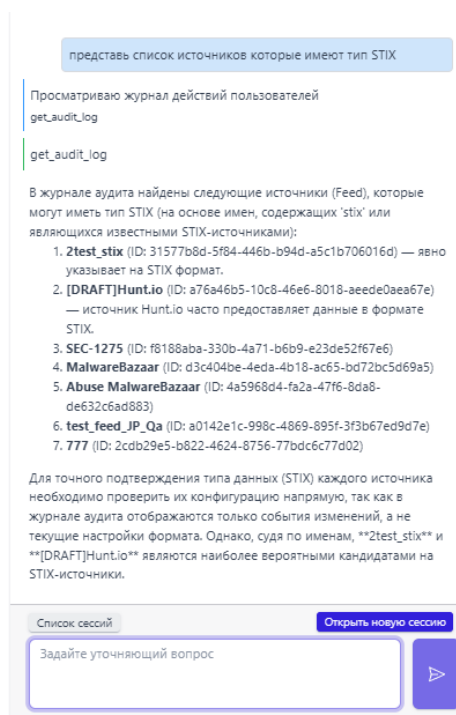


Рисунок 103 – Пример ответа от ИИ агента

5.5 Аналитика EDR

5.5.1. Индикаторы атак

Общая информация

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.

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 (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 выполняться за некоторое нормативное (но не гарантированное) сравнительно короткое время, чтобы прогресс атаки с момента ее обнаружения был минимальным.

Сервер TI может выступать в роли централизованной базы данных для индикаторов атак, применяемых на агентах всех серверов EDR, подключенных к RT Protect TI.

Определение индикаторов атак в RT Protect EDR

ИА 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 **Поля модели данных**)

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*-правил в качестве имени индикатора (например, `proc_creation_win_powershell_download_patterns`).

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» (`rule`) 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 **Типы индикаторов атак**

1. **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 **Синтаксис и семантика условных выражений индикаторов атак**.

2. **Критичность.** Критичность определяет соответствующий атрибут события-обнаружения, возникающего при срабатывании ИА.

3. **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).

4. **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.

5. **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.

6. **Описание.** Краткое описание активности, выявляемой ИА.

7. **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.

Типы индикаторов атак

Предусмотрено 25 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) Доступ к файлу (ACCESS);
- 13) Создание ключа реестра (CREATE KEY);
- 14) Удаление ключа реестра (DELETE KEY);
- 15) Изменение значения реестра (SET VALUE);
- 16) Переименование ключа реестра (RENAME KEY);
- 17) Событие журнала системы (EVENT LOG);
- 18) Загрузка драйвера (LOAD DRIVER);
- 19) Создание процесса (CREATE PROCESS);
- 20) Загрузка образа (LOAD IMAGE);
- 21) Доступ к стороннему процессу (OPEN PROCESS);
- 22) Создание нити (потока) в стороннем процессе (CREATE REMOTE THREAD);
- 23) Доступ к нити стороннего процесса (OPEN THREAD);
- 24) Загрузка образа в сторонний процесс (LOAD REMOTE IMAGE);
- 25) Загрузка сборки .NET (LOAD ASSEMBLY).



Важно

Для некоторых индикаторов атак можно задавать только детектирующее действие, это относится к таким типам индикаторов, как **Открытие локального порта на прием (LISTEN)**, **Событие журнала** и **Загрузка .NET-сборки**.

В системе RT Protect EDR условные выражения индикаторов атак являются логическими (т.е. результат выражения – это «истина» или «ложь») и имеют Си-подобный синтаксис.

Типы операндов

Операндами условных выражений ИА 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);
- time (время, временной штамп).

Битовые флаги исполняемого файла процесса (**exclfi**) и расшифровки для них представлены в таблице 7.

Таблица 7 – Флаги исполняемого файла процесса

Наименование флага	Расшифровка
PartialName	Неполное имя исполняемого модуля
TaskScheduler	Планировщик задач

AllowCodeInjection	Разрешение внедрения кода в сторонние программы
AllowWrite	Разрешение записи памяти сторонних программ
Rundll32	DLL-хост rundll32
PowerShell	Интерпретатор powershell
Cmd	Командный интерпретатор cmd
MsiExec	Установщик программы msiexec
Explorer	Проводник explorer
CSS	Критический системный компонент
Mshta	Хост HTML-приложений mshta
Svchost	Хост служб svchost
Lsass	Системный компонент LSASS
AllowControlRead	Разрешение чтения памяти сторонних программ и управления ими
Prefetcher	Служба Prefetcher Windows
ControlPanel	Панель управления Windows
ScriptEngine	Скриптовый движок
ImageWow64	Компонент имеет 32-х битную и 64-х битную версию
HostProcess	Хост-процесс
WhoAml	Утилита whoami
Csrss	Системный компонент CSRSS
TiWorker	Компонент подсистемы обновлений TiWorker
TCB	Максимальное доверие
NTDLL	Системная библиотека NTDLL
Vssadmin	Утилита управления резервным копированием vssadmin
Wmic	Утилита администрирования wmic
Wbadmin	Утилита администрирования wbadmin
BcdEdit	Утилита управления параметрами загрузки BCDEdit
DiskShadow	Утилита управления резервным копированием Diskshadow
Icacs	Утилита управления правами доступа к файлам iCACLs
Psexec	Утилита удаленного администрирования PsExec
VerifyTrust	Подтверждение по электронной подписи
SkipAllEvents	Исключение всей телеметрии
Browser	Браузер
Office	Офисная программа
AllowDirectDiskWrite	Разрешение прямого доступа к диску для записи
AllowDirectDiskRead	Разрешение прямого доступа к диску для чтения
CSSFriendly	Право взаимодействия с критическими системными программами
SkipNetEvents	Исключение из телеметрии сетевых событий
SkipFsEvents	Исключение из телеметрии файловых событий
SkipRegEvents	Исключение из телеметрии событий реестра Windows
AVEngine	Антивирусный компонент

SkipPmEvents	Исключение из телеметрии событий поведения
Verclsid	Утилита Verclsid
Regsvr32	Утилита Regsvr32
FsUtil	Утилита FsUtil
TrustedInstaller	Компонент подсистемы обновлений TrustedInstaller
TrustedDotNet	.NET-компоненты, которым есть доверие
CMSTP	Установщик профилей менеджера подключений Windows
WmiPrvSE	Хост WMI
InstallUtil	Утилита установки INF-файлов
Odbcconf	Утилита конфигурации ODBC
DismHost	Компонент DismHost
Dfsrs	Системный компонент Dfsrs
KnownDll	Известная DLL
DotNetNativelImage	Нативная версия .NET-сборки
KernelDll	Системная библиотека KERNEL32 или KERNELBASE
Advapi32	Системная библиотека ADVAPI32
RegAsm	Утилита регистрации .NET-сборки
Mavinject	Компонент платформы виртуализации приложений Windows
Mmc	Консоль управления Windows
Gacutil	Компонент управления GAC
Hh	Просмотрщик chm-файлов

Битовые флаги операции загрузки образа (**ldf**) и расшифровки для них представлены в таблице 8.

Таблица 8 – Флаги операции загрузки образа

Наименование флага	Расшифровка
ImageScriptEng	Скриптовый движок
ImageRenamed	Переименованный образ
ImageManaged	Управляемый образ
ImageRandomName	Имя образа похоже на случайную последовательность знаков
ImageRemap	Образ загружается повторно
ImageInjected	Образ внедрен сторонним процессом
ImageTransacted	На файле образа действует транзакция ФС
ImageUnsigned	Образ не имеет встроенной ЭП
ImageSigned	Образ имеет встроенную ЭП
ImageSyntheticLoad	Синтетическое событие
ImageSigningPropsAvailable	Имеется информация об ЭП, полученная от системы
ImageWhitelisted	Доверенный образ
ImageDeleted	Файл образа удален

ImagePostModified	Файл образа модифицирован после проецирования
-------------------	---

Битовые флаги поведенческих признаков процесса первой группы (rf0) и расшифровки для них представлены в таблице 9.

Таблица 9 – Флаги поведенческих признаков процесса (первая группа)

Наименование флага	Расшифровка
ProcHiveRoot	Главный процесс группы
Wow64	32-х битный процесс в 64-х битной системе
Native	Доверенный процесс
Synthetic	Событие создания процесса синтезировано
Managed	.NET-процесс
RunWithUAC	UAC-процесс
DroppedByParent	Процесс создал родитель и запустил
LaterStage	Основные системные модули загружены
IsInjected	API-вызовы процесса контролируются
FromExplorer	В цепочке родителей есть EXPLORER
SuspiciousDirectory	Каталог запуска: RECYCLER, System Volume Information и т.п.
HiddenDirectory	Каталог запуска: скрытый
FromInet	Исполняемый файл загружен из Интернета
TempDirectory	Каталог запуска: временный
SystemTempDirectory	Каталог запуска: системный временный
NetworkDirectory	Каталог запуска: сетевой путь
RemovableMedia	Каталог запуска: съемный носитель
AutorunDirectory	Каталог запуска: автозапуск
SystemDirectory	Каталог запуска: системный
ProgramFilesDirectory	Каталог запуска: Program Files
NetMalwareSignature	Срабатывание ИК в сетевом трафике: сигнатура
BlacklistedNetworkAccess	Попытка обращения по сети к заблокированным IP-адресам/доменным именам
NetworkServer	Прослушивание сетевого порта кроме loopback
NetworkAccess	Сетевой обмен (кроме loopback)
LoopbackAccess	Сетевое взаимодействие по loopback
RawSocketUse	Использование raw-сокетов
NetIOC	Срабатывание ИК в сетевом трафике: IP-адрес/доменное имя
NtAllocateVirtualMemory	Выделение памяти в стороннем процессе
NtAllocateVirtualMemoryEx	Выделение памяти в стороннем процессе/расширенное
NtDeviceIoControlFile	Взаимодействие с драйверами
NtGetContextThread	Получение контекста нити стороннего процесса
NtMapViewOfSection	Проецирование секции в сторонний процесс

NtMapViewOfSectionEx	Проецирование секции в сторонний процесс расширенное
NtProtectVirtualMemory	Изменение атрибутов защиты памяти стороннего процесса
NtQueryInformationThread	Получение информации о нити стороннего процесса
NtQueueApcThread	Отправка APC-нити стороннего процесса
NtQueueApcThreadEx	Отправка APC-нити стороннего процесса расширенная
NtReadVirtualMemory	Чтение памяти стороннего процесса
NtResumeThread	Возобновление работы нити стороннего процесса
NtSetContextThread	Установка контекста нити стороннего процесса
NtSetInformationProcess	Управление сторонним процессом
NtSetInformationThread	Управление нитью стороннего процесса
NtSuspendThread	Приостановка работы нити стороннего процесса
NtUnmapViewOfSection	Отмена проекции секции стороннего процесса
NtUnmapViewOfSectionEx	Отмена проекции секции стороннего процесса расширенная
NtWriteVirtualMemory	Запись памяти стороннего процесса
Tampering	Применение техник подмены исполняемых образов
PostModified	Исполняемый файл модифицирован после проецирования
Deleted	Исполняемый файл удален
Renamed	Исполняемый файл переименован
FromServices	В цепочке родителей есть диспетчер служб
FromBrowser	В цепочке родителей есть браузер
FromOffice	В цепочке родителей есть офисная программа
Protected	Защищенный процесс
Transacted	Транзакция на исполняемом файле
Trustlet	Изолированный процесс
WhiteListed	Известный легальный
Trusted	Подписан
Untrusted	Не подписан
Elevated	Повышенные привилегии

Битовые флаги поведенческих признаков процесса второй группы (rf1) и расшифровки для них представлены в таблице 10.

Таблица 10 – Флаги поведенческих признаков процесса второй группы

Наименование флага	Расшифровка
RegSecurityModify	Модификация security элементов реестра
RegStorePE	Запись потенциального исполняемого файла в реестр
InstallService	Регистрация службы в реестре
RegAsepModify	Модификация точек автозапуска реестра

MshtaRun	Запуск утилиты mshta
Regsvr32Run	Запуск утилиты regsvr32
VerclsidRun	Запуск утилиты verclsid
SystemRestoreDisable	Выключение механизма восстановления системы
IcaclsRun	Запуск icacls
HhRun	Запуск просмотрщика chm-файлов
GacutilRun	Запуск утилиты управления GAC
PsexecRun	Запуск psexec
PowerShellRun	Запуск powershell
CmdScriptRun	Запуск cmd /c
TaskManage	Запуск планировщика задач с параметрами /create или /change
MsiExecRun	Запуск msixexec
Rundll32Run	Запуск rundll32
ScriptRun	Запуск скриптового интерпретатора
WhoAmIRun	Выполнение команды whoami
ShellCodeExec	Выполнение shell-кода
ContainsManagedCode	Содержит .NET-код
MapRemoteView	Проецирование образа в сторонний процесс
DoSpoonParentId	Подмена родителя дочернему процессу
CreateRemoteThread	Создание нити в стороннем процессе
CmdLineTampering	Подмена командной строки
OpenThread	Открытие сторонней нити
OpenProcess	Открытие стороннего процесса
ControlPanelRun	Запуск панели управления Windows
CMSTPRun	Запуск установщика профилей диспетчера подключений Windows
InstallUtilRun	Запуск установщика INF-файлов
OdbcconfRun	Запуск утилиты администрирования ODBC
RegAsmRun	Запуск утилиты регистрации .NET-сборок
MavinjectRun	Запуск средства виртуализации приложений Windows
MmcRun	Запуск консоли управления Windows
Unprotected	Нештатно уменьшен уровень защиты
ProtectionElevated	Нештатно увеличен уровень защиты
HasRemoteView	Содержит спроецированный извне образ
Tampered	Подменен образ исполняемого файла
HasRemoteThread	Содержит нить, созданную извне
ThreadOpen	Открытие нити процесса извне
ProcessOpen	Открытие процесса извне
MemoryWritten	Память процесса записана извне
MemoryRead	Память процесса прочитана извне
MemoryMadeExecutable	Участок памяти процесса извне отмечен как исполняемый код

SpoofParentId	Подменен родительский процесс
RegisterTask	Создание файлов в каталоге задач
SetAutorun	Создание файлов в каталоге автозапуска
CreateMofFile	Создание *.mof-файлов в каталоге WMI
ReadSystemPEFile	Чтение системных исполняемых файлов, не связанное с их запуском
WriteExeFile	Запись в исполняемые файлы
NamedPipeClient	Клиент именованного канала
FileNameHasStreamComponent	В имени исполняемого файла присутствует компонент ntfs-потока
UnusualExeFileExtension	Имя исполняемого файла имеет нетипичное расширение
RandomFileName	Случайное имя файла
NamedPipeServer	Сервер именованного канала
CreateExeFile	Создание файлов с потенциально активным содержимым

Состав операторов

Набор операторов, доступных в условных выражениях ИА 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 ?;

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 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`).

Поля модели данных

Модель данных `sysmon` частично поддерживается в форме набора синонимов над мнемониками нативной модели RT Protect EDR, а соответственно и TI-сервером. Полный перечень синонимов `sysmon`, а также их соответствие типам ИА и полям нативной модели данных событий описаны в таблице 11.

Таблица 11 – Модель 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
TerminalSessionId	uint	любой	sess
User	string	любой	sid
CommandLine	string	любой	cmdl
CallTrace	string	любой	trace

Имя	Тип поля	Тип ИА	Нативное имя
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	*
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
FileVersion	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	fver
Description	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	fdecs
Company	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	fcomp
Product	string	CREATE PROCESS LOAD IMAGE	fprod

Имя	Тип поля	Тип ИА	Нативное имя
		LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	
OriginalFileName	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	ofn
Signature	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	sgnr
SignatureStatus	uint	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	sgnr_s
Signed	bool	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	*
Hashes	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	*
ImageLoaded	string	LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	path
TargetProcessId	uint	OPEN PROCESS OPEN THREAD CREATE REMOTE THREAD LOAD REMOTE IMAGE	tpid
TargetImage	string	OPEN PROCESS CREATE REMOTE THREAD LOAD REMOTE IMAGE	tpath
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	name

Имя	Тип поля	Тип ИА	Нативное имя
		ACCESS	
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).

Нативные поля для написания индикаторов атак описаны в таблице 12.

Таблица 12 – Поля для написания индикаторов атак

Наименование поля	Расшифровка
Act	Действие, связанное с событием
Time	Время регистрации события
Pid	Идентификатор процесса на агентской системе
Ppid	Идентификатор родительского процесса на агентской системе
App	Полное имя исполняемого файла процесса
Cmdl	Командная строка процесса
Sess	Номер сессии, в которой работает процесс на агентской системе
rf0	Поведенческие признаки процесса (первая группа)
rf1	Поведенческие признаки процесса (вторая группа)
Exclf	Флаги исполняемого файла процесса
Sid	SID пользователя, создавшего процесс
agent_build_number	Номер сборки агента
History	История сработавших индикаторов атак
Proto	Протокол
ipv6	Признак работы по IPv6
Out	Отправка (1) или прием (0)
Size	Размер полезных данных (payload) сетевого пакета
Host	Имя хоста, соответствующее удаленному ip
ssl_h	Имя хоста (server_name) из сообщения SSL Client Hello
dnsq_h	Имя хоста из DNS-запроса
dnsq_t	Тип DNS-запроса

Наименование поля	Расшифровка
dnsq_s	Статус DNS-запроса
dnsq_r	Результат DNS-запроса
r_p	Удаленный порт
r_ip	Удаленный IP-адрес
l_p	Локальный порт
l_ip	Локальный IP-адрес
Who	Полное имя исполняемого модуля–инициатора операции
Whof	Флаги исполняемого модуля–инициатора операции
Whotid	Идентификатор нити–инициатора операции
whoaddr	Стартовый адрес нити–инициатора операции
Trace	Стек вызовов операции
Wdir	Рабочий каталог процесса
Cmdlp	Командная строка родительского процесса
Cmdlg	Командная строка прародителя (grand parent)
When	Время создания процесса
Cpath	Полное имя процесса-инициатора операции
Prot	Уровень защиты процесса
Base	Базовый адрес образа
Isizе	Размер образа
Crtime	Время создания файла
Chtime	Время последнего изменения файла
Fsize	Размер файла
Ftype	Тип файла
Attr	Атрибуты файла
sha1	SHA-1 файла
md5	MD5 файла
sha256	SHA-256 файла
Sgnr	Электронная подпись файла
sgnr_s	Статус электронной подписи файла
Pack	Тип упаковщика файла
Ofn	Оригинальное имя файла
Fcomp	Компания-издатель файла
Fver	Версия файла
Fdesc	Описание файла
Fprod	Продукт, к которому относится файл
Path	Полное имя файла образа
lmgf	Флаги образа
Ldf	Флаги операции загрузки образа
Tpath	Полное имя целевого процесса

Наименование поля	Расшифровка
Tpid	Идентификатор целевого процесса
Targf	Флаги образа целевого процесса
trf0	Поведенческие признаки целевого процесса (первая группа)
trf1	Поведенческие признаки целевого процесса (вторая группа)
Tid	Идентификатор целевой нити
Taddr	Стартовый адрес целевой нити
Tf	Флаги нити
Dsrd	Запрашиваемые права
Grnt	Предоставленные права
Asep	Ключ/значение относится к категории автозапуска
Key	Путь ключа
val_n	Имя значения
val_t	Тип данных значения
val_s	Размер данных значения
val_d	Данные значения
Name	Полное имя файла
Fnew	Новое имя файла
Delete	Доступ на удаление
Read	Доступ на чтение
Modify	Доступ на модификацию
Save	Для файла была создана резервная копия
Ads	Операция совершается над альтернативным потоком данных файла
Arun	Файл расположен в директории автозапуска
Owrt	Файл был заменен

Наборы индикаторов атак

Страница с наборами индикаторов атак (рис. 104) включает в себя следующие структурные элементы:

- Фильтры;
- таблица с наборами индикаторов атак;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы;
- кнопка Сбросить фильтры.

Индикаторы атак

Название набора: Поиск по полям набора: Автор / Пользователь:

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
123111	Доступен всем	0	14.05.2025, 16:25:48	14.05.2025, 16:25:38	14.05.2025, 16:25:48	✎ ✖
123111	Доступен всем	0	14.05.2025, 16:02:38	14.05.2025, 16:02:00	14.05.2025, 16:02:21	✎ ✖
123111	Доступен всем	0	14.05.2025, 15:14:58	14.05.2025, 16:25:35	14.05.2025, 15:14:58	✎ ✖
123111	Доступен всем	0	14.05.2025, 15:06:38	14.05.2025, 15:07:25	14.05.2025, 15:06:31	✎ ✖
123111	Доступен всем	0	14.05.2025, 14:52:14	14.05.2025, 15:04:49	14.05.2025, 14:52:14	✎ ✖
123111	Доступен всем	0	14.05.2025, 13:59:51	14.05.2025, 13:59:51	14.05.2025, 13:59:51	✎ ✖
test distributed	Доступен всем	0	14.05.2025, 13:59:58	14.05.2025, 16:27:17	14.05.2025, 13:59:58	✎ ✖
[WIN] Базовый (v4)	Доступен всем	208	12.05.2025, 18:28:48	12.05.2025, 18:28:58	12.05.2025, 18:28:58	✎ ✖
[WIN] СТРОИТЕЛЬ (v4)	Доступен всем	21	12.05.2025, 18:28:07	12.05.2025, 18:28:23	12.05.2025, 18:28:23	✎ ✖
[WIN] Базовый (v7)	Доступен всем	515	12.05.2025, 18:14:51	12.05.2025, 18:14:59	12.05.2025, 18:14:59	✎ ✖

Добавить набор

Рисунок 104 – Наборы индикаторов атак

В таблице с наборами индикаторов содержатся следующие поля:

- Название набора;
- Доступен организациям;
- **Количество записей** (показывает, сколько индикаторов атак содержится в наборе);
- **Дата создания/Автор** (отображается дата создания набора и автор, создавший набор);
- **Дата изменения/автор** (отображается дата изменения и автор изменивший набор);
- **Дата последнего сохранения** (отображается дата последнего сохранения набора);
- Действия (содержит кнопки Редактировать, Удалить).

Для фильтрации информации на странице имеются следующие фильтры:

- Название набора;
- **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: Значение,

Издатель ЭП, Правила, Комментарий);

- Автор/Пользователь;
- Дата создания/изменения.

На странице пользователь может выполнить следующие операции:

- просматривать ранее созданные наборы индикаторов атак;
- добавлять новые наборы;
- редактировать название выбранного набора;
- применить изменения выбранного набора;

— удалять выбранные наборы.

Рядом с именем набора имеется иконка , которая показывает, что набор не был сохранен в файл, который экспортируется другим потребителям, подключенным к серверу аналитики.

Кнопка  позволяет сохранить и обновить файл, который используется всеми серверами EDR как база с индикаторами атак. Точно такой же файл экспорта есть у всех разделов аналитики и исключений.

Для перехода к странице **Индикаторы атак** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Индикаторы атак»

На странице **Индикаторы атак** содержится информация о правилах. Правила позволяют проводить динамический анализ событий, поступающих с агента в системах типа EDR. Кроме того, страница содержит инструменты конфигурирования этих правил и ссылки на MITRE ATT&CK.

Ссылки приводятся на те правила, которые описывают детектирование известных и указанных в базе знаний MITRE ATT&CK техник проникновения и атак на компьютерные сети и системы (рис. 105).

Индикаторы атак vp-test-10a-1

Поиск по полям набора

Имя: Условие: Тип:

Критичность (не менее): MITRE: Действие: Комментарий:

Описание: Признак активации: Автор / Пользователь:

Дата создания / изменения: ☒ Список ☐ Календарь

Показывать по:

	Имя	Тип	Критичность / Действия	MITRE	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☒	10a_2	Сет. Входящее подключение			14.03.2025, 13:46:52	18.03.2025, 17:05:11 homer@simpson.ru	
☒	10a_3	Сет. SSL HELLO			14.03.2025, 13:46:52		
☒	10a_2	Сет. Входящее подключение			14.03.2025, 13:44:52		
☒	10a_3	Сет. SSL HELLO			14.03.2025, 13:44:52		
☒	10a_4x	Сет. DNS-ответ			12.03.2025, 11:33:33 test_SP@rt.ru	14.03.2025, 15:19:23 homer@simpson.ru	
☒	10a_3	Сет. SSL HELLO			12.03.2025, 11:33:33 test_SP@rt.ru		
☒	10a_2	Сет. Входящее подключение			12.03.2025, 11:33:33 test_SP@rt.ru		
☒	10a_test1	Сет. Входящее подключение			12.03.2025, 11:33:33 test_SP@rt.ru		
☒	10a_test1	Сет. Входящее подключение			12.03.2025, 11:33:33 test_SP@rt.ru		
☒	10a_4	Сет. DNS-ответ			12.03.2025, 10:17:48		

Найдено: 55, показано с 1 по 10

Добавить индикатор

Удалить выбранные

Рисунок 105 – Индикаторы атак

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

— **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);

- Имя;
- Условие;
- Тип;
- Критичность (не менее);
- MITRE;
- Действие;
- Комментарий;
- Описание;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

На странице с индикаторами атак можно выполнить следующие операции:

- просматривать информацию о ранее созданных индикаторах;
- создать новый индикатор атаки;
- выполнить поиск по имени индикатора;
- выполнить поиск по условию индикатора;
- копировать индикатор атаки из одного набора в другой;
- переместить индикатор атаки из одного набора в другой;
- экспортировать индикатор в файл;
- импортировать данные из файла;
- активировать/деактивировать индикатор атаки;
- редактировать индикатор атаки;
- удалить индикаторы атак из набора.

Для добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы. В открывшемся окне **Добавить индикатор** (рис. 106) следует прописать условия, на основании которых будет срабатывать правило.

Рисунок 106 – Добавление индикатора

После написания условия необходимо нажать кнопку **Добавить**. В нижней части страницы появится сообщение о добавлении нового правила (рис. 107).

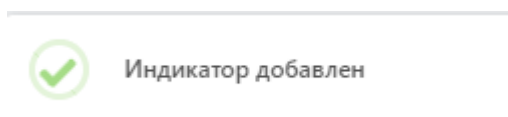


Рисунок 107 – Сообщение о добавлении индикатора атаки

При написании индикаторов атак отдельные элементы условия будут подсвечиваться (операторы, значения полей).

Написание условий подразумевает проверку синтаксиса, которая запускается или с помощью кнопки в нижней части окна () или при сохранении индикатора атаки.

Для создания индикатора и его дальнейшего применения необходимо, чтобы условие не противоречило синтаксису правил.

Для редактирования индикатора следует нажать кнопку **Редактировать**  в строке выбранного индикатора атаки и в открывшемся окне **Редактировать индикатор** внести необходимые изменения (рис.108).

Если во время редактирования перейти на вкладку **Конструктор**, то условие необходимо переписывать полностью, редактировать часть условия индикатора атаки возможно только в ручном режиме.

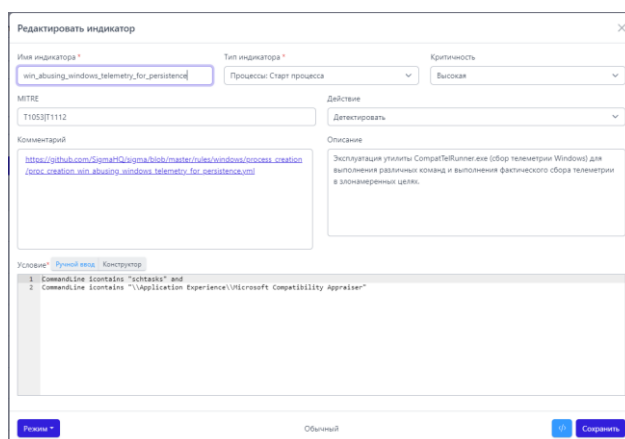


Рисунок 108 – Редактирование индикатора атаки

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении правила (рис. 109).

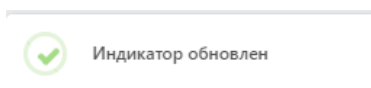


Рисунок 109 – Сообщение об обновлении индикатора атаки

В выпадающем списке **Режим** пользователь может установить режим обнаружения индикатора атаки.

Доступны следующие режимы:

- 1) Обычный (без определенных условий);
- 2) Без генерации обнаружения (инцидент создаваться не будет);
- 3) Однократная генерация обнаружения (будет создан только один инцидент, даже если событие, которое сгенерировало инцидент, произойдет неоднократно).

Чтобы экспортировать индикаторы атак в файл, необходимо нажать кнопку . Экспорт производится в файл формата CSV и JSON. Файл сохранится в директории **Загрузки**. Экспортируется выбранный набор целиком.

Чтобы импортировать индикаторы атак из файла в выбранный набор, необходимо нажать кнопку , после чего выбрать файл с импортируемыми индикаторами и нажать кнопку **Открыть**.

Для активации/деактивации правила необходимо нажать кнопку  или  в поле **Управление**. Деактивация или активация правила тоже считается изменением в наборе, поэтому информация о пользователе, выполнившем это действие, будет отображаться в поле **Последнее изменение/Пользователь**.

Для удаления индикатора атаки необходимо выбрать его с помощью кнопки выбора, установив флажок, после чего нажать кнопку **Удалить выбранные**. Также можно нажать кнопку  в строке с индикатором.

Для завершения операции ее необходимо подтвердить в открывшемся окне **Подтверждение действия**.

5.5.2. Индикаторы компрометации

Индикаторы компрометации, 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 только по имени файла.

Индикаторы по хэш-сумме файла работают только для файлов с активным содержимым. К файлам с активным содержимым в текущей реализации относятся исполняемые файлы (определяются по формату или расширению EXE, DLL, SYS, COM, OCX, SCR, CPL), а также файлы с расширениями PDF, PS1, PSM1.

При обращении к файлу, хэш-сумма которого совпадает с хэш-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. Таким образом блокируются все операции с файлом, изолируя его «по месту», без перемещения в карантин. Запуск исполняемого файла, хэш 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.

Общая информация

При открытии раздела **Индикаторы компрометации** администратор видит информацию о наборах с индикаторами компрометации. Обнаружение событий, связанных с описанными в наборах компрометации артефактами, вызывает определенное действие, зафиксированное в наборе. Таким действием может быть блокирование или детектирование вызываемого процесса, связанного с артефактом (например, блокируется открытие сайта, связанного с блокируемым доменом).

Наборы индикаторов компрометации

Страница **Индикаторы компрометации** представлена на рисунке 110. На странице отображаются наборы с индикаторами компрометации, сохраненные на сервере аналитики.

☐	Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	string	Доступен всем	0	07.05.2025, 15:16:55		07.05.2025, 15:16:55	
☐	teteeteet	Доступен всем	2	15.04.2025, 16:18:30		15.04.2025, 16:18:30	
☐	qtwefqwe	Доступен всем	9	17.03.2025, 14:54:12		17.03.2025, 14:54:12	
☐	asfsofso	Доступен всем	0	17.03.2025, 14:54:09		17.03.2025, 14:54:09	
☐	ewiqeww	Доступен всем	0	17.03.2025, 14:54:07		17.03.2025, 14:54:07	
☐	erhwreh	Доступен всем	0	17.03.2025, 14:54:03		17.03.2025, 14:54:03	
☐	vqewqeww	Доступен всем	0	17.03.2025, 14:54:01		17.03.2025, 14:54:01	
☐	asdfsasf	Доступен всем	0	17.03.2025, 14:53:58		17.03.2025, 14:53:58	
☐	for_test_3	Доступен всем	0	22.04.2025, 17:22:36			
☐	for_test_2	Доступен всем	0	22.04.2025, 17:15:12			

Рисунок 110 – Наборы индикаторов компрометации

Информация на странице представлена в табличном виде. В шапке таблицы представлены следующие поля:

- 1) Кнопка выбора (отмечена элементом);
- 2) Название набора;
- 3) Доступен организациям;
- 4) Количество записей;
- 5) Дата создания/Автор (показывает, когда и кто создал набор);

6) **Последнее изменение/Пользователь** (показывает, когда и кто производил последние изменения с набором);

7) **Действие** (содержит кнопки **Редактировать** (позволяет редактировать название набора) и **Удалить**).

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Название набора;
- **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Автор/Пользователь;
- Дата создания/изменения.

В нижней части страницы **Индикаторы компрометации** находятся кнопки **Добавить набор** и **Удалить выбранные наборы**. Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Создать набор** (рис. 111) в строке **Название** ввести название нового набора.

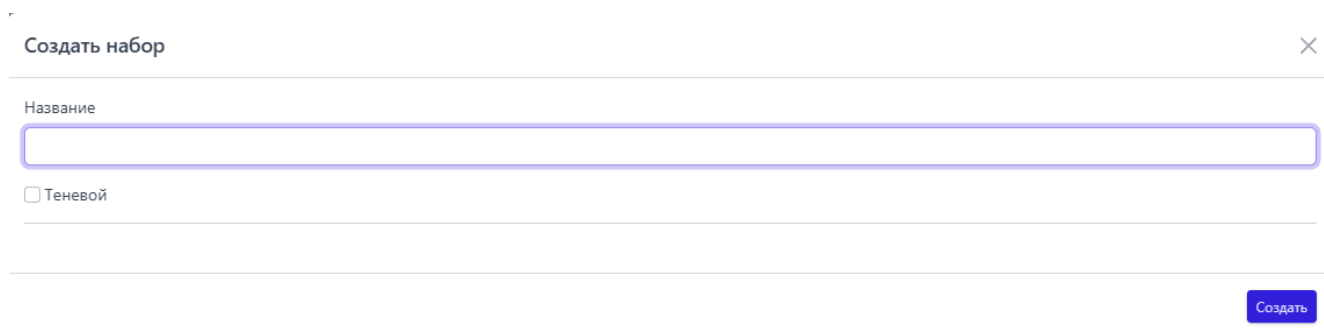


Рисунок 111 – Окно «Создать набор»

Для завершения операции добавления необходимо нажать кнопку **Создать**, после чего в нижней части страницы появится сообщение о добавлении набора (рис. 112), а строка с новым набором появится в таблице.



Рисунок 112 – Сообщение о добавлении набора

Для удаления одного или нескольких наборов индикаторов компрометации следует отметить флажками соответствующие им кнопки выбора , после чего нажать кнопку **Удалить выбранные наборы**.

Страница «Индикаторы компрометации»

Переход на страницу с таблицей **Индикаторы компрометации** происходит при нажатии ЛКМ на названии набора в таблице с наборами индикаторов компрометации.

На странице **Индикаторы компрометации** пользователь может выполнить следующие операции:

- просматривать информацию об индикаторах, входящих в выбранный набор;
- создавать новые индикаторы компрометации;
- изменять индикаторы компрометации, входящие в выбранный набор;
- экспортировать индикаторы в файлы формата CSV;
- импортировать данные из файла в набор индикаторов;
- активировать/деактивировать выбранные индикаторы компрометации;
- удалять из набора выбранные индикаторы компрометации.

В верхней части области **Индикаторы компрометации** отображается имя набора и фильтр **Показывать по** (возможно задавать значения **10, 20, 50 и 100**), **Имя индикатора**, **Артефакт** (фильтрует по значению артефакта), **Тип** (фильтрует по типу артефакта).

Шапка таблицы с индикаторами содержит следующие поля:

- 1) Кнопка выбора (отмечена элементом 
- 2) **Имя** (отображается название индикатора);
- 3) **Тип артефакта** (имя файла, SHA-256, IP-адрес, доменное имя, сетевая сигнатура, TLSH, подпись, SHA-1, MD5, URL);
- 4) **Артефакт**;
- 5) **Комментарий**;
- 6) **Дата создания/Автор**;
- 7) **Последнее изменение/Пользователь**;
- 8) **Действия** (в поле содержатся кнопки активации/деактивации индикатора, кнопки **Редактировать** и **Удалить**).

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

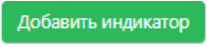
— **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);

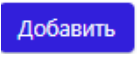
- Имя индикатора;
- Артефакт;
- Тип индикатора;
- Комментарий;
- Описание;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

В нижней части таблицы индикаторов находятся кнопки операций с индикаторами:

- 1)  ;
- 2) Сохранить набор в файл экспорта ();
- 3) Импортировать CSV-файл –  ;
- 4) Экспортировать набор в файл формата CSV;
- 5) Удалить индикатор или индикаторы  .

Для добавления индикатора в области **Индикаторы компрометации** необходимо нажать кнопку

 .

Далее в открывшемся окне **Добавить индикатор** (рис. 113) следует заполнить поля, обязательными для заполнения из которых являются поля **Имя индикатора**, **Тип индикатора** и **Артефакт**, после чего нажать кнопку  .

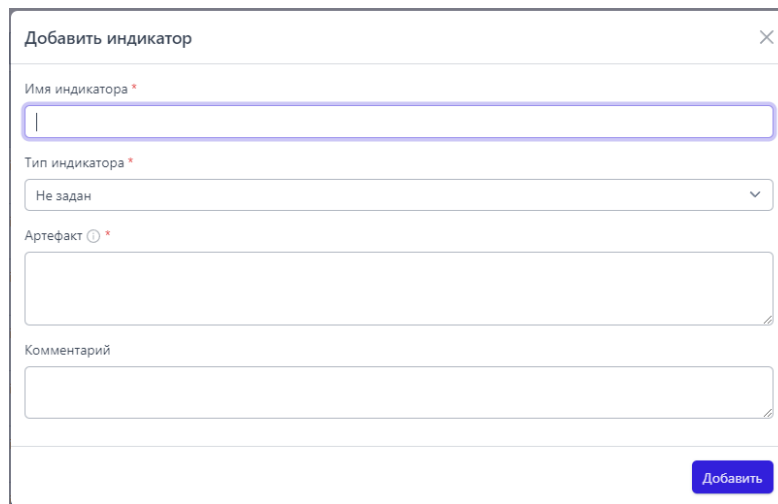


Рисунок 113 – Окно «Добавить индикатор»

В нижней части страницы появится сообщение о добавлении индикатора компрометации (рис. 114).



Рисунок 114 – Сообщение о добавлении индикатора

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата csv** . Созданный файл будет сохранен в папку, в которую настроена загрузка файлов в операционной системе. Для импорта данных из файла с индикаторами следует нажать кнопку  **Импортировать CSV-файл**. После нажатия кнопки открывается окно файлового менеджера, 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 индикаторов компрометации.

5.5.3. Журналы

Общая информация

Правила, создаваемые в разделе **Журналы**, позволяют отслеживать события ETW-системы для Windows. Для этого пользователь, используя инструментарий сервера аналитики, может подписаться на события определенного провайдера.

Наборы с журналами

Страница с наборами журналов (рис. 115) открывается при выборе на панели слева раздела **Журналы** и включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- фильтры и элемент Показывать по;
- таблица с наборами журналов (Windows);
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы.

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
1111	Доступен всем	2	17.03.2025, 15:40:00		17.03.2025, 15:40:00	✎ ✖
21312	Доступен всем	1	17.03.2025, 15:37:43		17.03.2025, 15:37:43	✎ ✖
Irina_Test	Доступен всем	1	10.03.2025, 16:49:19		10.03.2025, 16:49:19	✎ ✖
123	Доступен всем	5	17.02.2025, 17:47:20		03.03.2025, 18:19:43	✎ ✖
test-qa	Доступен всем	4	30.01.2025, 11:58:42		03.03.2025, 18:20:15	✎ ✖
test_api	Доступен всем	3	19.11.2024, 17:33:19		19.11.2024, 17:33:19	✎ ✖
PMI_Test_1.1	Доступен всем	2	11.11.2024, 19:24:32		19.11.2024, 17:13:58	✎ ✖
WinEvt-Test	Доступен всем	0	03.09.2024, 17:58:33		03.09.2024, 17:58:33	✎ ✖
test_QA1	Доступен всем	3	09.08.2024, 17:27:05	29.01.2025, 17:33:18	30.01.2025, 18:54:42	✎ ✖
fghfg	Доступен всем	0	17.07.2024, 14:06:56		17.07.2024, 14:06:56	✎ ✖

Рисунок 115 – Наборы с журналами

На странице используется следующая система фильтров:

- Поиск по полям набора;
- Имя журнала;
- Признак активации;
- Автор/пользователь;
- Дата создания/Изменения.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Создать набор** ввести название нового набора журналов. Для завершения операции необходимо нажать кнопку **Создать**. Для удаления набора необходимо нажать кнопку **Удалить** (🗑️) или **Удалить выбранные наборы**.

При нажатии ЛКМ на имени набора открывается страница **Журналы** для выбранного набора (рис. 116).

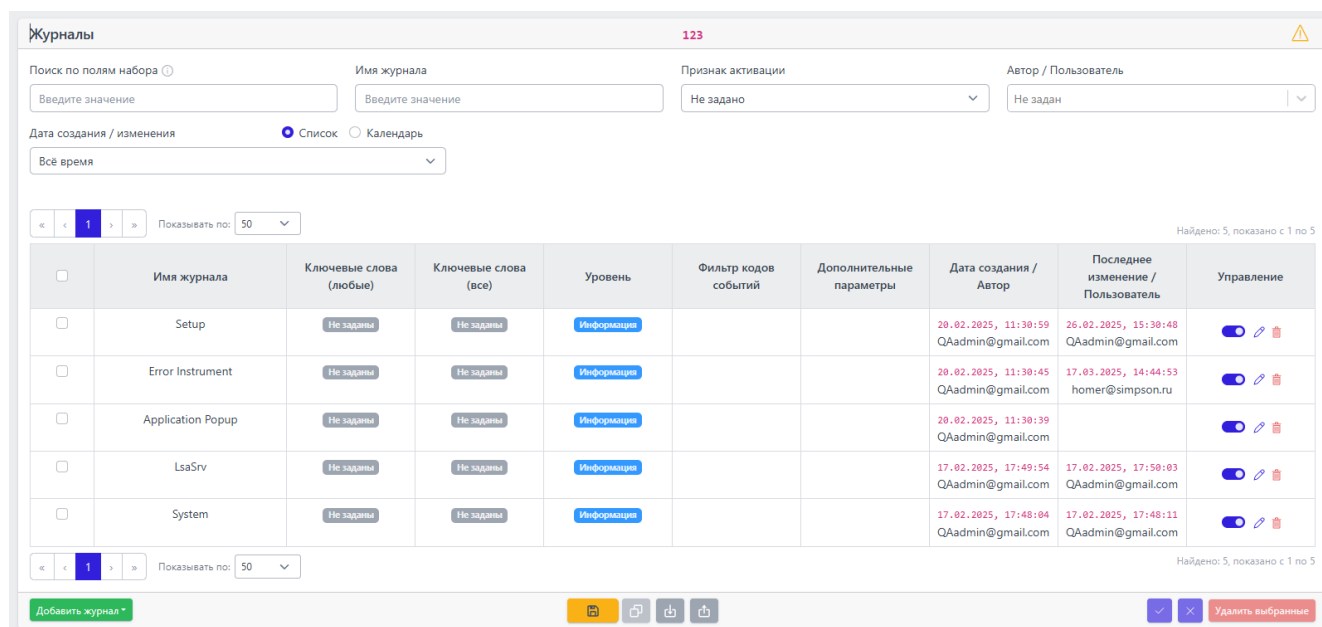


Рисунок 116 – Страница «Журналы»

Страница «Журналы»

На странице **Журналы** можно выполнять следующие операции:

- просматривать ETW-журналы из выбранного набора;
- добавлять новые журналы в выбранный набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать журнал;
- редактировать настройки логирования выбранного журнала;
- удалить выбранный журнал из набора.

На странице используется следующая система фильтров:

- Поиск по полям набора;
- Имя журнала;

- Признак активации;
- Автор/пользователь;
- Дата создания/Изменения.

Для добавления нового журнала необходимо нажать кнопку **Добавить журнал**, после чего выбрать, добавлять журнал по GUID или по именованному каналу.

В зависимости от выбора откроется окно **Добавить журнал по GUID** или **Добавить журнал по именованному каналу**. В этих окнах необходимо указать требуемые для выбранного провайдера параметры логирования.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата CSV** (). Набор будет сохранен в папке **Загрузки** в указанном формате. Для импорта журналов из файла требуется нажать кнопку **Импортировать CSV-файл** (). Далее выбрать на компьютере файл, содержащий нужные журналы, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать журнал из выбранного набора, необходимо нажать кнопку  или . Действия требуют подтверждения в отдельном окне.

Для удаления журнала(ов) из набора необходимо отметить флажками журнал(ы), который(е) требуется удалить и нажать кнопку **Удалить выбранные** или удалить журналы по отдельности с помощью кнопки **Удалить** ().

Для редактирования условий логирования выбранного провайдера следует нажать кнопку **Редактировать** () , после чего внести изменения в открывшемся окне с журналом. После внесения изменений в журнал необходимо нажать кнопку **Сохранить**.

5.5.4. Yara-правила (файлы)

Общая информация

Правила, указанные в разделе **YARA-правила (файлы)**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа вредоносных файловых сигнатур.

Подробное описание структуры правил, особенностей их написания и работы с YARA-правилами содержится в документе «Руководство аналитика RT Protect TI».

Наборы YARA-правил (файлы)

Страница с наборами YARA-правил для файлов (рис. 117) включает в себя следующие структурные элементы:

- таблица с наборами YARA-правил;
- кнопка **Добавить набор**;
- кнопка **Удалить выбранные наборы**.

The screenshot shows the 'YARA-правила (файлы)' interface. At the top, there are filters for 'Название набора', 'Поиск по полям набора', 'Автор / Пользователь', and 'Дата создания / изменения'. Below the filters is a table with columns: 'Название набора', 'Доступен организациям', 'Количество записей', 'Дата создания / Автор', 'Дата изменения / Автор', 'Дата последнего сохранения', and 'Действия'. The table contains 10 rows of data. At the bottom, there are buttons for 'Добавить набор' and 'Удалить выбранные', and a footer indicating 'Экспортируемые наборы из основного раздела'.

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
set_sk	Доступен всем	9	22.04.2025, 17:02:03		22.04.2025, 17:02:26	
Irma_Test	Доступен всем	0	10.03.2025, 16:53:43		10.03.2025, 16:53:43	
проверка_2	Доступен всем	1	24.01.2025, 12:06:04		24.01.2025, 12:11:48	
Проверка	Доступен всем	28	24.01.2025, 11:59:39		28.02.2025, 16:55:55	
ABC	Доступен всем	1	20.11.2024, 14:23:26		14.04.2025, 16:59:00	
abcd	Доступен всем	0	12.11.2024, 17:25:54	10.11.2024, 14:15:44	03.03.2025, 18:23:14	
test	Доступен всем	1	12.11.2024, 17:24:11		12.11.2024, 17:24:12	
PMI_Test_1.1	Доступен всем	1	11.11.2024, 19:38:40		11.11.2024, 19:32:52	
111	Доступен всем	0	06.11.2024, 14:37:03		06.11.2024, 14:37:16	
new_name	Доступен всем	0	06.11.2024, 12:35:22	06.11.2024, 12:50:10	06.11.2024, 12:35:22	

Рисунок 117 – Наборы YARA-правил (файлы)

Для фильтрации информации на странице имеется система фильтров, представленная в списке:

- Название набора;
- Поиск по полям набора;
- Автор/пользователь;
- Дата создания/Изменения.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Добавить набор** ввести название нового набора YARA-правил. Для завершения операции необходимо нажать кнопку **Добавить**.

Для удаления набора необходимо нажать кнопку **Удалить** () или **Удалить выбранные наборы**.

При нажатии ЛКМ по имени набора открывается страница YARA-правила для выбранного набора (рис. 118).

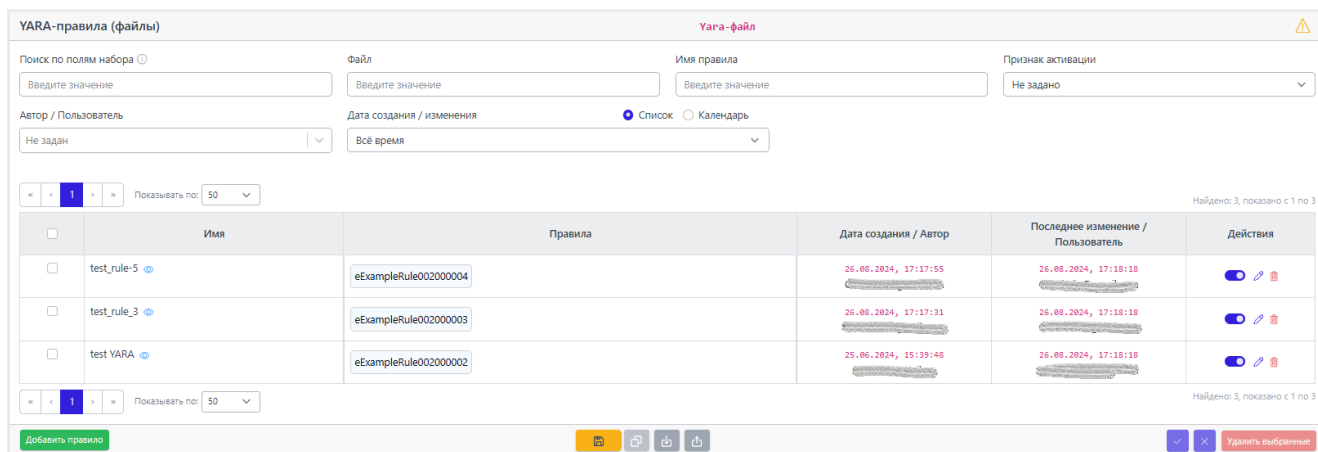


Рисунок 118 – YARA-правила

На странице YARA-правила (файлы) можно выполнять следующие операции:

- просматривать правила из выбранного набора;
- добавлять новые правила в выбранный набор;
- применять наборы после изменения правил;
- копировать/перемещать выбранные правила в другой набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать правило;
- редактировать выбранное правило;
- удалить выбранное правило из набора.

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Поиск по полям набора;
- Файл;
- Имя правила;
- Признак активации;

- Автор/Пользователь;
- Дата создания/изменения.

Для добавления нового правила необходимо нажать кнопку **Добавить правило**.

Подробная информация о синтаксисе YARA содержится в документе «Руководство аналитика RT Protect EDR» и [официальной документации YARA](#). Пример правила YARA приведен на рисунке 119.

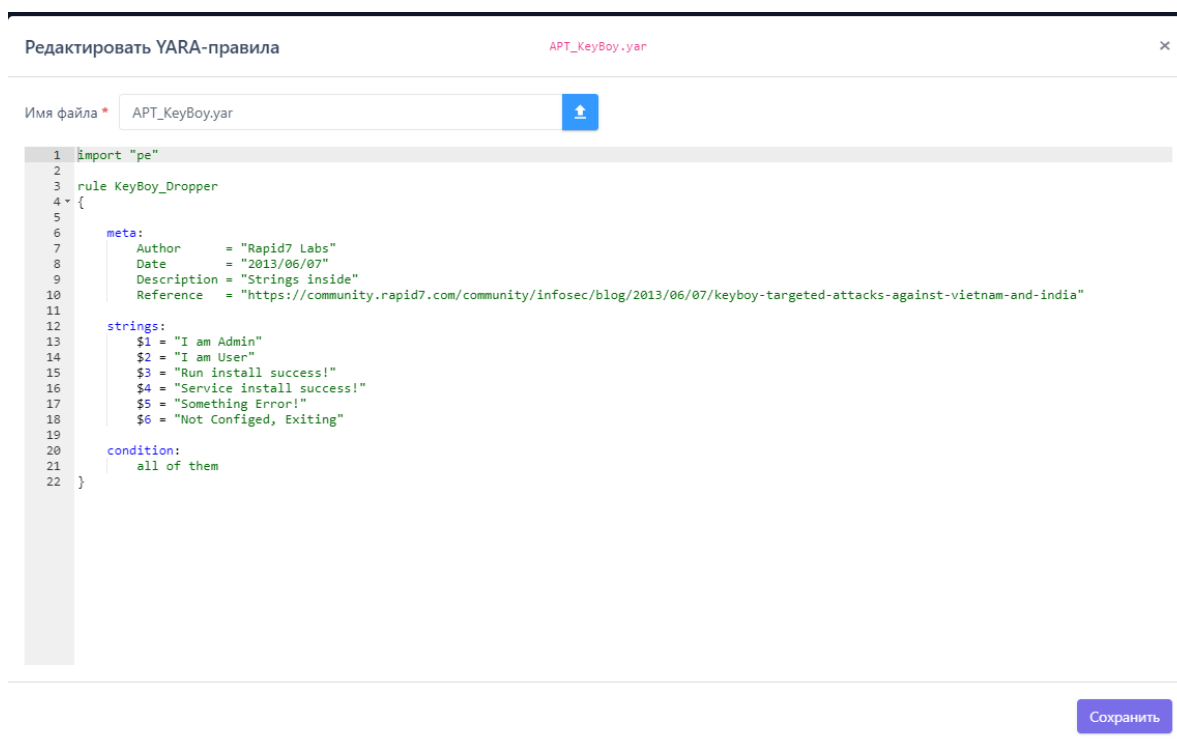


Рисунок 119 – Пример правила YARA

Для корректной работы после любых изменений в наборе необходимо нажать кнопку **Применить набор** ().

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл** () (формат yara). Набор будет сохранен в папке **Загрузки** в соответствующем формате.

Для импорта правил из файла требуется нажать кнопку **Импортировать данные из файла в набор**, поддерживаемые форматы: JSON ().

Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать правило из выбранного набора, необходимо нажать кнопку  или выполнить активацию/деактивацию с помощью кнопок **Активировать** **выбранные элементы**/Деактивировать выбранные элементы ( ).

Для удаления правил из набора необходимо отметить флажками правила, которые требуется удалить и нажать кнопку **Удалить выбранные** или удалить правила по отдельности с помощью кнопки **Удалить** ().

Для редактирования правила следует нажать кнопку **Редактировать** (), после чего внести изменения в открывшемся окне с правилом. После внесения изменений в правило необходимо нажать кнопку **Сохранить**.

На странице предусмотрена фильтрация YARA-правил по имени, а также фильтрация файлов по имени файла в соответствующих строках. При этом необходимо помнить, что поиск по имени правил требует ввода полного имени правила.

5.5.5. YARA-правила (память)

Правила, указанные в разделе **YARA-правила (память)**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа памяти процесса на наличие вредоносных сигнатур. В Программе предусмотрены YARA-правила в наборе по умолчанию, а также инструментарий для создания новых правил.

Наборы YARA-правил (память)

Страница с наборами YARA-правил для памяти включает в себя те же структурные элементы, что и страница **Наборы YARA-правил (файлы)**:

- таблица с наборами YARA-правил;
- кнопка **Добавить набор**;
- кнопка **Применить набор**;
- кнопка **Удалить выбранные наборы**.

Для фильтрации информации на странице имеется система фильтров, представленная в списке:

- **Название набора**;
- **Поиск по полям набора**;

- Автор/пользователь;
- Дата создания/Изменения.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Добавить набор** ввести название нового набора YARA-правил. На этом этапе можно добавить YARA-правила из базового набора в новый. Для завершения операции необходимо нажать кнопку **Добавить**.

После любого изменения набора для корректной его работы требуется применять сделанные изменения, для этого необходимо нажать кнопку **Применить** () или **Применить все наборы** ()

Для удаления набора необходимо нажать кнопку **Удалить** () или **Удалить выбранные наборы**.

При нажатии ЛКМ на имени набора открывается страница **YARA-правила (память)** для выбранного набора.

Страница «YARA-правила (память)»

На странице **YARA-правила (память)** можно выполнять следующие операции:

- просматривать правила из выбранного набора;
- добавлять новые правила в выбранный набор;
- применять наборы после изменения правил;
- копировать/перемещать выбранные правила в другой набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать правило;
- редактировать выбранное правило;
- удалить выбранное правило из набора.

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Поиск по полям набора;
- Файл;
- Имя правила;
- Признак активации;

- Автор/Пользователь;
- Дата создания/изменения.

Для добавления нового правила необходимо нажать кнопку **Добавить правила**, после чего необходимо выбрать операцию **Новый файл** (для добавления одного файла в режиме набора текста или загрузки с хоста администратора) или **Загрузить файлы** (для добавления одного или нескольких файлов путём загрузки с хоста администратора). После выбора операции **Новый файл** откроется окно **Добавить YARA-правила**, в котором необходимо добавить имя YARA-файла и написать правило или несколько правил в соответствии с синтаксисом YARA. Администратор может добавить файл в формате .yar с помощью кнопки **Импортировать yara-файл** ()

Для корректной работы после любых изменений в наборе необходимо нажать кнопку **Применить набор** ()

При выборе операции **Импортировать yara-файл** откроется окно, в котором необходимо нажать кнопку **Выбрать файлы**, после чего в открывшемся окне выбрать один или несколько файлов с расширением .yar. Для завершения операции необходимо нажать кнопку **Загрузить файлы на сервер**.

Для копирования или перемещения правила 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 в файл следует нажать кнопку **Экспортировать набор в файл** () (формат JSON). Набор будет сохранен в папке **Загрузки** в соответствующем формате.

Для импорта правил из файла требуется нажать кнопку **Импортировать данные из файла в набор**, поддерживаемые форматы: JSON ()

Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать правило из выбранного набора, необходимо нажать кнопку  или выполнить активацию/деактивацию с помощью кнопок **Активировать** **выбранные элементы**/Деактивировать выбранные элементы ( ).

Для удаления правил из набора необходимо отметить флажками правила, которые требуется удалить и нажать кнопку **Удалить выбранные** или удалить правила по отдельности с помощью кнопки **Удалить** ().

Для редактирования правила следует нажать кнопку **Редактировать** (), после чего внести изменения в открывшемся окне с правилом. После внесения изменений в правило необходимо нажать кнопку **Сохранить**.

На странице предусмотрена фильтрация YARA-правил по имени, а также фильтрация файлов по имени файла в соответствующих строках. При этом необходимо помнить, что поиск по имени правил требует ввода полного имени правила.

5.6 Исключения EDR

В области **Исключения EDR** содержатся разделы:

- Исключения для программ;
- Исключения для файлов;
- Сетевые исключения;
- Исключения индикаторов атак.

С помощью этих разделов выполняется настройка исключений для исполняемых файлов, которые позволяют разрешить работу программ или запретить операции с ними без создания инцидентов.

Кроме наборов, создаваемых вручную, в представленных выше разделах могут содержаться автоматически создаваемые наборы.

В эти наборы попадают артефакты согласно алгоритмам сервера, например, в исключения для файлов попадают наиболее часто встречающиеся безопасные хеши.

5.6.1. Исключения для программ

Общая информация

На странице с наборами исключений для программ (рис. 120) содержится список программ, исполнение которых должно соответствовать определенным 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, соответственно, 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 администратору уменьшить количество ложных срабатываний, а также настроить особенности исполнения программ в защищаемой инфраструктуре.

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐ test	Доступен всем	5	14.03.2025, 14:10:10		14.03.2025, 14:10:10	
☐ testfl	Доступен всем	22	14.03.2025, 12:23:44		14.03.2025, 12:23:44	
☐ лимиты полей	Доступен всем	6	06.03.2025, 18:02:33		06.03.2025, 18:09:42	
☐ vp-test	Доступен всем	4	28.02.2025, 20:23:51		28.02.2025, 20:23:51	
☐ тест	Доступен всем	151	19.02.2025, 18:28:52	19.02.2025, 18:29:14	03.03.2025, 18:24:27	
☐ test_set1	Доступен всем	20	19.02.2025, 17:21:45		26.02.2025, 16:45:17	
☐ test_flags	Доступен всем	7	19.02.2025, 11:57:50		19.02.2025, 14:59:38	
☐ 123	Доступен всем	11	12.02.2025, 15:01:27		03.03.2025, 18:24:11	
☐ for-test	Доступен всем	27	05.02.2025, 12:21:40		19.02.2025, 15:01:50	
☐ 1	Доступен всем	13	05.02.2025, 10:19:55		19.02.2025, 15:12:30	

Рисунок 120 – Наборы исключений для программ

Наборы исключений для программ

Страница с наборами исключений для программ включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- фильтры;
- таблица с наборами исключений для программ;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы.

Для фильтрации информации на странице имеется система фильтров, представленная в списке:

- Название набора;
- Поиск по полям набора;
- Автор/пользователь;
- Дата создания/Изменения.

Чтобы добавить новый набор с исключениями для программ, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. 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 **Исключения для программ** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Исключения для программ»

На странице **Исключения для программ** (рис. 121) можно выполнять следующие операции:

- просматривать исключения для программ в выбранном наборе;
- добавлять новое исключение по имени файла;
- добавлять новое исключение по хешу;
- добавлять новое исключение по командной строке;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

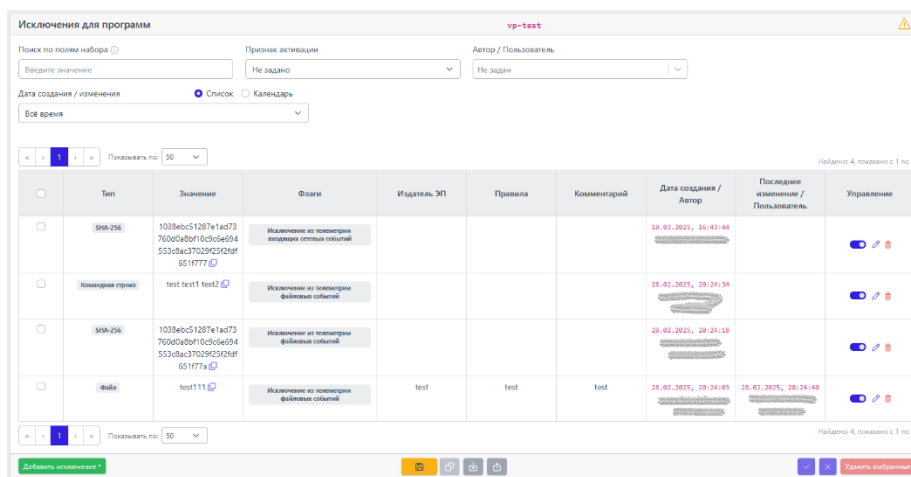


Рисунок 121 – Исключения для программ

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Поиск по полям набора;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

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** (рис. 122).

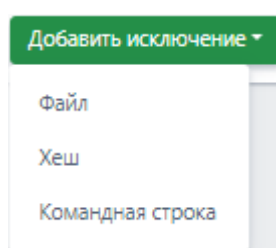


Рисунок 122 – Добавить исключение для программ (выбор типа)

Далее в открывшемся окне **Добавить исключение** следует 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: **Файлы**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий** (рис. 123).

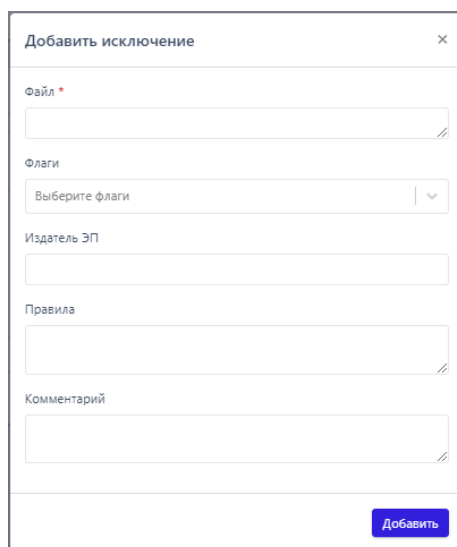


Рисунок 123 – Добавление исключения для программы (тип «Файл»)

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы**, **Хеш-сумма**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий** (рис. 124).

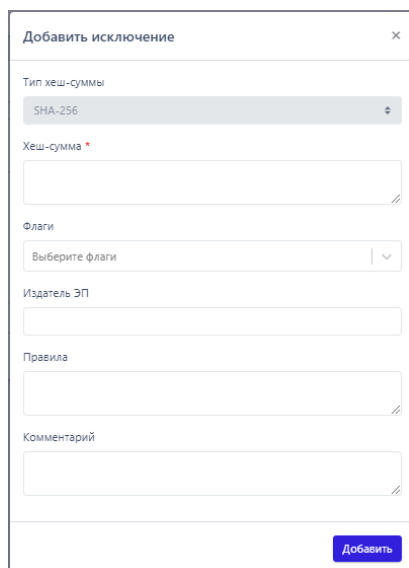


Рисунок 124 – Добавление исключения для программы (тип «Хеш»)

Для типа исключений **Командная строка** необходимо определить следующие параметры: **Командная строка прародителя**, **Командная строка родителя**, **Командная строка процесса**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий** (рис. 125).

Рисунок 125 – Добавление исключения для программы (тип «Командная строка»)

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.

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**.

Командная строка прародителя – в поле прописывается значение командной строки для процесса, являющегося прародителем по отношению к процессу, для которого добавлено исключение.

Командная строка родителя – в поле прописывается значение командной строки для процесса, являющегося родителем по отношению к процессу, для которого добавлено исключение.

Командная строка процесса – в поле прописывается значение командной строки процесса, для которого назначено исключение. После добавления исключения значение командной строки отображается в таблице **Исключения для программ** в поле **Значение**.

Флаги – в поле определяются условия, согласно которым будут исполняться файлы, добавленные в список исключений для программ.

В RT Protect TI предусмотрены следующие флаги:

- 1) Разрешить внедрение кода в сторонние программы;
- 2) Разрешить запись памяти сторонних программ;
- 3) Разрешить чтение памяти сторонних программ и управления ими;
- 4) Компонент имеет 32-х битную и 64-х битную версию (NOTE: (syswow 64/system 32);
- 5) Хост-процесс;
- 6) Подтверждение по электронной подписи;
- 7) Разрешение прямого доступа к диску для записи;
- 8) Разрешение прямого доступа к диску для чтения;
- 9) Право взаимодействия с критическими системными программами;
- 10) Антивирусный компонент;
- 11) Исключение из телеметрии сетевых событий;
- 12) Исключение из телеметрии файловых событий;
- 13) Исключение из телеметрии событий реестра Windows;
- 14) Исключение из телеметрии событий поведения;
- 15) Исключение всей телеметрии.

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**.

Правила – в поле администратором или аналитиком прописывается название правила, на срабатывание которого пишется исключение, например, CmdLineTampering или Ransomware.

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**.

Для завершения операции добавления исключения для программы необходимо после ввода информации в окне **Добавить исключение** нажать кнопку **Добавить**.

Чтобы удалить исключение для программы, необходимо отметить одно или несколько исключений, установив флажок в кнопке выбора, и нажать кнопку **Удалить выбранные**. Также можно удалить исключение из набора с помощью кнопки **Удалить** (). Для внесения изменений в исключение для программы необходимо нажать кнопку **Редактировать** () в соответствующей строке таблицы **Исключения для программ** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для завершения редактирования необходимо нажать кнопку **Сохранить** после внесения изменений в редактируемый элемент.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл формата CSV** (). Набор будет сохранен в папке **Загрузки**.

Для импорта исключений из файла требуется нажать кнопку **Импортировать CSV-файл** (). Далее выбрать на компьютере файл, содержащий нужные исключения, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку .

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** ().

5.6.2. Исключения для файлов

Общая информация

На странице **Наборы исключений для файлов** (рис. 126) содержится список файлов, исполнение которых должно быть разрешено или заблокировано (без создания инцидента, как в случае с индикатором компрометации). В отличие от исключений для программ, где можно задавать различные параметры с помощью флагов, тем самым влияя на динамику исполнения программы, исключения для файлов работают в статике, то есть разрешение или запрет на запуск файла происходит в момент обращения к этому файлу.

Наличие этой возможности позволяет администратору уменьшить количество ложных срабатываний, а в случае необходимости, заблокировать ту или иную программу в целях обеспечения безопасности.

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
irina	Доступен всем	1	04.04.2025, 12:00:13		04.04.2025, 12:00:13	
для импорта	Доступен всем	6	06.03.2025, 17:30:14		06.03.2025, 17:39:46	
test_0011	Доступен всем	7	19.02.2025, 16:14:22	19.02.2025, 16:18:53	06.03.2025, 17:27:36	
test_ip+_1	Доступен всем	8	13.02.2025, 16:30:20		13.02.2025, 16:30:20	
test_ip	Доступен всем	10922	13.02.2025, 16:16:25		03.03.2025, 18:25:46	
test_ip	Доступен всем	18	15.01.2025, 18:33:37		04.03.2025, 18:53:01	
test	Доступен всем	6	13.02.2025, 17:51:11		13.02.2025, 17:51:11	
test#903	Доступен всем	0	05.03.2025, 15:22:22		16.05.2025, 15:18:07	
TestFileExcl_123	Доступен всем	10	03.03.2025, 17:40:06	29.04.2025, 17:13:03	16.05.2025, 15:06:30	
set(shadow)	Доступен всем	100	20.12.2024, 16:21:00		14.05.2025, 23:00:38	

Рисунок 126 – Наборы исключений для файлов

Наборы исключений для файлов

Страница с наборами исключений для файлов включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- фильтры Название набора и Показывать по;
- таблица с наборами исключений для файлов;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы.

Для фильтрации информации на странице имеется система фильтров, представленная в списке:

- Название набора;
- Поиск по полям набора;
- Автор/пользователь;
- Дата создания/Изменения.

Чтобы добавить новый набор с исключениями для файлов, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора.

При установке галочки «Теневой» будет создан набор с исключениями в концепции теневого набора. Подробнее с концепцией теневых наборов можно ознакомиться в п. **Ошибка! Источник ссылки не найден..** Для завершения операции необходимо нажать кнопку **Добавить**.

В таблице с наборами теневые наборы в столбце названия набора имеют вид  test_jp_1 , где  - указатель на то, что набор синхронизирован с источником данных, на основании которого создан набор, test_jp_1 - название набора,  - указатель что набор обновляется автоматически.

В столбце **Действия** для теневых наборов, в отличие от обычных наборов, имеется иконка для синхронизации наборов  и для скачивания наборов .

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 для файлов** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Исключения для файлов»

На странице **Исключения для файлов** (рис. 127) можно выполнять следующие операции:

- просматривать исключения для файлов в выбранном наборе;
- добавлять новое исключение по имени файла;
- добавлять новое исключение по хешу;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

Исключения для файлов

test_jpr_1

Поиск по полям набора

Значение

Тип

Комментарий

Введите значение

Введите значение

Не задано

Введите значение

Действие

Признак активации

Автор / Пользователь

Не задан

Не задано

Не задан

Дата создания / изменения

Список

Календарь

Все время

Показывать по: 50

	Тип	Значение	Действие	Флаги	Комментарий	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☐	SHA-256	63f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	25.02.2025, 16:01:45	05.03.2025, 14:55:46	☐
☐	SHA-256	64f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	25.02.2025, 16:01:45		☐
☐	SHA-256	62f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	25.02.2025, 16:01:45	05.03.2025, 13:03:31	☒
☐	SHA-256	61f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	25.02.2025, 16:01:45	05.03.2025, 13:03:31	☒
☐	SHA-256	64f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	17.02.2025, 16:14:33	17.02.2025, 16:16:10	☐
☐	SHA-256	63f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	17.02.2025, 16:14:33	17.02.2025, 16:16:12	☐
☐	SHA-256	62f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	17.02.2025, 16:14:33	17.02.2025, 16:15:16	☒
☐	SHA-256	61f6e6415923ed6c604446a2bb461c8d1fdd52d107ad626bc5f39aff4ed37f8a	Разрешить		for-test	17.02.2025, 16:14:33	17.02.2025, 16:15:16	☒

Показывать по: 50

Найдено: 8, показано с 1 по 8

Добавить исключение

Удалить выбранные

Рисунок 127 – Исключения для файлов

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Поиск по полям набора;
- Значение;
- Тип;
- Комментарий;
- Действие;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

Для добавления в набор нового исключения для файлов необходимо нажать кнопку **Добавить исключение** и в открывшемся списке выбрать тип добавляемого исключения: **Файл** или **Хеш**.

Далее в открывшемся окне **Добавить исключение**, следует выбрать параметры исключения. В зависимости от выбора типа исключения (**Файл** или **Хеш**) окно **Добавить исключение** будет содержать поля с

различными параметрами. Для типа исключений **Файл** необходимо определить следующие параметры: **Файл** (прописывается имя файла, добавляемого в исключения), **Действие** (блокировать или разрешить), **Комментарий** (рис. 128).

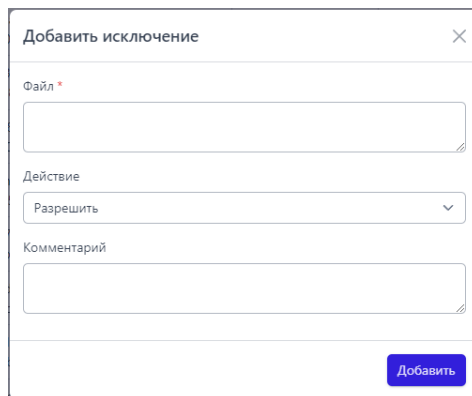


Рисунок 128 – Добавление исключения для файла (тип «Файл»)

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы**, **Хеш-сумма** (можно добавлять несколько хеш-сумм построчно), **Действие** (разрешить или блокировать), **Комментарий** (рис. 129).

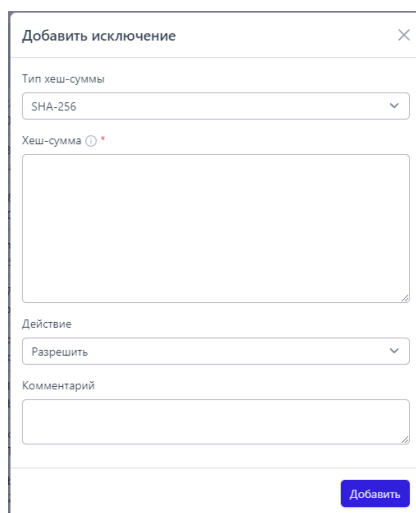


Рисунок 129 – Добавление исключения для файла (тип «Хеш»)

Файл – в поле прописываются имена исполняемых файлов, которые необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** в поле **Значение**, а в поле **Тип** будет указан тип исключения.

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**.

Хеш-сумма – в поле прописываются значения хеш-сумм для исполняемых файлов, которые необходимо добавить в исключения.

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**.

Для завершения операции добавления исключения для программы необходимо после ввода информации в окне **Добавить исключение** нажать кнопку **Добавить**.

Чтобы удалить исключение для файла, необходимо отметить одно или несколько исключений, установив флажок в кнопке выбора, и нажать кнопку **Удалить выбранные**. Также можно удалить исключение из набора с помощью кнопки **Удалить** (). 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. Для завершения редактирования необходимо нажать кнопку **Сохранить** после внесения изменений в редактируемый элемент.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл формата CSV** ().

Набор будет сохранен в папке **Загрузки**. Для импорта исключений из файла требуется нажать кнопку **Импортировать CSV-файл** (). Далее выбрать на компьютере файл, содержащий нужные исключения, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку .

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** (.

5.6.3. Сетевые исключения

Общая информация

На странице **Сетевые исключения** представлены имена наборов исключений, в которых указываются IP-адреса и доменные имена в качестве идентификаторов при создании исключений. Предусмотрены следующие действия при создании сетевых исключений для взаимодействия с IP-адресами и доменными именами: **Разрешить (всегда)**, **Блокировать**, **Разрешить (кроме изоляции)**.

При создании сетевого исключения, действия, которые следует прописать в соответствующем поле, имеют следующий смысл:

— **Разрешить (всегда)** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем разрешается, при этом функциональность сохраняется даже тогда, когда агент изолирован);

— **Блокировать** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-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 (кроме изоляции)** (означает, что взаимодействие машины, на которой установлен агент с указанным в исключении IP-адресом или доменным именем разрешается, кроме того случая, когда машина, на которой установлен агент, находится в режиме изоляции.

Использование сетевых исключений позволяет подавлять сетевые срабатывания на конечных точках и снижать количество анализируемой системой информации, так как при сетевом взаимодействии с элементами “белого” списка агент EDR, с которым выполняет взаимодействие TI-платформа, не анализирует данные потока (не производит матчинг сетевых сигнатур).

Наборы сетевых исключений

Страница **Сетевые исключения** содержит наборы с сетевыми исключениями и включает в себя следующие структурные элементы (рис. 130):

- таблица с наборами сетевых исключений;
- кнопка **Добавить набор**;
- кнопка **Удалить выбранные наборы**.

Сетевые исключения

Название набора: Поиск по полям набора: Автор / Пользователь:

Дата создания / изменения:

Всё время

Показывать по: 10

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐ for_test_1	Доступен всем	10	26.03.2025, 15:17:58		26.03.2025, 15:17:58	
☐ для_теста	Доступен всем	1	26.03.2025, 15:11:03		26.03.2025, 15:11:03	
☐ 321321yy	Доступен всем	2	17.03.2025, 14:09:45	17.03.2025, 14:23:10	17.03.2025, 14:15:03	
☐ asdasd	Доступен всем	3	17.03.2025, 12:40:55		17.03.2025, 12:40:55	
☐ 65нб5н	Доступен всем	24	17.03.2025, 12:00:51		17.03.2025, 12:00:51	
☐ value	Доступен всем	0	14.03.2025, 16:56:22		14.03.2025, 16:56:22	
☐ тест имп	Доступен всем	6	05.03.2025, 16:19:59		05.03.2025, 16:19:59	
☐ тест импорта_1	Доступен всем	7	05.03.2025, 12:23:18		05.03.2025, 12:23:18	
☒ World top 5000 domains	Доступен всем	5273	19.03.2025, 12:46:30		19.04.2025, 15:04:57	
☒ test_shadow	Доступен всем	2	19.03.2025, 11:40:28	19.03.2025, 12:10:46	19.05.2025, 19:00:01	

Добавить набор

Удалить выбранные

Рисунок 130 – Страница наборов сетевых исключений

Для фильтрации информации на странице имеется система фильтров, представленная в списке:

- Название набора;
- Поиск по полям набора;
- Автор/пользователь;
- Дата создания/Изменения.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора.

При необходимости можно создать теневой набор, указав галочку после названия набора. Подробнее с концепцией теневых наборов можно ознакомиться в п. **Ошибка! Источник ссылки не найден.** данного руководства.

В таблице с наборами теневые наборы в столбце названия набора имеют вид test_jp_1 , где - указатель на то, что набор синхронизирован с источником данных, на основании которого создан набор, test_jp_1 - название набора, - указатель, что набор обновляется автоматически.

В столбце **Действия** для теневых наборов, в отличие от обычных наборов, имеется иконка для синхронизации наборов и для скачивания наборов .

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**.

Страница «Сетевые исключения»

На странице **Сетевые исключения** (рис. 131) можно выполнять следующие операции:

- просматривать сетевые исключения в выбранном наборе;
- добавлять новое исключение по IP-адресу;
- добавлять новое исключение по доменному имени;
- сохранять набор в файл экспорта;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

Сетевые исключения 65n65n

Поиск по полям набора: Значение: Тип: Комментарий:

Действие: Признак активации: Автор / Пользователь:

Дата создания / изменения: ☐ Список ☐ Календарь

Всё время

Показывать по: 10

Тип	Значение	Действие	Флаги	Комментарий	Дата создания / Автор	Последнее изменение / Пользователь	Управление
IP-Адрес	123.123.123.123	Разрешить (сервис исключен)			18.03.2025, 12:26:58		☐ ☐
Доменное имя	domain.ru	Разрешить (сервис исключен)			18.03.2025, 12:22:42		☐ ☐
Доменное имя	domain.ru	Разрешить (сервис исключен)			18.03.2025, 12:11:46	18.03.2025, 12:23:02	☐ ☐
Доменное имя	domain.ru	Разрешить (сервис исключен)			18.03.2025, 12:11:35		☐ ☐
IP-Адрес	123.123.123.123	Разрешить (сервис исключен)			18.03.2025, 12:11:29		☐ ☐
Доменное имя	321.321.321.321	Разрешить (сервис исключен)			18.03.2025, 12:03:07		☐ ☐
IP-Адрес	2001:4100:1008::	Разрешить (сервис исключен)		https://www.urlencoder.org/	17.03.2025, 12:11:30		☐ ☐
Доменное имя	азбука.ру	Блокировать			17.03.2025, 12:11:30		☐ ☐
Доменное имя	дом.рф	Разрешить (сервис исключен)			17.03.2025, 12:11:30		☐ ☐
Доменное имя	ab57.ru	Блокировать			17.03.2025, 12:11:30		☐ ☐

Добавить исключение

Удалить выбранные

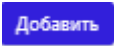
Рисунок 131 – Страница «Сетевые исключения»

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Поиск по полям набора;
- Значение;
- Тип;
- Комментарий;
- Действие;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

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.

Чтобы завершить операцию, после ввода параметров в окне **Добавить исключение** следует нажать кнопку . В одном исключении можно написать несколько доменов или IP-адресов, каждое новое значение следует писать в новую строку.

В поле **Значение** таблицы с сетевыми исключениями отображается элемент , который позволяет скопировать IP-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 **Редактировать**. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

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 файл** (). 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 **Деактивировать сетевое исключение/Активировать сетевое исключение** .

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.

5.6.4. Исключения индикаторов атак

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.

Исключение работает по имени и типу индикатора, к условию которого добавляется условие исключения, поэтому важно указывать правильные имя и тип индикатора атак.

При срабатывании исключения на странице **Активность** будет показано событие со статусом **Разрешено** и причиной **Исключение для индикаторов атак**.

Наборы исключений индикаторов атак

Страница **Наборы исключений индикаторов атак** включает в себя следующие структурные элементы (рис. 132):

- таблица с наборами исключений для индикаторов атак;
- кнопка **Добавить набор**;
- кнопка **Применить набор**;

— кнопка Удалить выбранные наборы.

☐	Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	Irina_Test	Доступен всем	0	18.03.2025, 15:54:35		18.03.2025, 15:54:35	
☐	555	Доступен всем	3	05.03.2025, 16:53:12	24.03.2025, 12:41:35	24.03.2025, 12:41:46	
☐	333	Доступен всем	1	05.03.2025, 16:31:38		24.03.2025, 12:41:57	
☐	1115	Доступен всем	1	05.03.2025, 16:27:58	24.03.2025, 12:45:56	24.03.2025, 12:45:38	
☐	test_Julia	Доступен всем	6	05.03.2025, 12:57:11		24.03.2025, 12:49:54	
☐	testimport	Доступен всем	5	04.03.2025, 12:23:44		04.03.2025, 12:23:44	
☐	Julia	Доступен всем	6	03.03.2025, 16:47:11		03.03.2025, 18:39:43	
☐	test1	Доступен всем	7	03.02.2025, 11:16:15		03.03.2025, 18:39:51	
☐	PMI_Test_1.1	Доступен всем	3	11.11.2024, 20:05:14		19.11.2024, 18:06:31	
☐	Test_ios1	Доступен всем	32	27.09.2024, 12:32:55	11.01.2025, 17:19:12	03.02.2025, 11:38:02	

Рисунок 132 – Страница «Наборы исключений индикаторов атак»

Для фильтрации информации на странице имеется система фильтров, представленная в списке:

- Название набора;
- Поиск по полям набора;
- Автор/пользователь;
- Дата создания/Изменения.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**.

Для завершения операции необходимо нажать кнопку **Создать**.

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**.

На странице **Исключения индикаторов атак** можно выполнять следующие операции:

- просматривать исключения 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 фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Поиск по полям набора;
- Имя;
- Условие;
- Тип;
- Комментарий;
- Описание;
- Действие;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

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.



Важно

Имя исключения должно соответствовать имени исключаемого индикатора.

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.

Чтобы завершить операцию добавления исключения, после ввода параметров в окне **Добавить исключение** следует нажать кнопку

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 . Для отмены изменений следует нажать кнопку **Заккрыть 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** ().

6. Действия после сбоя и ошибки

6.1 Общие сведения

Большинство ошибок можно разделить на следующие типы:

1) Ошибки конфигурации:

- некорректные настройки параметров безопасности;
- некорректная установка компонентов программы;
- некорректные действие со стороны пользователя;
- критические ошибки.

2) Ошибки оборудования:

- выход из строя аппаратных средств, на которых установлена программа;
- выход из строя сервера (или компонентов на сервере), с которыми взаимодействуют компоненты программы, установленные на оборудовании пользователя;
- перебои питания со стороны клиентской или серверной части.

Для устранения ошибки требуется обратиться к администратору программы.

7. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице 13.

Таблица 13 – Перечень сокращений

ИС	Информационная система
ИТ	Информационная технология
ЛКМ	Левая кнопка мыши
ПКМ	Правая кнопка мыши
ПО	Программное обеспечение
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦП	Центральный процессор
APT	Advanced Persistent Threat (постоянная серьезная угроза)
ID	Identifier (идентификатор)
IT	Information Technology (информационные технологии)
NSRL	National Software Reference Library (Национальная справочная библиотека программного обеспечения)
PID	Process Identifier (идентификатор процесса)
PPID	Parent Process Identifier (идентификатор родительского процесса)
RPC	Remote Procedure Call (удалённый вызов процедур)
SID	Security Identifier (идентификатор безопасности)
TI	Threat Intelligence
URL	Uniform Resource Locator

Цитирование документа допускается только со ссылкой на настоящее руководство. Руководство не может быть полностью или частично воспроизведено, тиражировано или распространено без разрешения АО «РТ-Информационная безопасность».