RT Protect TI

Руководство аналитика

Версия 1.0.20 от 17 октября 2024
Разработано компанией АО «РТ-Информационная безопасность»

Оглавление

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 9
3.1 Общие сведения 9
3.2 Комплектность поставки 9
3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения 9
4. Особенности функционирования программы 10
4.1 Требования к среде функционирования 10
5. Интерфейс программы 11
5.1 Окно авторизации и общие сведения 11
5.2 Горизонтальная панель управления 13
5.2.1. Меню «Пользователь» 13
5.3 Главная страница 15
5.4 Администрирование 18
5.4.1. Организации 19
5.4.2. Источники данных 20
5.4.3. Теги 38
5.5 Аналитика 48
5.5.1. Активность 48
5.5.2. Заключения аналитика 62
5.5.3. Отчеты 65

5.5.4. Граф связей 68
5.5.5. Yara-правила 72
5.5.6. Распространяемая аналитика 78
5.5.7. Алгоритм вынесения вердикта в TI 85
5.5.8. Теневые наборы 88
5.6 Аналитика EDR 91
5.6.1. Индикаторы атак 91
5.6.2. Индикаторы компрометации 115
5.6.3. Журналы Windows 121
5.6.4. Yara-правила (файлы) 124
5.6.5. YARA-правила (память) 127
5.7 Исключения EDR 130
5.7.1. Исключения для программ 131
5.7.2. Исключения для файлов 138
5.7.3. Сетевые исключения 144
5.7.4. Исключения индикаторов атак 148
6. Действия после сбоя и ошибки 153
6.1 Общие сведения 153
7. Перечень сокращений 154
8. Заключение 155

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 1.0.20 (актуальна для версии продукта frontend 0.8.3/backend 2.9.4)
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» 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
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-потоком 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
	Информация, требующая внимания пользователя
	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 8 ядер частотой минимум 2,4 ГГц	Не менее 10 ядер частотой минимум 2,4 ГГц
Оперативная память	16 ГБ	32ГБ
Жесткий диск (свободное пространство)	1 ТБ	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).

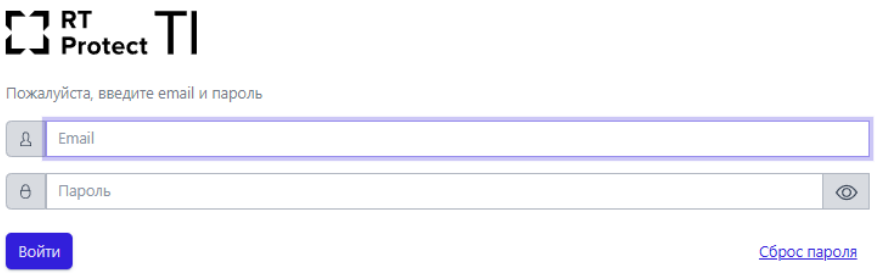


Рисунок 1 – Окно авторизации

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

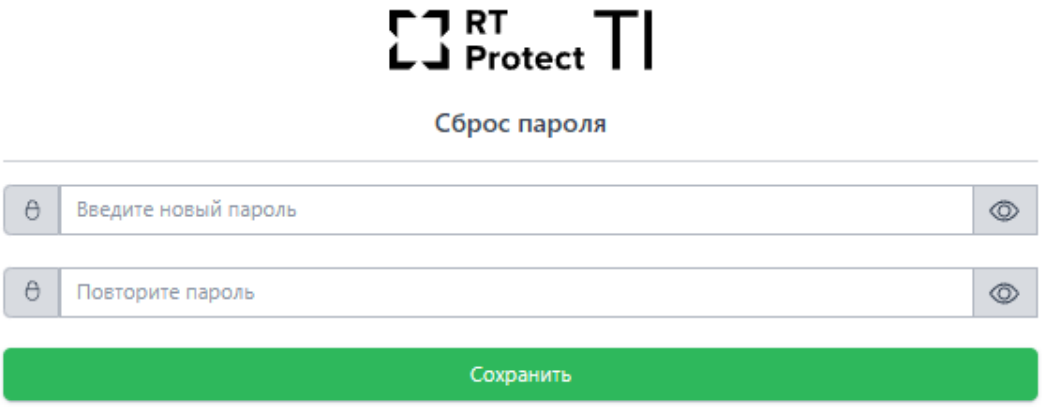


Рисунок 2 – Окно ввода параметром для сброса пароля

После ввода нового пароля потребуется вновь авторизоваться, введя 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).

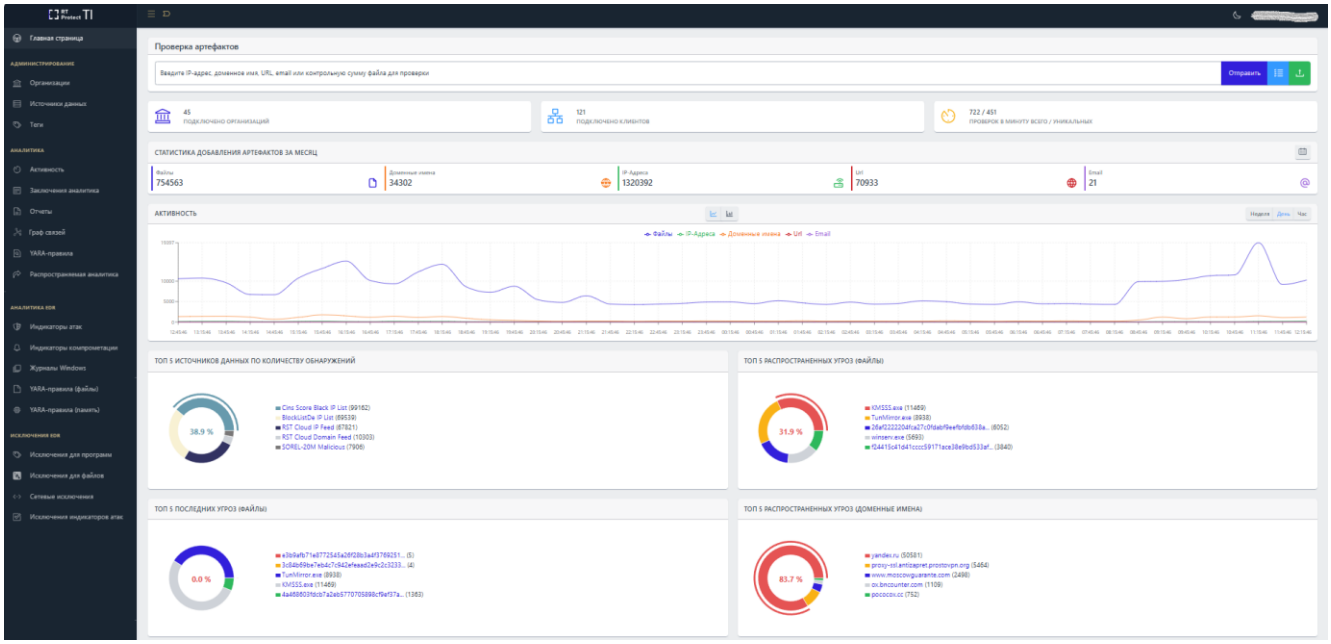
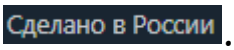


Рисунок 3 – Главная страница

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 5.4).

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 – 

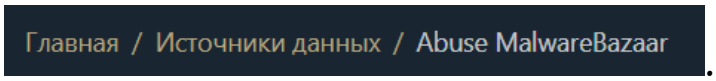
.

5.2 Горизонтальная панель управления

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

Рисунок 4 – Горизонтальная панель управления

Вертикальная и горизонтальная панели управления являются общими для всех страниц и разделов программы. При нажатии кнопки **Скрыть/показать панель разделов** () панель разделов скрывается и на странице отображается только поле для проверки артефактов и графики с информацией о программе. Для возврата первоначального вида необходимо повторно нажать на кнопку  .

При нажатии по иконке  на горизонтальной панели отображается, на какой странице с уровнем вложенности находится пользователь, например, 

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

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** и кнопка **Выход** для выхода из программы с текущего устройства (рис. 5).

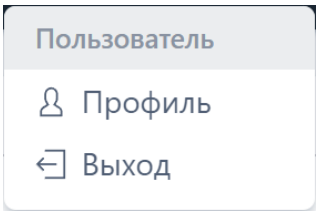


Рисунок 5 – Меню «Пользователь»

Подменю **Профиль** представлено на рисунке 6.

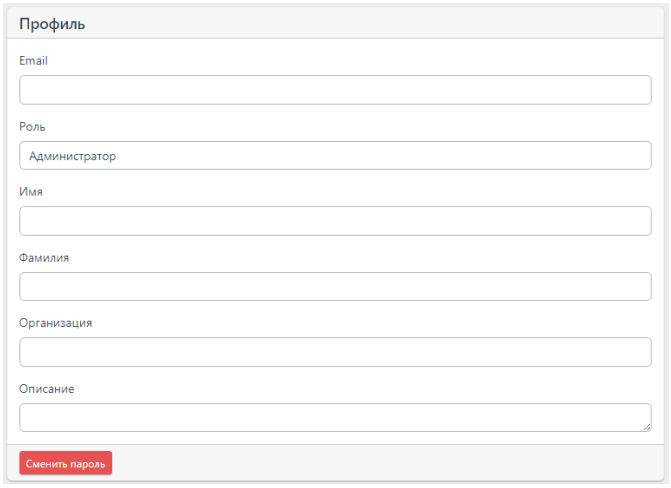


Рисунок 6 – Подменю «Профиль»

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

– адрес электронной почты для своей учетной записи;

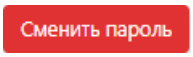
– роль, назначенная пользователю (администратор, пользователь, аналитик);

– имя и фамилия пользователя;

– поле с описанием профиля пользователя;

– организация;

– описание.

Изменять пароль возможно с помощью кнопки 

. При нажатии кнопки **Сменить пароль** открывается окно для смены пароля (рис. 7).

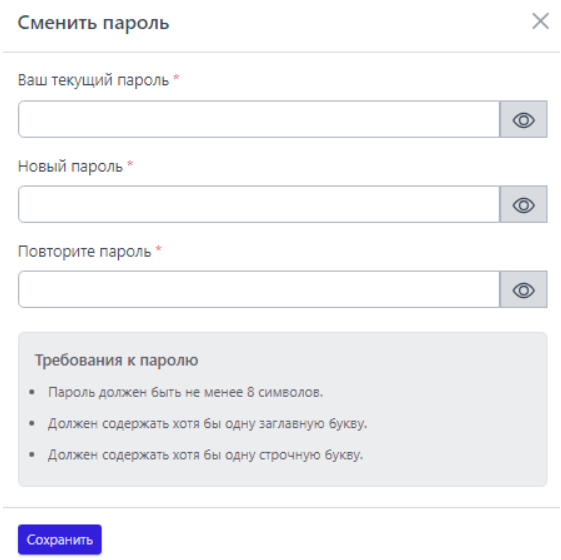


Рисунок 7 – Окно смены пароля

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 Главная страница

При открытии раздела **Главная страница** на правой панели отобразится страница со следующими информационными областями:

– область проверки артефактов и загрузки файлов;

– информация о подключенных организациях и клиентах;

– общее количество проверок и количество уникальных проверок в минуту;

– статистика добавления артефактов различных типов за месяц;

– топ 5 источников данных по количеству обнаружений;

– график **Активность** – отображение количества проверенных артефактов различных типов (файлы, IP-адреса, доменные имена, URL, EMAIL) за последнюю неделю, день, час;

– топ 5 распространенных угроз по различным типам артефактов (файлы, IP-адреса, доменные имена);

– топ 5 последних угроз по различным типам артефактов (файлы, IP-адреса, доменные имена);

– график отчетности проверок артефактов по базе VirusTotal за последнюю неделю, день или час;

– график отчетности проверок артефактов по базе Public TI за последнюю неделю, день или час;

– график отчетности проверок артефактов по базе RST Cloud за последнюю неделю, день или час;

– график, отображающий количество добавленных контрольных сумм, распределенных по времени;

– график, отображающий количество добавленных IP-адресов, распределенных по времени;

– график, отображающий количество добавленных доменных, распределенных по времени;

– график, отображающий количество добавленных файлов в хранилище, распределенных по времени.

В области **Графики** имеются иконки для управления размером отображения графика (50 или 100 %).

Данные иконки имеют вид :  - ширина 100%,  - ширина 50 %.

Примеры отображения области **Графики** представлены на рисунках 8 - 9.

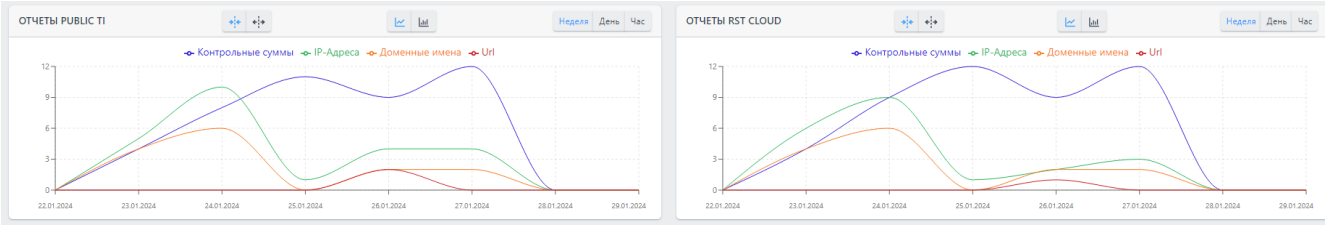


Рисунок 8 – Области с графиками с шириной 50%

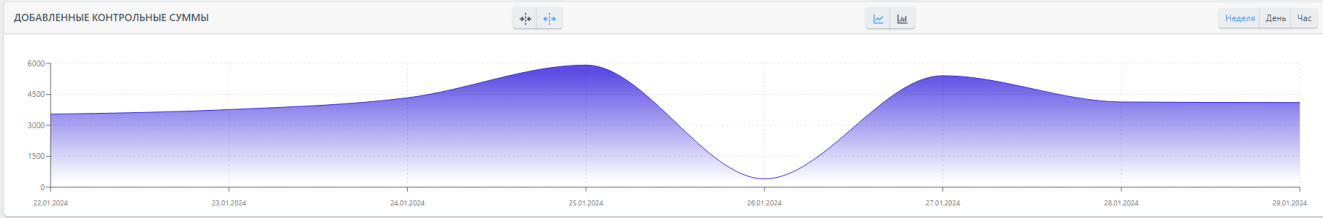


Рисунок 9 – Область с графиком с шириной 100%

В области **Проверка артефактов** Аналитик может получить вердикт для IP-адреса, домена, URL-адреса или хеш-суммы. Для этого необходимо ввести данные соответствующего артефакта в строку и нажать кнопку **Отправить**. Откроется отчет сервера аналитики.

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 сервер аналитики, а после завершения его загрузки выводится отчет с вердиктом.

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 10.

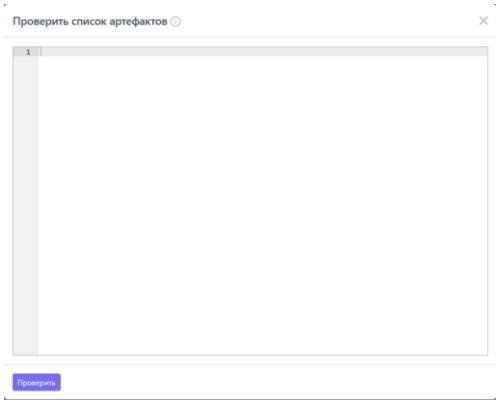


Рисунок 10 – Окно для написания списка артефактов для проверки

В данном окне артефакты добавляются по одному в каждой строчке (строчки нумеруются).

Проверка артефактов списком ограничена количеством в 100 строк. После написания артефактов требуется нажать по иконке «Проверить».

Если вердикт TI-платформы отсутствует, пользователь программы может добавить заключение аналитика. В этом случае ему необходимо нажать кнопку **Добавить заключение аналитика** и в открывшемся окне выбрать вердикт (безопасный или вредоносный), далее написать комментарий и выбрать время, в течение которого будет актуален вердикт для выбранного артефакта. Заключение аналитика является приоритетным для любого артефакта в программе, поэтому пользователь программы может обозначать артефакты, которые внешними источниками отмечены безопасными, как вредоносные, и наоборот.

Аналитик может в любой момент отредактировать вердикт по артефакту по своему усмотрению, добавив или отредактировав заключение аналитика.

5.4 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.

5.4.1. Организации

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

Общий вид страницы представлен на рисунке 11.

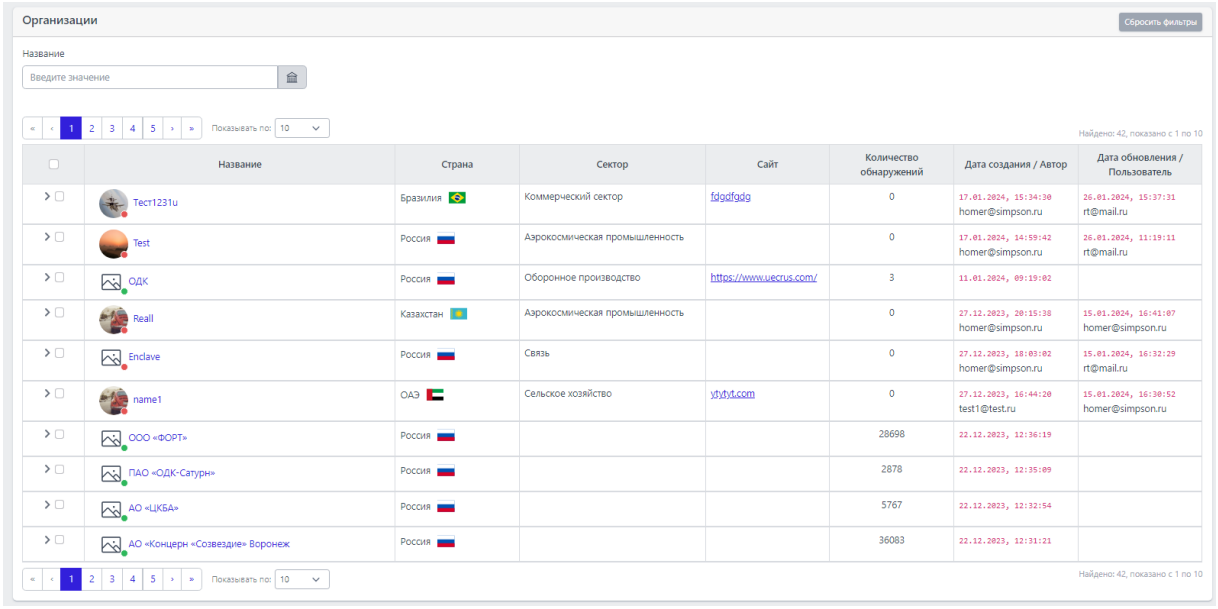


Рисунок 11 – Общий вид страницы «Организации»

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.

5.4.2. 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.

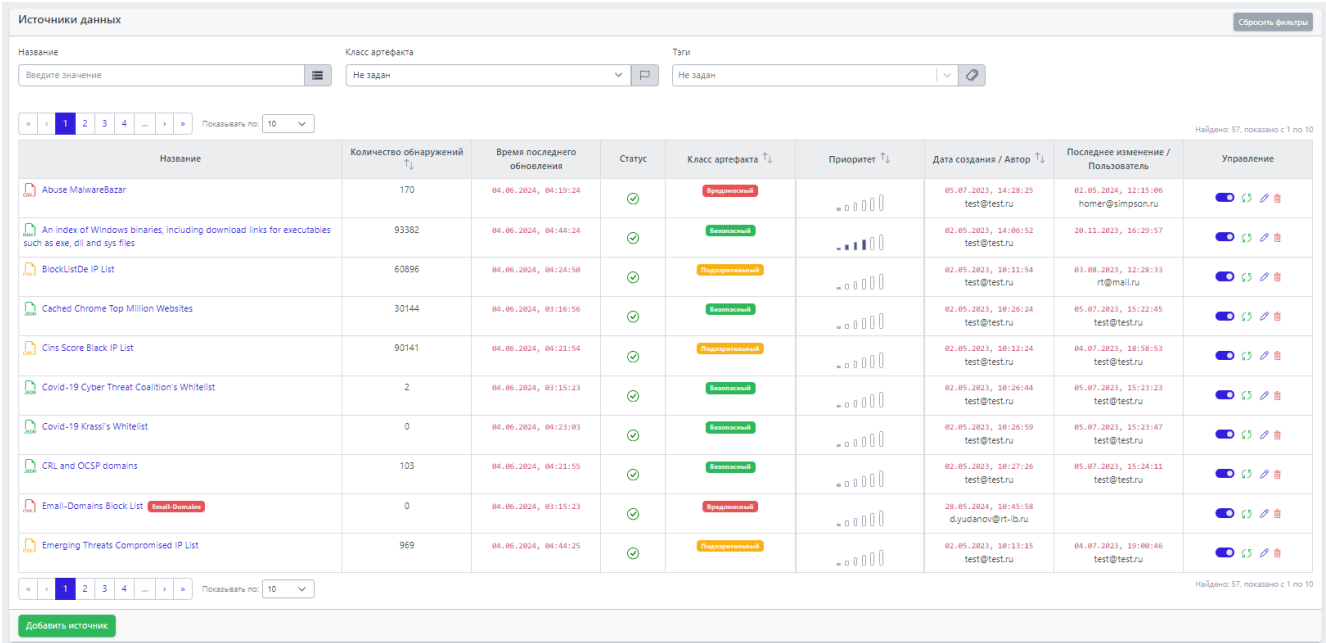


Рисунок 12 – Окно раздела «Источники данных»

Таблица со списками источников данных имеет следующие поля:

– **Название** (отображается название базы данных);

– **Количество обнаружений**;

– **Время последнего обновления** (отображается время последнего обновления базы данных);

– **Статус** (отображается информация о статусе обновления базы);

– **Класс артефакта** (отображается класс артефакта, который при сопоставлении базы и анализируемого артефакта будет выводиться при заключении вердикта);

– **Приоритет** (минимальный/средний);

– **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).

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.

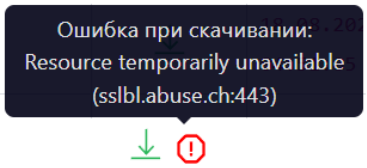


Рисунок 13 – Сообщение об ошибке при скачивании обновления источника

При нажатии по названию источника, например, Abuse MalwareBazaar откроется окно с информацией по источнику, представленное на рисунке 14.

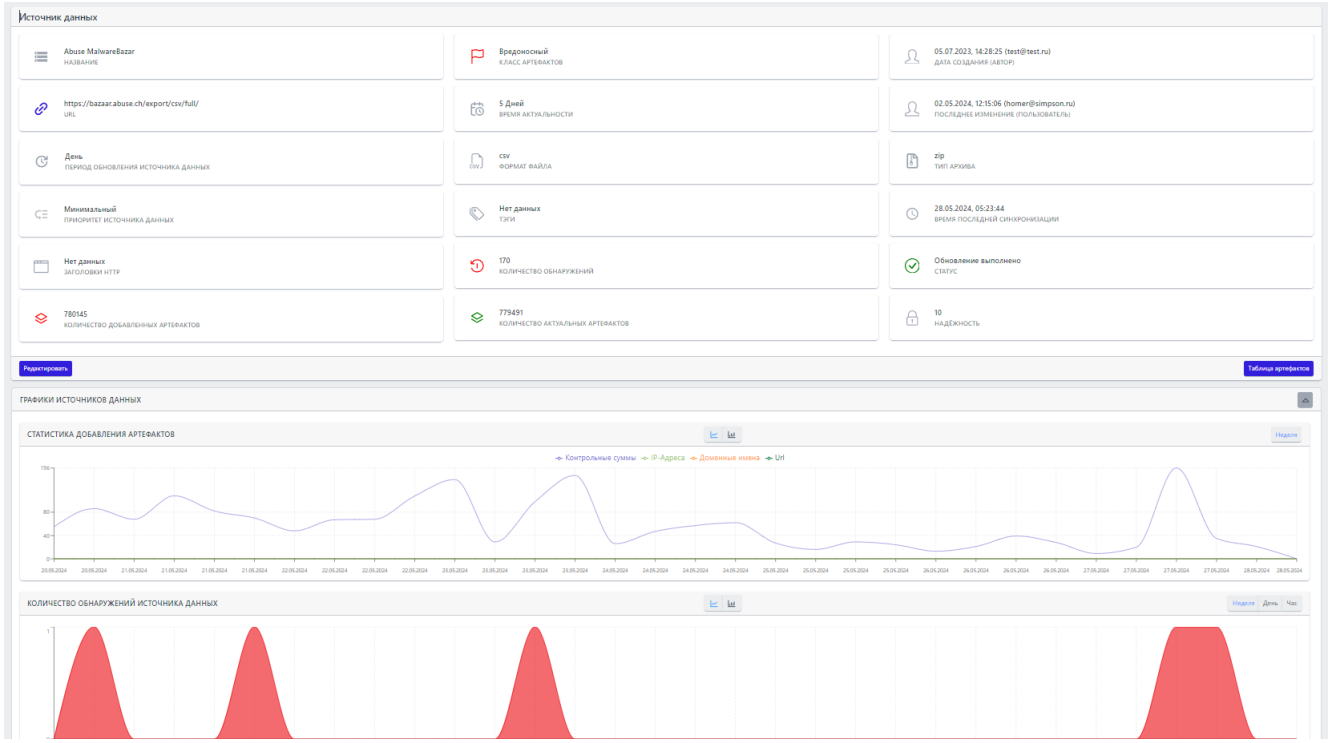


Рисунок 14 – Окно информации по источнику данных

В данном окне представлены следующие области:

– источник данных (выводится информация о добавленном источнике);

– статистика добавления артефактов (выводится в графическом виде статистика по добавленным артефактам, относящимся к данному источнику);

– количество обнаружений источника данных (выводится в графическом виде статистика по обнаружениям, относящимся к данному источнику);

– область с иконками редактирования источника данных и просмотр таблицы артефактов.

При нажатии по иконке Редактировать открывается окно для редактирования информации по источнику данных, представленное на рисунке 15.

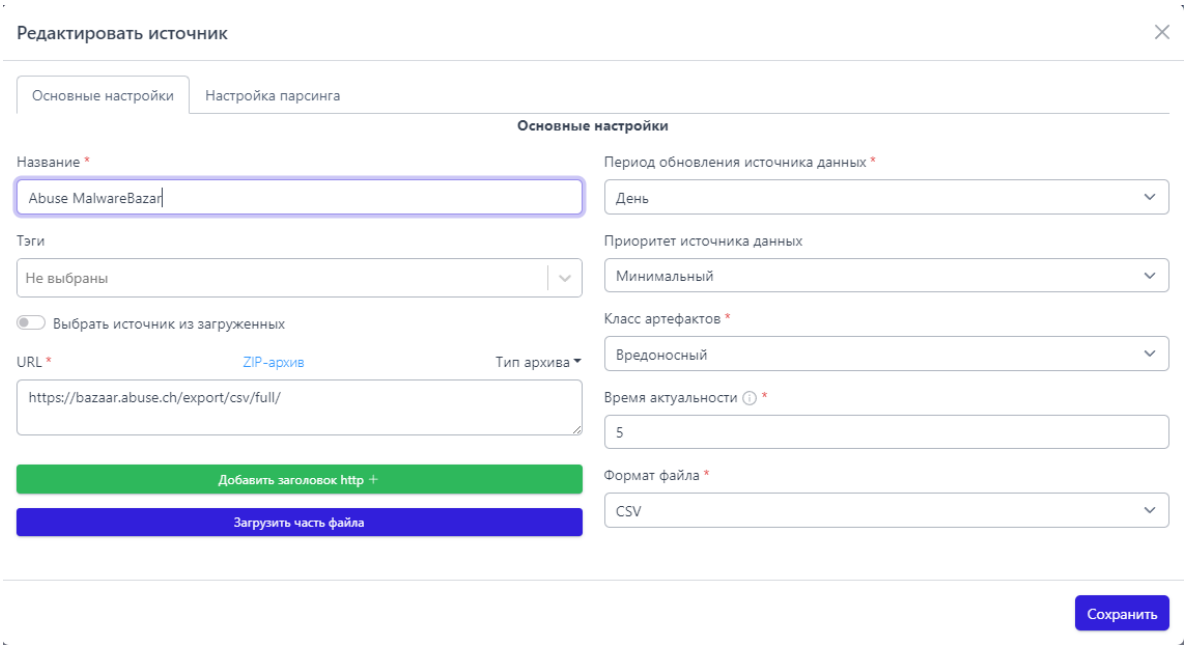


Рисунок 15 – Окно редактирования источника данных

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 открывается окно с таблицей, показывающей список артефактов, представленных по этому источнику данных (рисунок 16).

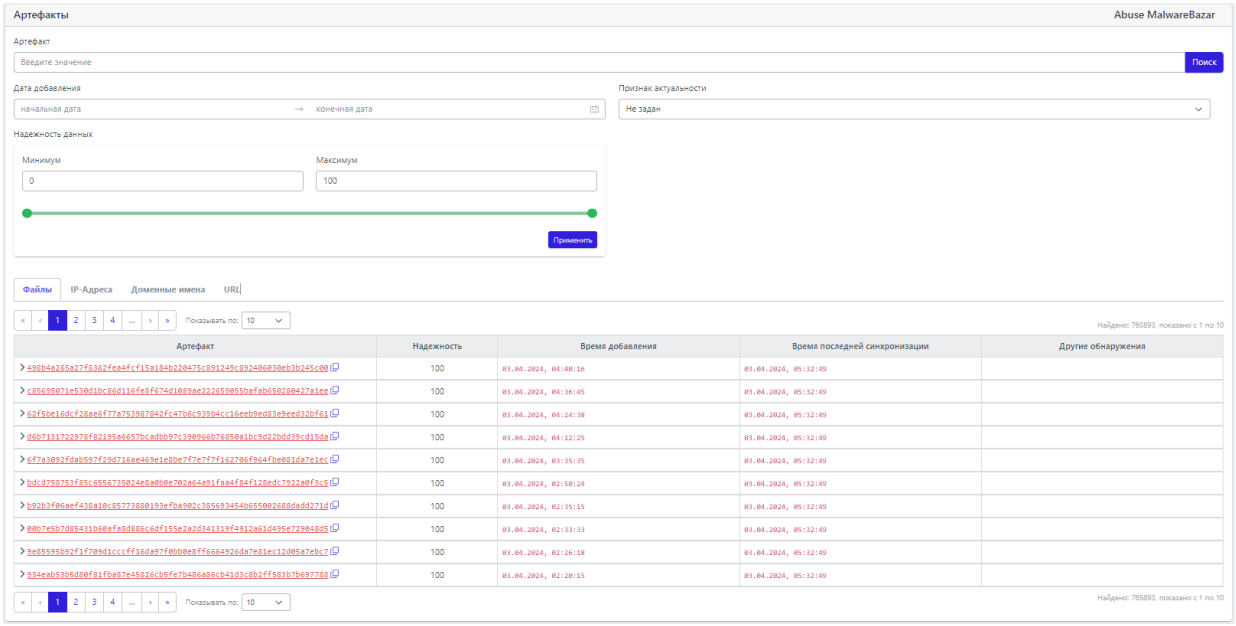


Рисунок 16 – Окно Таблица артефактов по источнику данных

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

– Артефакт;

– Дата добавления (начальная и конечная даты);

– Признак актуальности (не задан, актуальный, не актуальный);

– Надежность данных.

Важно

Фильтрация, а также отображение параметра надежности данных для артефактов в источнике будет доступна, только если при настройке источника данных этот параметр был определен.

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

Графики на странице 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 данных требуется нажать по иконке 

, после чего будет открыто окно добавления источника, представленное на рисунке 17.

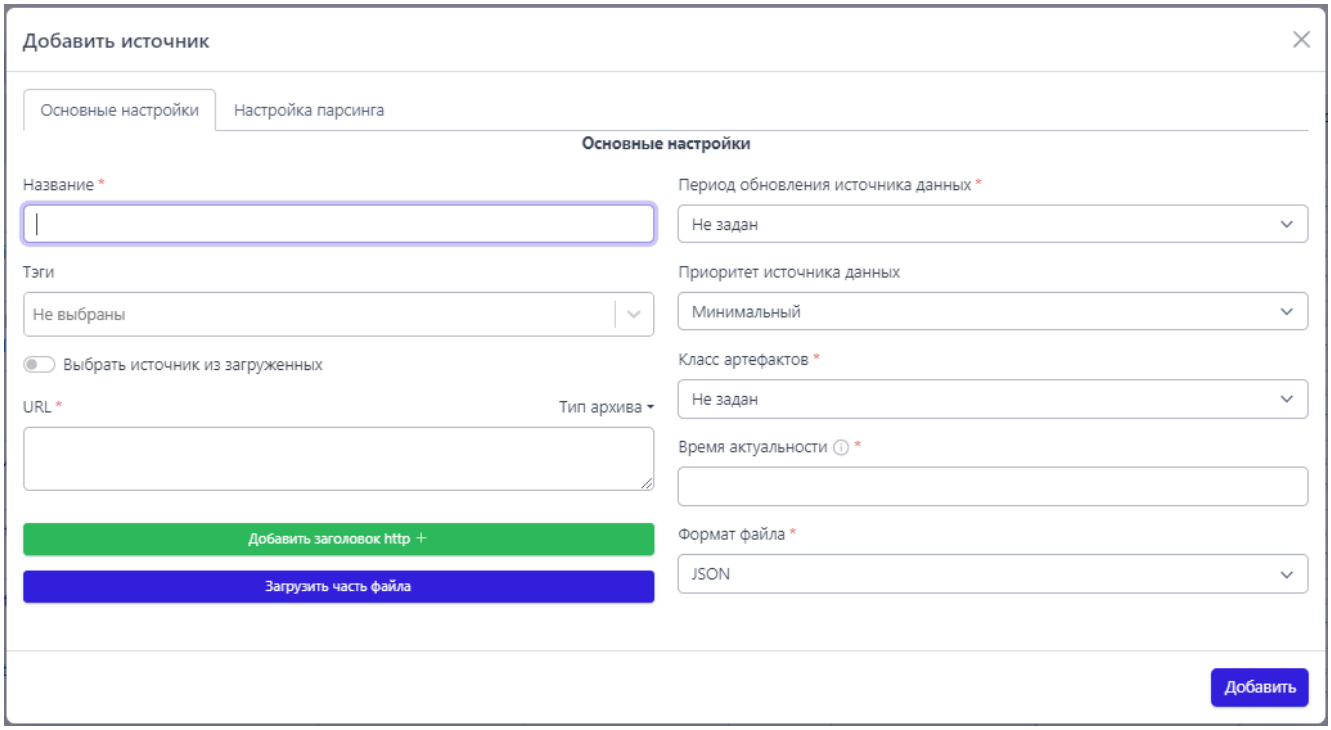


Рисунок 17 – Окно добавления источника данных

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

1) Основные настройки;

2) Настройки парсинга.

Название источника.

Тэги (ключевые слова для удобства категорирования и классификации).

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

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

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).

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.

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).

Время актуальности – период после последней синхронизации, в который полученные об артефакте из файла данные будут считаться актуальными и влиять на вердикт по артефакту. Время актуальности не должно быть меньше периода обновления источника данных, иначе по истечению периода актуальности все данные источника будут считаться устаревшими до следующей синхронизации. Если при последующей синхронизации артефакт пропадает из получаемых данных, данные по нему будут считаться актуальными в указанный период.

Формат файла – 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.

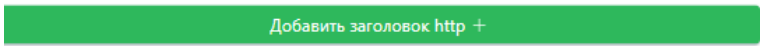
CSV:

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.

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.

При нажатии по иконке 

появляются поля, где 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 выбора источника данных из имеющихся загруженных источников следует сделать активной кнопку выбора ***Выбрать источник из загруженных***, переведя ползунок кнопкой мыши вправо (рисунок 18), при этом становятся активны иконки  – **Загрузить файл,**  – **Перейти к хранилищу**.

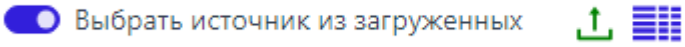


Рисунок 18 – Выбор источника из загруженных

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 19).

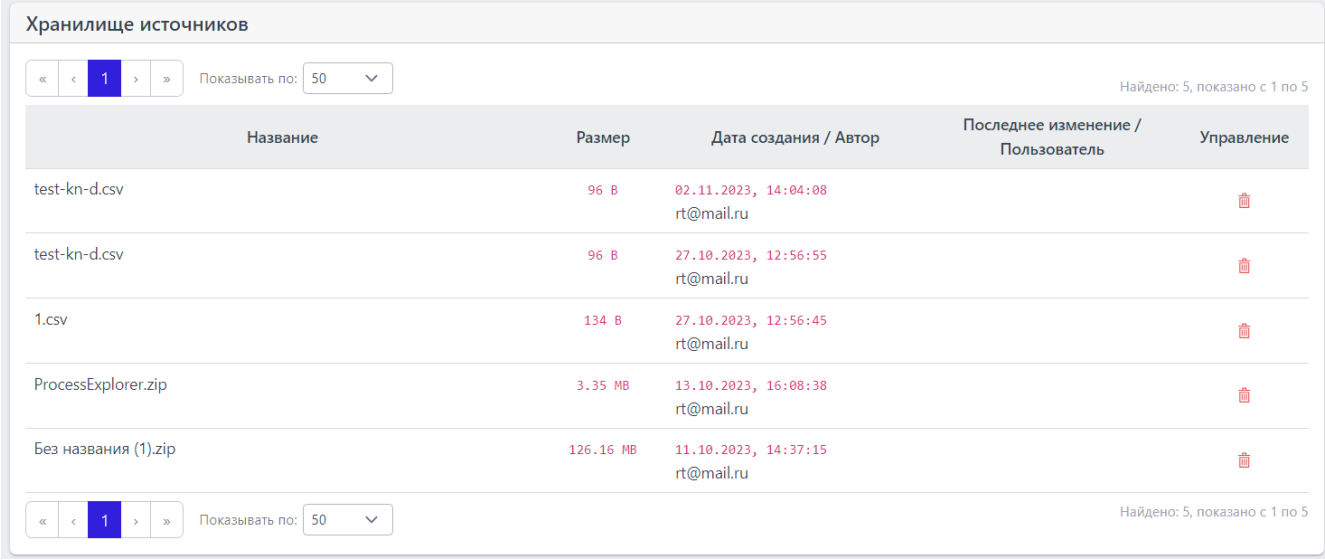


Рисунок 19 – Страница «Хранилище источников»

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 в зависимости от выставленного ранее типа формата файла имеет разные настройки и представлено на рисунках 20 - 22.

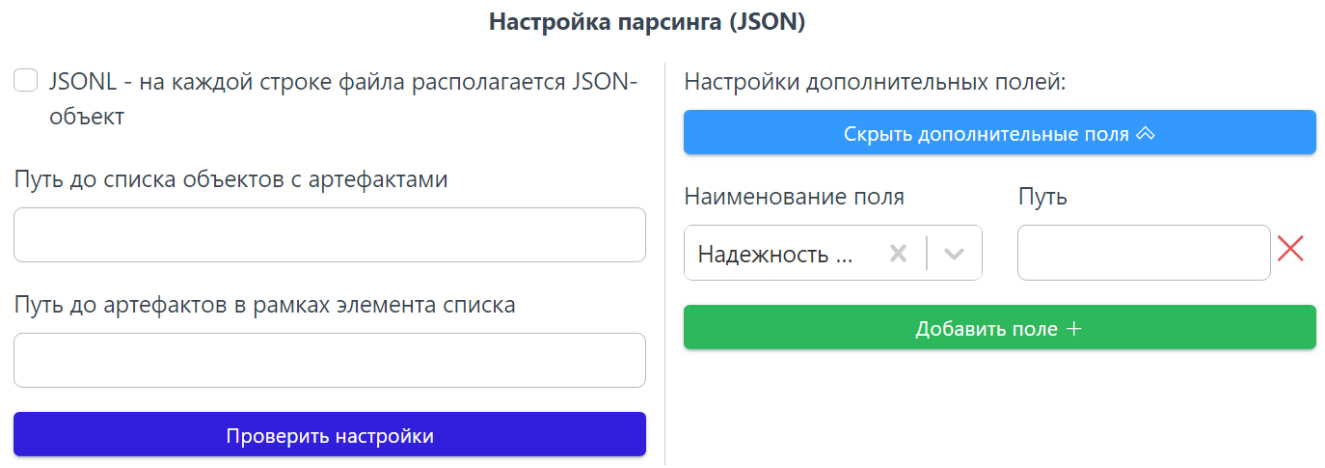


Рисунок 20 – Настройка парсинга файлов в формате JSON

Рисунок 21 – Настройка парсинга файлов в формате CSV

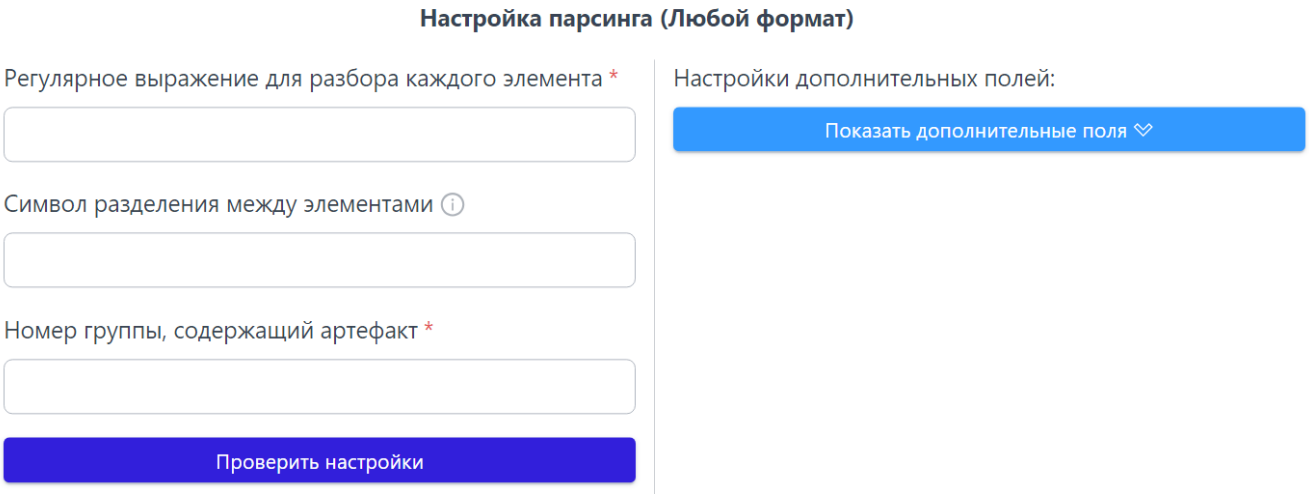


Рисунок 22 – Настройка парсинга файлов любого формата

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 по иконке ***Показать дополнительные поля***, после чего откроется два поля для настройки.

В области ***Наименование поля*** можно выбрать настройку следующих параметров: ***Надежность данных*** и ***Дата обнаружения***.

При выборе параметра настройки ***Надежность данных*** в общей области настройки данных парсинга появляется дополнительное окно, с помощью которого можно мышью изменять параметр надежности данных (указывается в процентах). (рис 23).

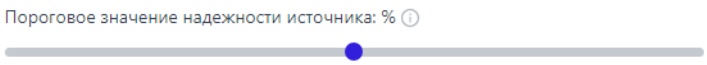


Рисунок 23 – Инструмент по управлению настройки параметра значения надежности источника

Примечание

Поле надежность данных (Confidence) означает надежность, уверенность в данных, доступных об индикаторе компрометации. Можно указать пороговое значение этого поля, ниже которого вердикт из источника данных не будет учитываться. То есть в поле **Путь** будет указываться источник надежности, с которым будет сравниваться задаваемое значение.

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 24.

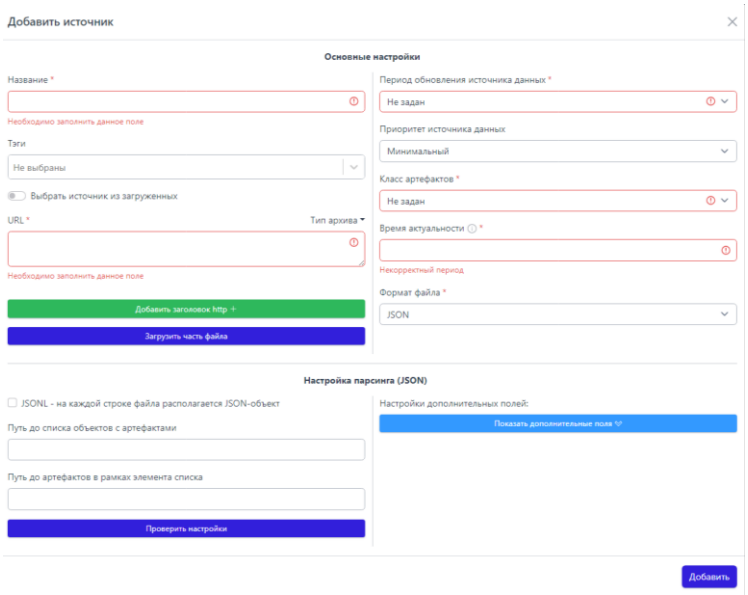


Рисунок 24 – Сообщение об ошибках при добавлении/редактировании информации об источнике

При нажатии по иконке **Загрузить часть файла** в отдельном окне ниже данной иконки будет показана часть файла, предоставленного источником данных (рисунок 25).

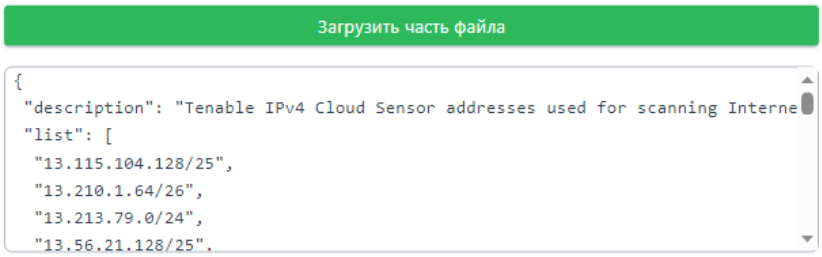


Рисунок 25 – Часть файла, предоставленного источником данных

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 26).

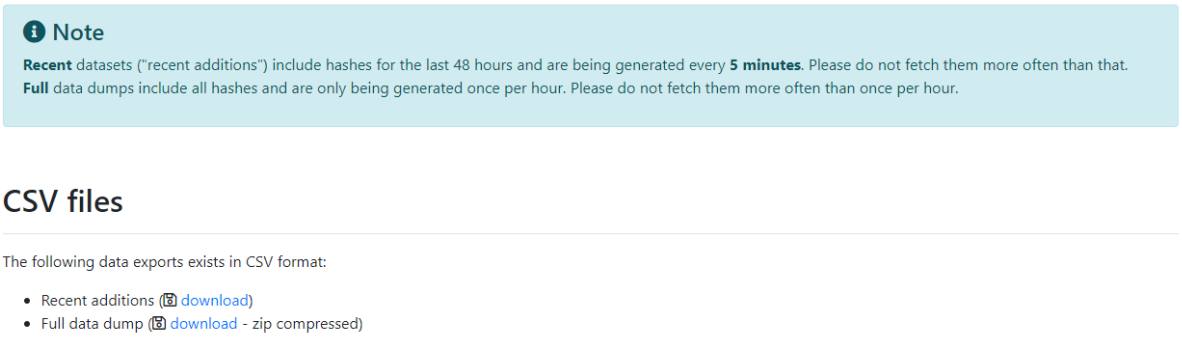


Рисунок 26 – Информация со страницы ссылки на источник

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 **Название**, 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.

Если поля заполнены правильно, через некоторое время на форме отобразится окно, содержащее несколько строчек настраиваемого файла. Это свидетельствует о том, что сервер смог загрузить файл по переданному URL и смог распаковать содержимое файла из архива согласно переданному типу архива (рисунок 27).

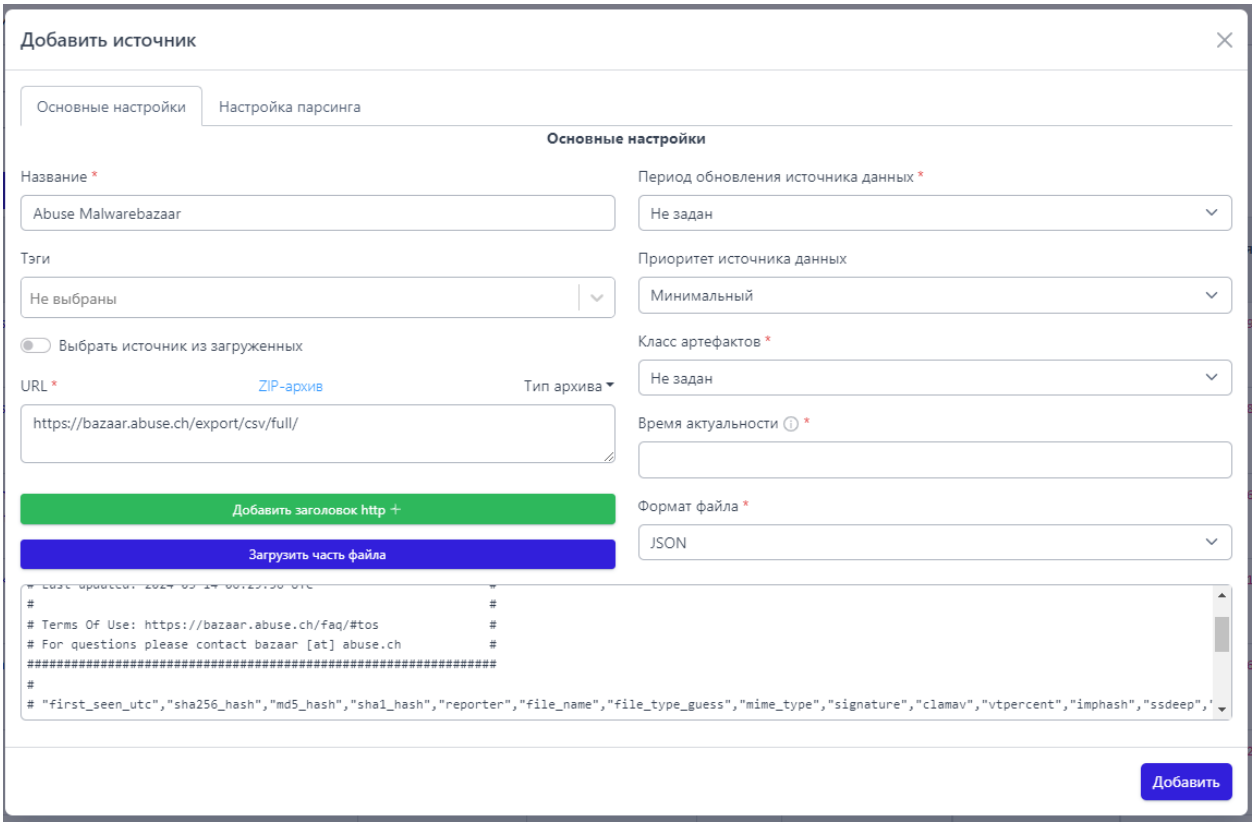


Рисунок 27 – Настройка при добавлении источника

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.

Заполнение полей при настройке источника данных согласно выше приведенному описанию представлено на рисунке 28.

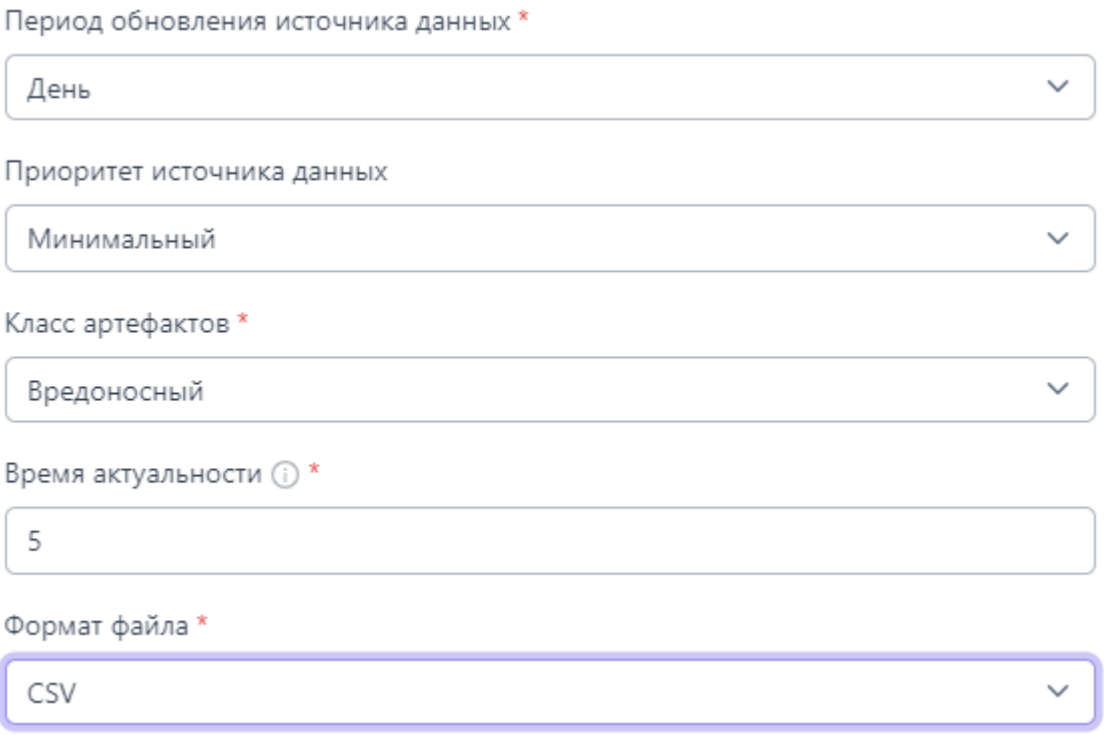


Рисунок 28 – Пример заполнения полей при настройке источника

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","vtpercent","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.

Настройка дополнительных полей при настройке парсинга источника данных представлена на рисунке 29.

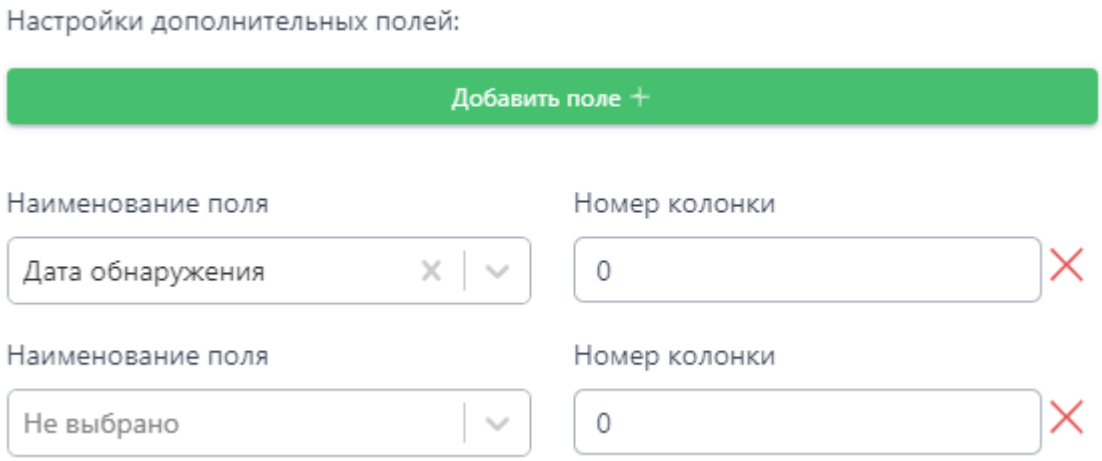


Рисунок 29 – Пример заполнения полей дополнительных полей при настройке парсинга

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 SHA-256 файлов и отображаются 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 30).

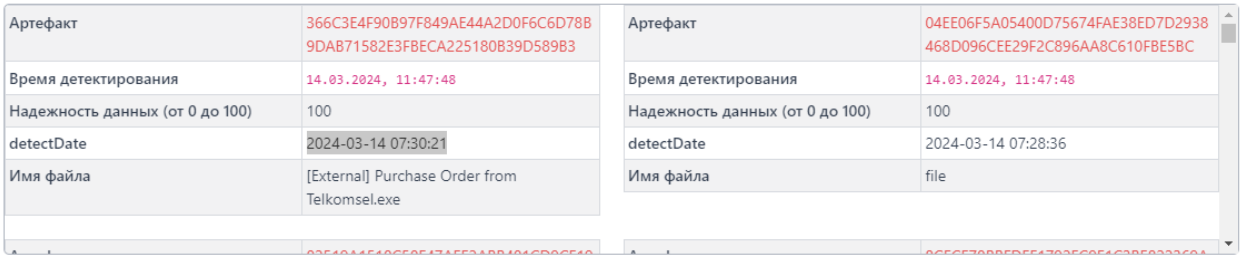


Рисунок 30 – Проверка корректности настроек

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 в 03:00 по времени сервера.

5.4.3. 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 31.

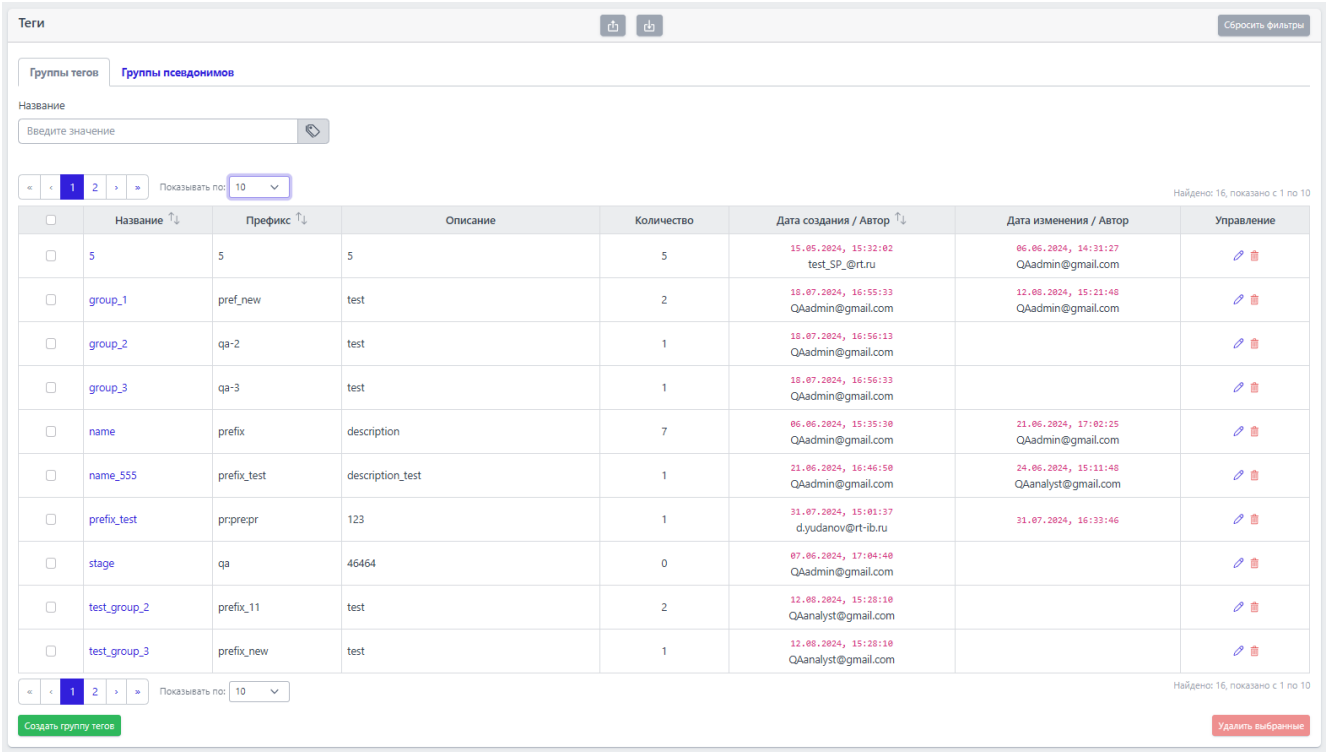


Рисунок 31 – Страница Теги

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 фильтра **Название**.

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 Удалить выбранные.

Для создания новой группы тегов требуется нажать по иконке Создать группу тегов, после чего откроется окно создания группы тегов, представленное на рисунке 32.

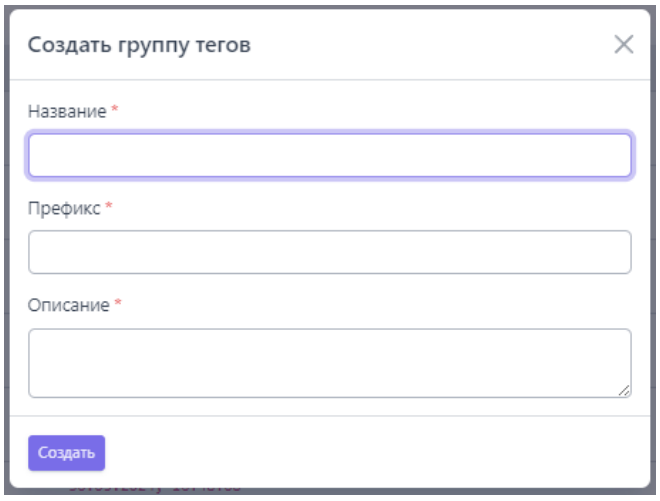


Рисунок 32 – Окно создания группы тегов

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 33.

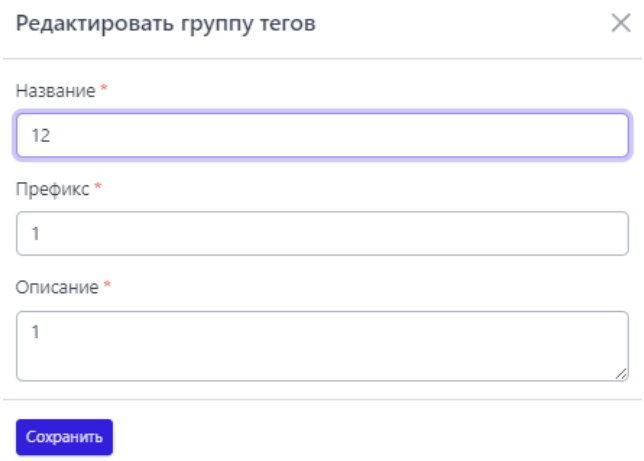


Рисунок 33 – Окно редактирования группы тегов

Название группы тегов на странице **Теги** вкладки **Группы тегов** является активной ссылкой, при нажатии по которой открывается окно с тегами данной группы (рисунок 34).

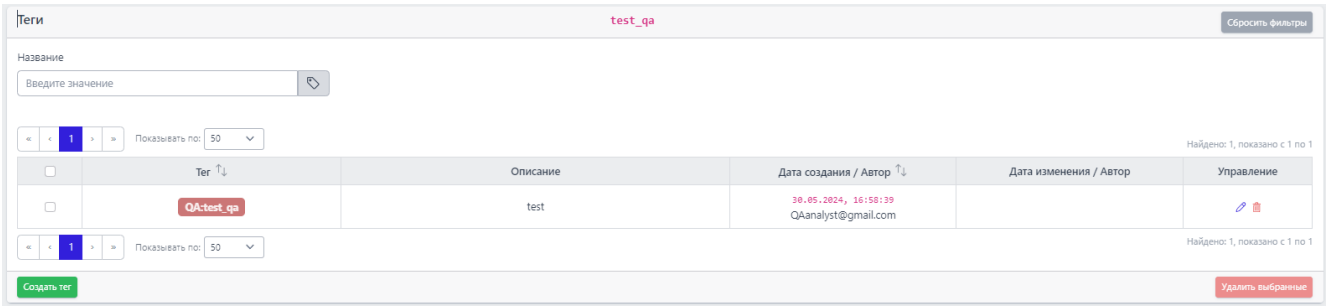


Рисунок 34 – Окно Теги в группе тегов

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

– Кнопка выбора ☐;

– Тег;

– Описание;

– Дата создания/Автор;

– Дата изменения/Автор;

– Управление (редактировать тег , удалить тег).

Для редактирования тега следует в области **Управление** нажать по иконке , после чего появится окно редактирования тега, представленное на рисунке 35.

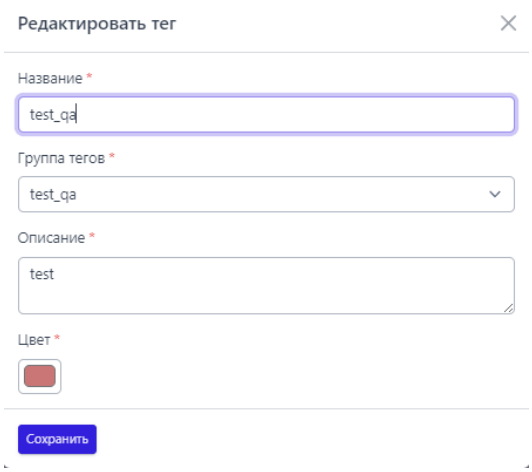


Рисунок 35 – Окно редактирования информации о теге

Для создания нового тега в данной группе следует нажать по иконке Создать тег, после чего откроется окно создания тега, представленное на рисунке 36.

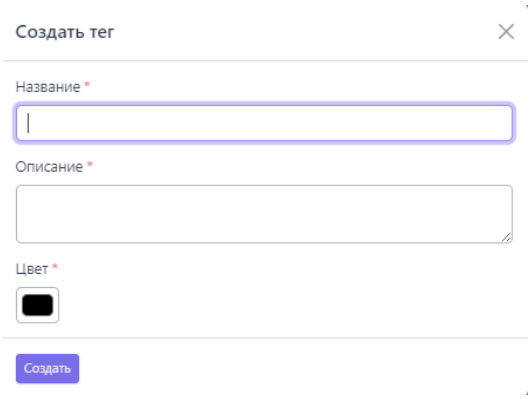


Рисунок 36 – Окно создания тега

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 37.

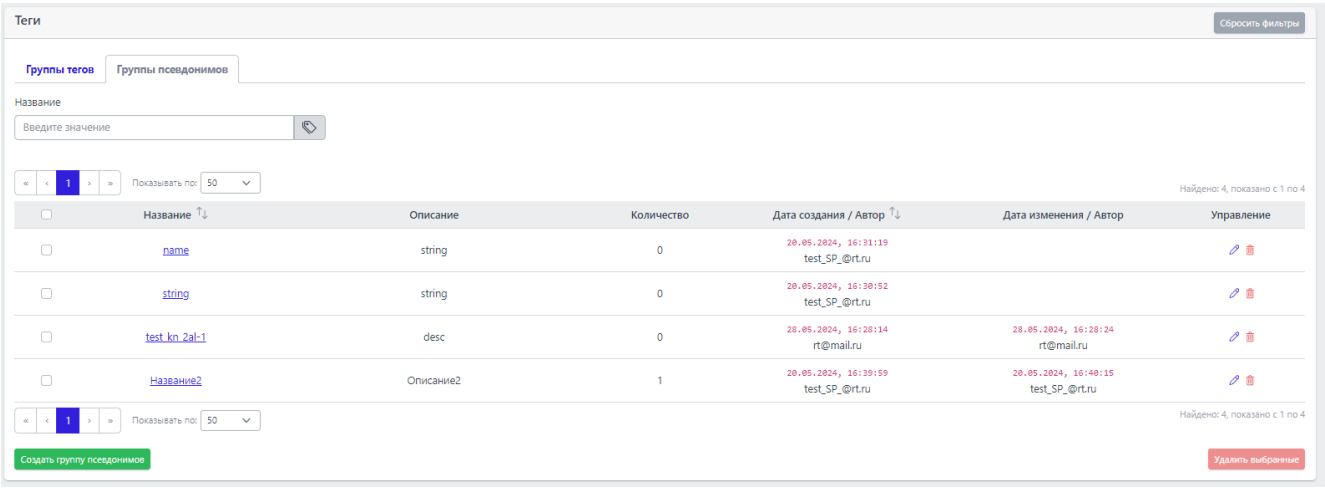


Рисунок 37 – Окно вкладки Группы псевдонимов

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 Удалить выбранные.

Для создания новой группы псевдонимов требуется нажать по иконке Создать группу псевдонимов, после чего откроется окно создания группы, представленное на рисунке 38.

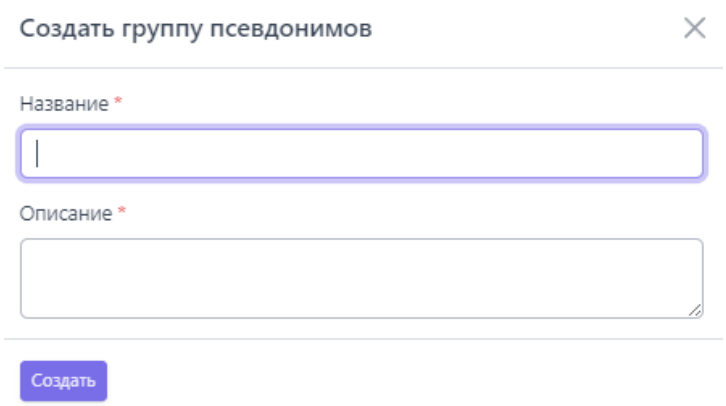


Рисунок 38 – Окно создания группы псевдонимов

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 39.

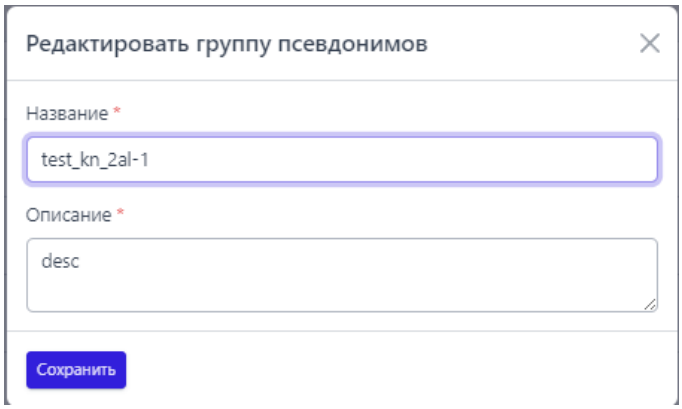


Рисунок 39 – Окно редактирования группы псевдонимов

Название группы псевдонимов на странице **Теги** вкладки **Группы псевдонимов** является активной ссылкой, при нажатии по которой открывается окно с псевдонимами данной группы (рисунок 40).

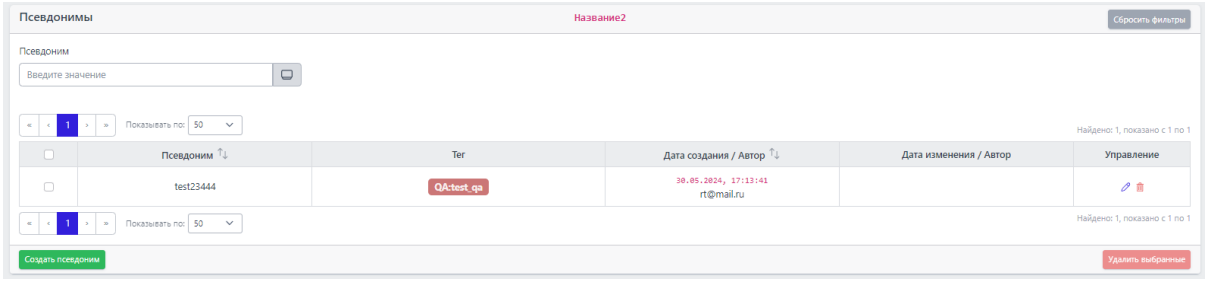


Рисунок 40 – Окно Псевдонимы в группе псевдонимов

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

– Кнопка выбора ;

– Псевдоним;

– Тег;

– Дата создания/Автор;

– Дата изменения/Автор;

– Управление (редактировать псевдоним , удалить псевдоним).

Для редактирования псевдонима следует в области **Управление** нажать по иконке , после чего появится окно редактирования псевдонима, представленное на рисунке 41.

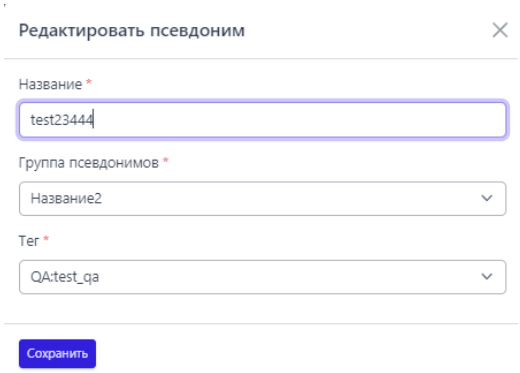


Рисунок 41 – Окно редактирования информации о псевдониме

Для создания нового тега в данной группе следует нажать по иконке Создать тег, после чего откроется окно создания псевдонима, представленное на рисунке 42.

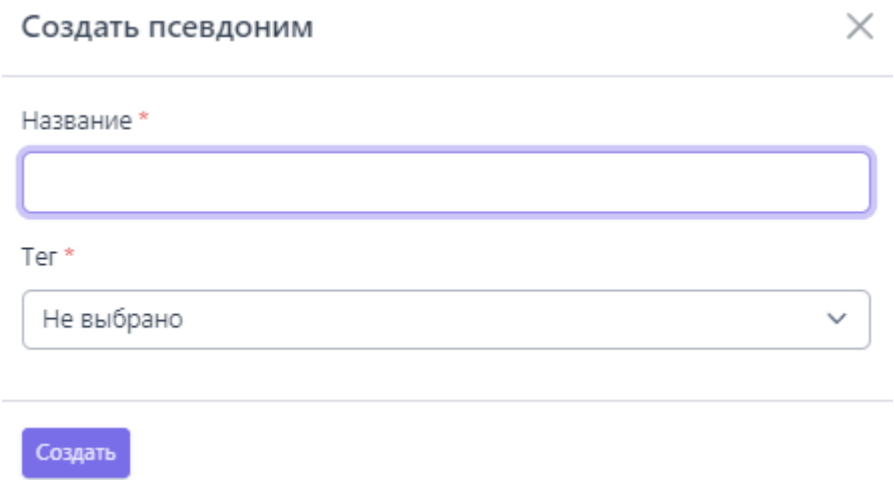


Рисунок 42 – Окно создания псевдонима

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

У пользователя имеется возможность экспортировать в файл наборы с группами тегов, нажав по иконке  . Для импорта файла в набор тегов используется иконка  .

Механизм тегов в RT Protect TI

В механизме тегов в RT Protect TI теги из собственной библиотеки тегов могут назначаться трем различным 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.

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 пунка 3 выше. Если псевдоним не найдет, 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 назначенные элементу каждого источника данных (п. 3.). При этом редактируется только та часть тегов, назначенная 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.

5.5 Аналитика

5.5.1. 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 43 - 45.

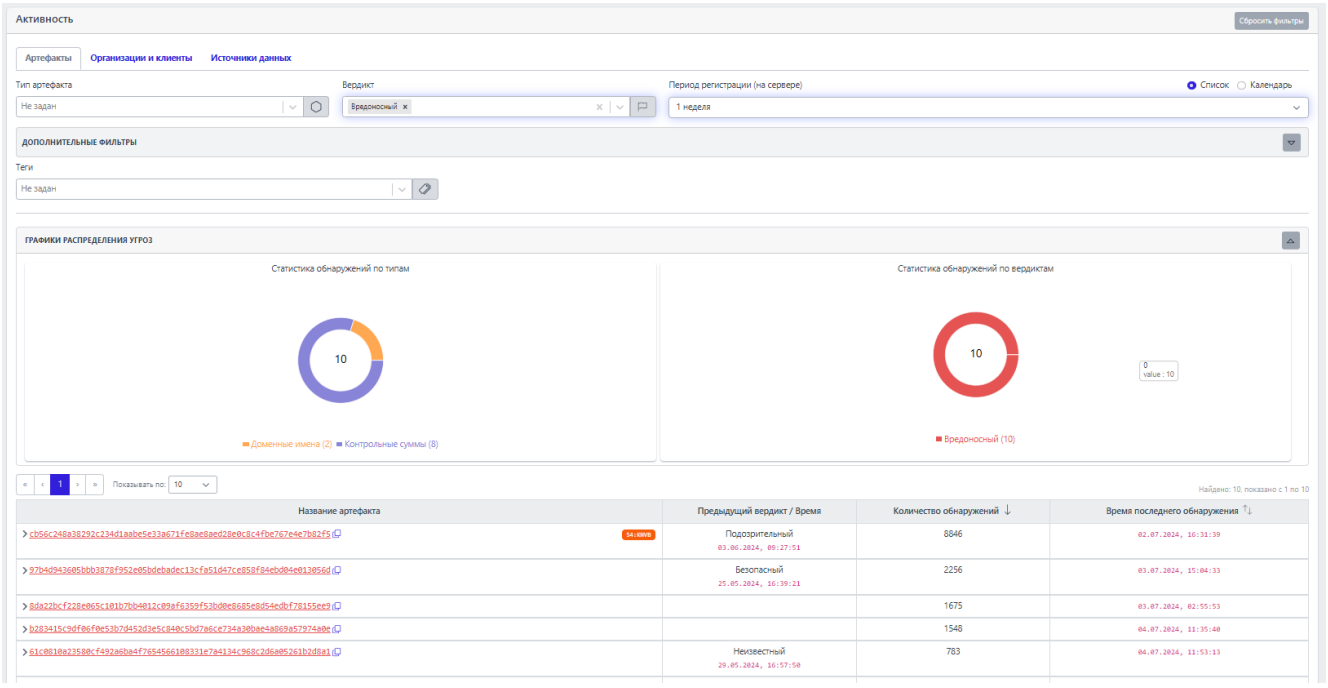


Рисунок 43 – Страница Активность вкладка Артефакты

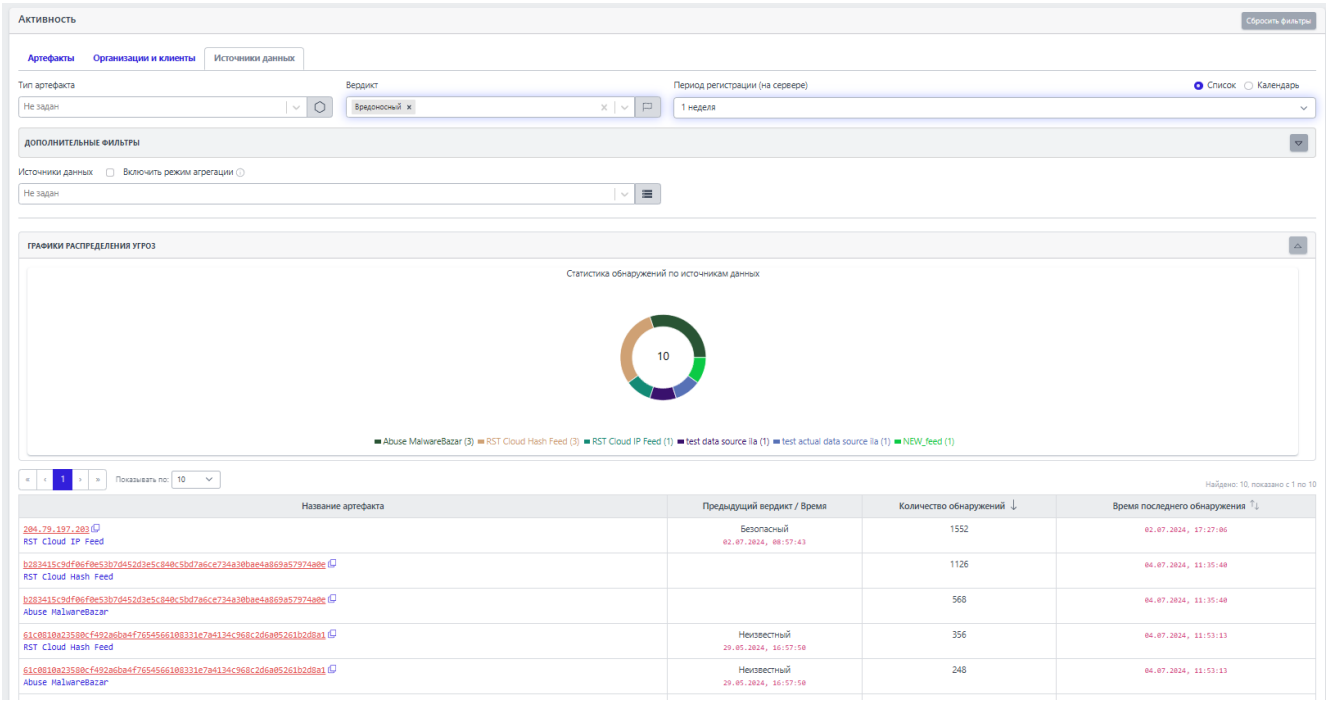


Рисунок 44 – Страница Активность вкладка Источники данных

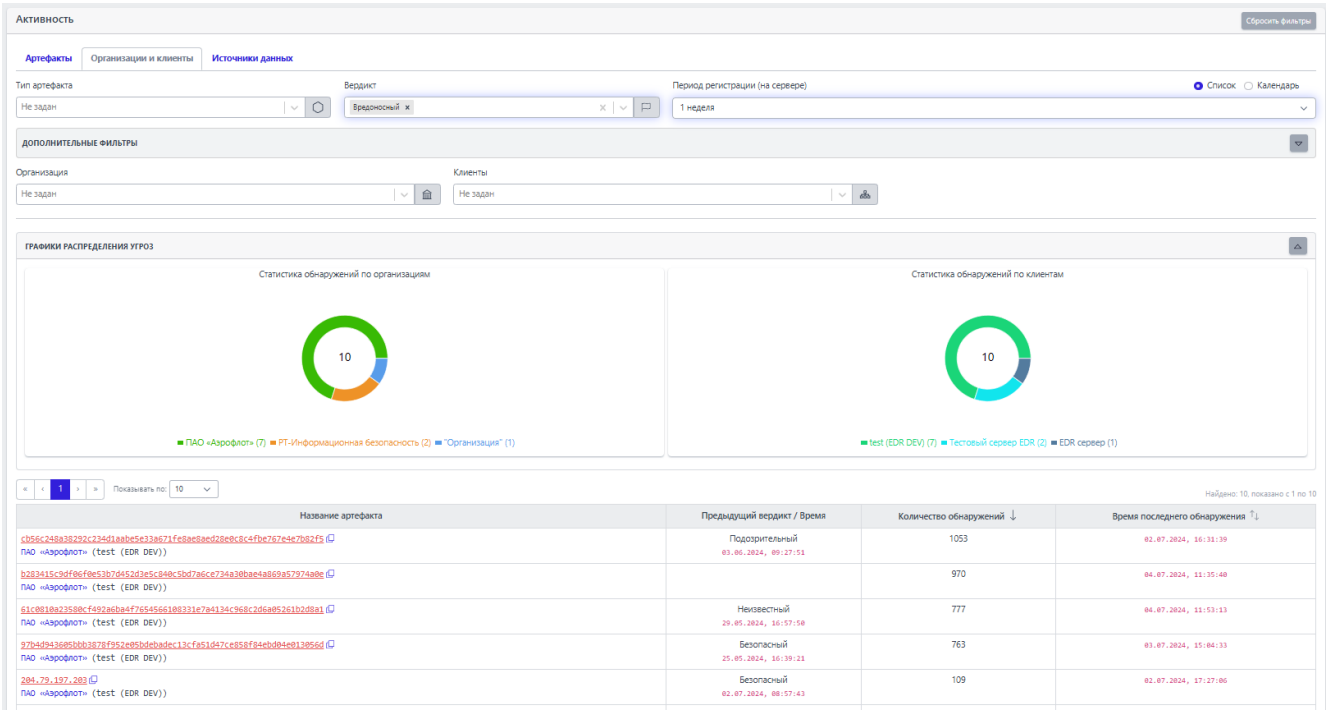


Рисунок 45 – Страница Активность вкладка Организации и клиенты

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:

– 630ae106a99ae7da5d8dd33e7704b27701f69 – вредоносный артефакт (шрифт красного цвета);

– 02f0c498bb4e5f62722ab5e8a63f5b3779db88ef – безопасный артефакт (шрифт зеленого цвета);

– B73753C4C69A03F9A3E09F121B6599D77B1A4BE0247F9B71B56572555E1FE12B – неизвестный артефакт (шрифт серого цвета);

– 61F897ED69646E0509F6802FB2D7C5E88C3E3B93C4CA86942E24D203AA878863 – подозрительный артефакт (шрифт оранжевого цвета).

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 46.

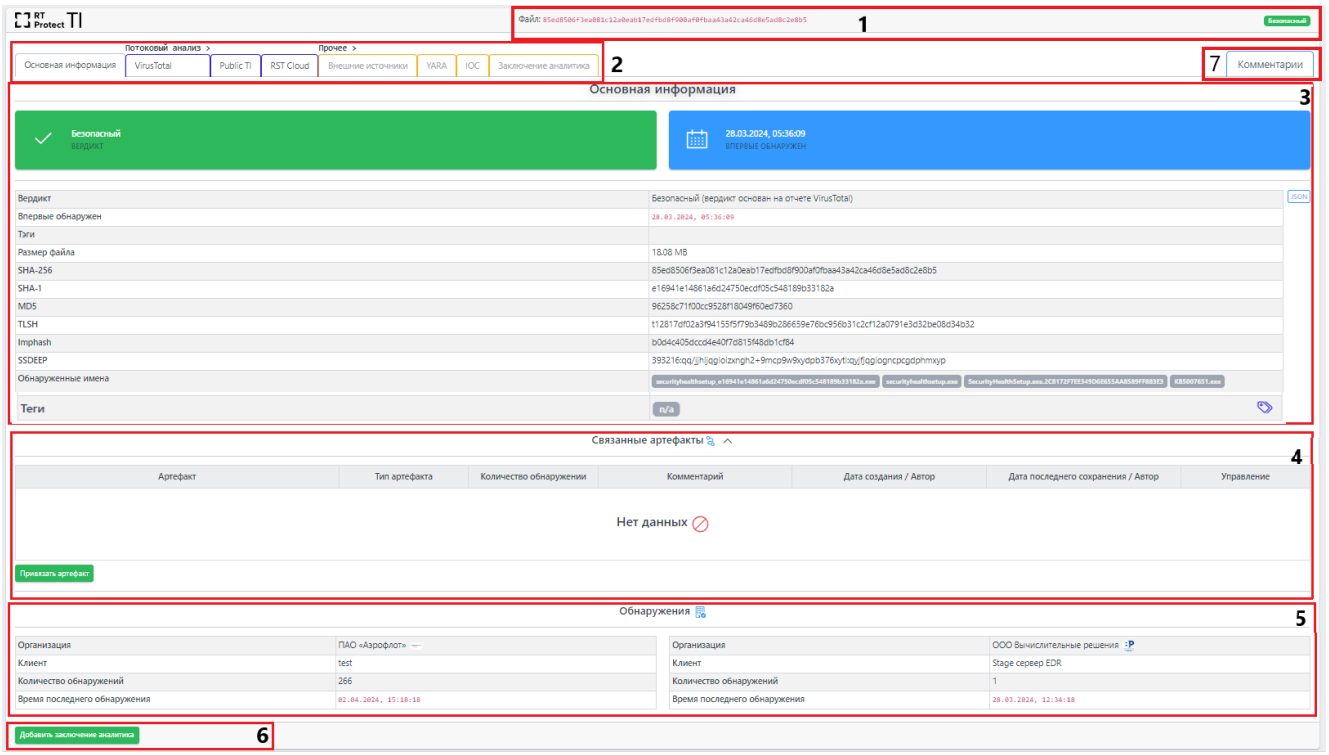


Рисунок 46 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

1) область краткой информации об угрозе;

2) область вкладок;

3) область основной информации;

4) область связанных с артефактом других артефактов;

5) область обнаружения (оказывает другие организации на которых были обнаружения по данному артефакту);

6) область добавления заключения аналитика;

7) область для добавления комментария.

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 вкладок отображается вкладка основной информации отчета TI-платформы, вкладки отчетов по угрозе от сторонних подключенных сервисов, разделенных по группам:

1) потоковый анализ (Virus Total, Public TI, RST Cloud и т.д.);

2) остальные (Внешние источники, YARA, IOC, Заключение аналитика).

Состав этих вкладок может меняться в зависимости от интегрированных модулей и интеграций.

Если в области вкладок запись отображается серым цветом, запрос информации по данному артефакту в том или ином сервисе недоступен. При нажатии ЛКМ по одной из вкладок появляется окно результатов по анализу артефакта (рис. 47).

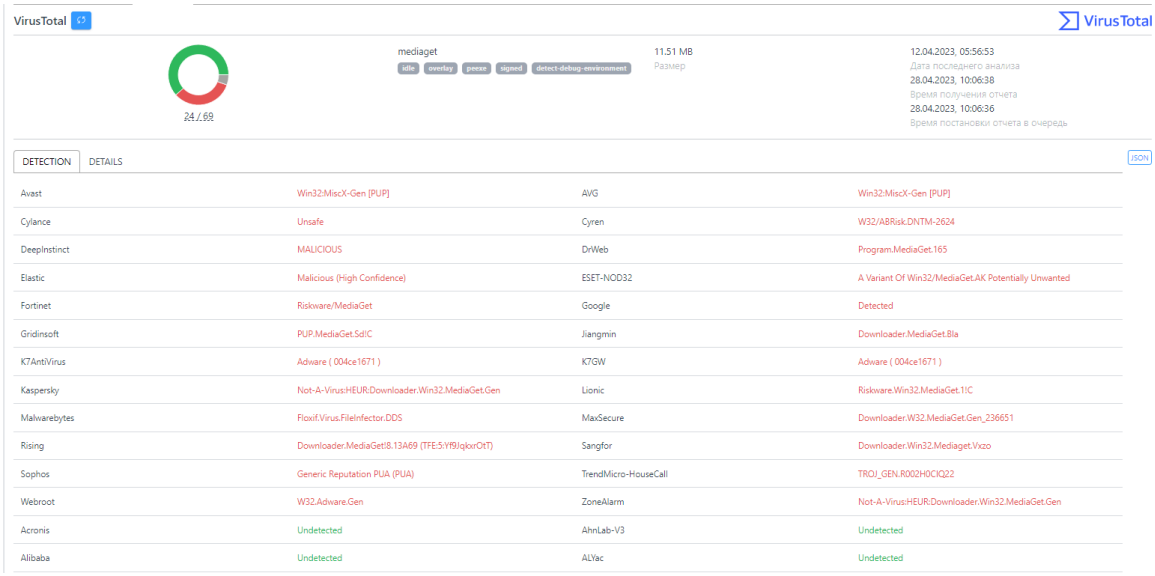


Рисунок 47 – Результаты анализа артефакта на странице Virus Total

Окно основной информации по результатам анализа артефакта в формате HTML представлено на рисунке 48.

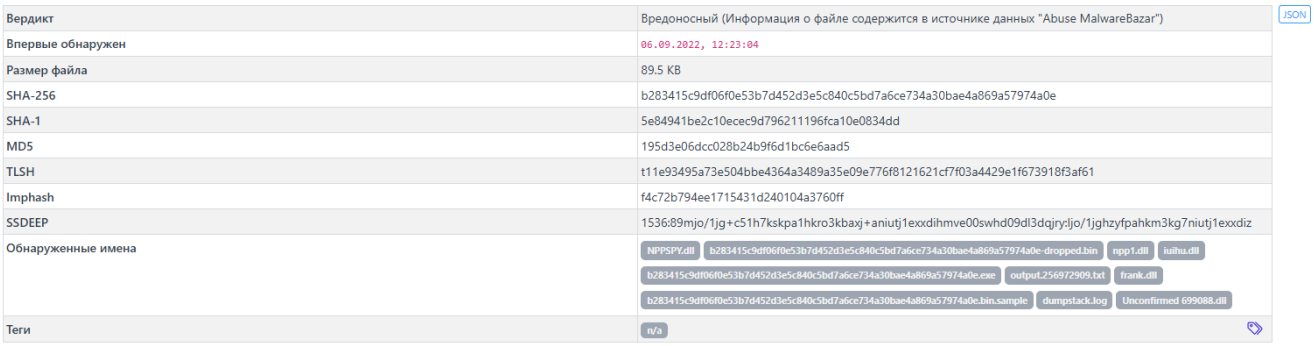


Рисунок 48 – Информация отчета об артефакте в формате HTML

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 49.

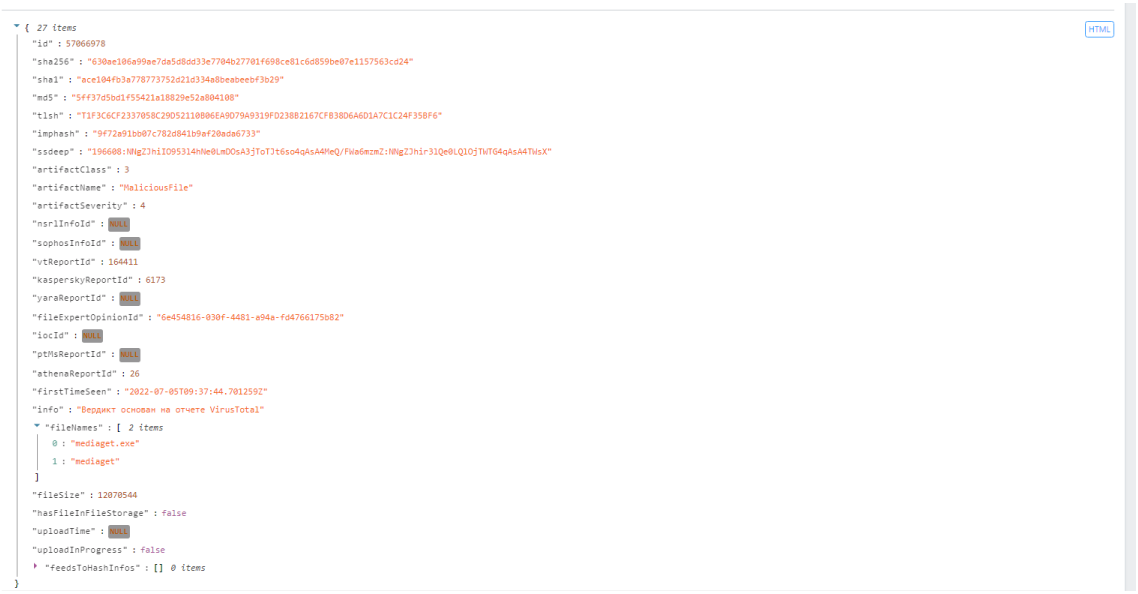
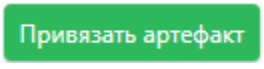


Рисунок 49 – Информация отчета об артефакте в формате JSON

В области **Связанные артефакты** показывается таблица с описанием артефакта, связанного с тем артефактом, отчет по которому просматривается на данный момент. При нажатии по иконке 

, открывается окно для привязки артефактов друг к другу (см. рисунок 50).

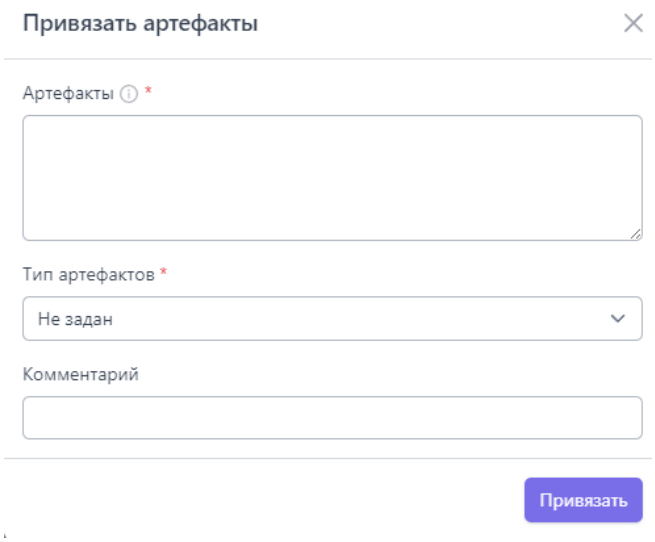


Рисунок 50 – Окно для привязки артефакта

В данном окне добавляется один или несколько артефактов, тип артефакта и комментарий.

После добавления информации следует нажать по иконке «Привязать». После привязки артефакт появится в списке связанных артефактов.

Примечание

Привязка разных типов артефактов допускается. Т.е. ip-адрес и хеш-сумма могут быть привязаны друг к другу.

Для любого артефакта, хранящегося на сервере аналитики, администратор или аналитик может создать заключение, которое будет показывать, как артефакт определяется в программе. То есть заключение аналитика является приоритетным по отношению к любым внешним источникам данных.

При нажатии по иконке Добавить заключение аналитика появляется окно, в котором администратор/аналитик выносят вердикт по результатам анализа артефакта (рис. 51).

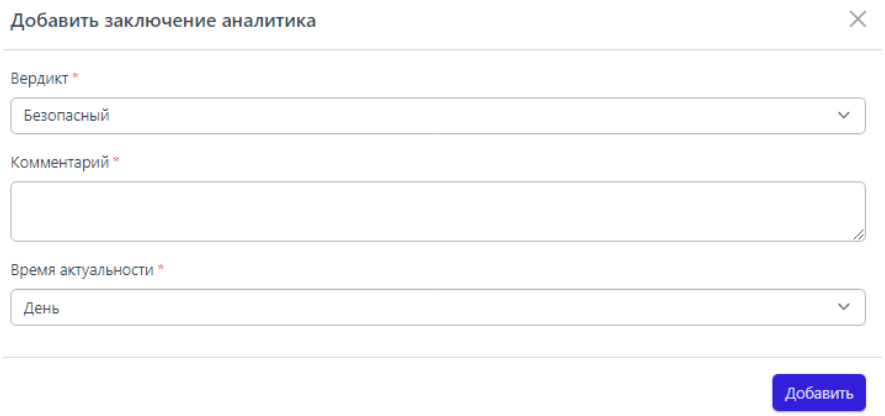


Рисунок 51 – Окно добавления заключения аналитика

После заполнения информации в данном окне требуется сохранить результат, нажав по иконке **Добавить.**

После добавления заключения аналитика информацию можно просмотреть, перейдя на вкладку **Заключение аналитика** на странице с отчетом (рисунок 52).

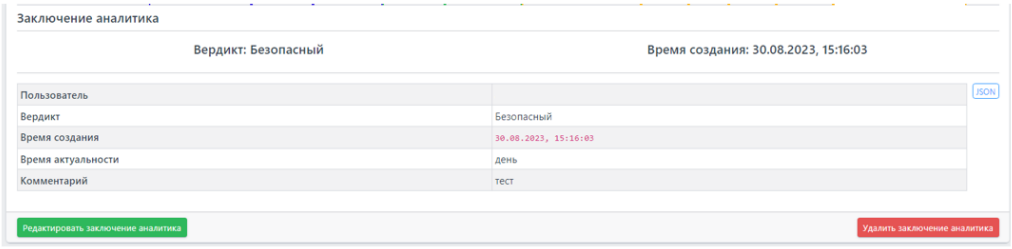


Рисунок 52 – Информация в поле «Заключение аналитика»

Заключение аналитика можно редактировать или удалить, нажав по соответствующим иконкам.

Заключение аналитика является приоритетным для любого артефакта в программе, поэтому пользователь программы может обозначать артефакты, которые внешними источниками отмечены безопасными, как вредоносные и наоборот. Пользователь может в любой момент отредактировать вердикт по артефакту по своему усмотрению, добавив или отредактировав заключение аналитика.

Для добавления комментария на странице отчет TI платформы по обнаруженной угрозе требуется нажать по иконке Комментарии, после чего откроется поле добавления комментария, представленное на рисунке 53.

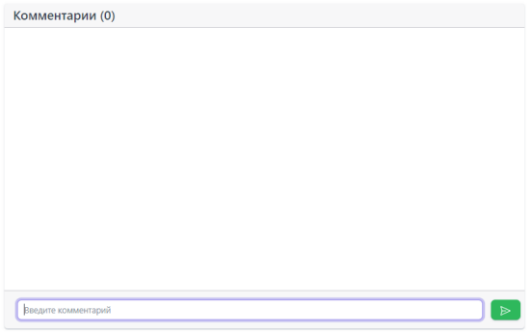


Рисунок 53 – Окно ввода комментария

После ввода текста комментария требуется нажать по иконке , после чего появится короткое всплывающее сообщение о добавлении комментария, и он будет добавлен в поле **Комментарии** с указанием, какой пользователь и когда добавил комментарий. После добавления комментария имеется возможность его редактировать или удалить.

В области **Основная информация** в нижней строке имеется иконка , с помощью которой можно добавить тег для артефакта. При нажатии по данной иконке во всплывающем окне (см. рисунок 54), можно выбрать тег из списка тегов, созданных с помощью раздела **Теги**.

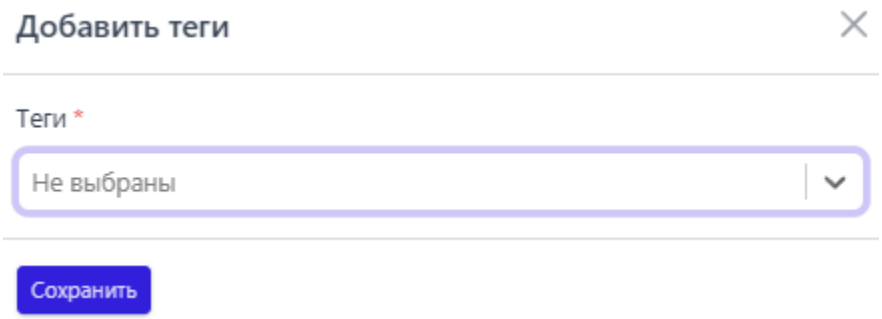


Рисунок 54 – Добавление тега

Для фильтрации информации на странице **Активность** вкладки **Артефакты** 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, все время), либо в виде календаря (начальная и конечная даты);

– **Теги.**

Также имеется система дополнительных фильтров, которые по умолчанию скрыты, но при нажатии по кнопке  появляются следующие фильтры, которые представлены на рисунке 55.

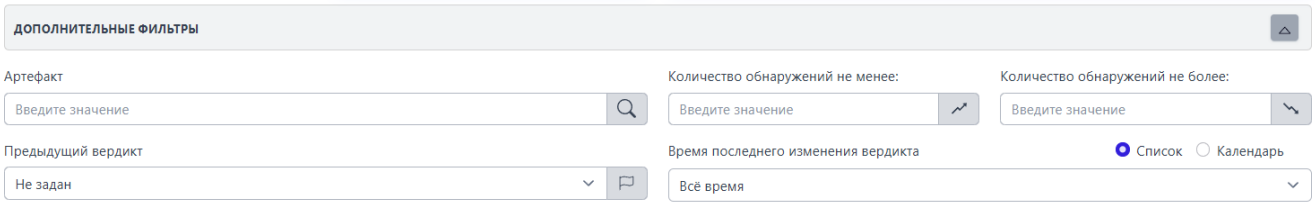


Рисунок 55 – Дополнительные фильтры на странице Активность/Артефакты

Дополнительные фильтры представлены согласно следующего списка:

– **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта.**

На странице **Активность** вкладки **Артефакты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 56).

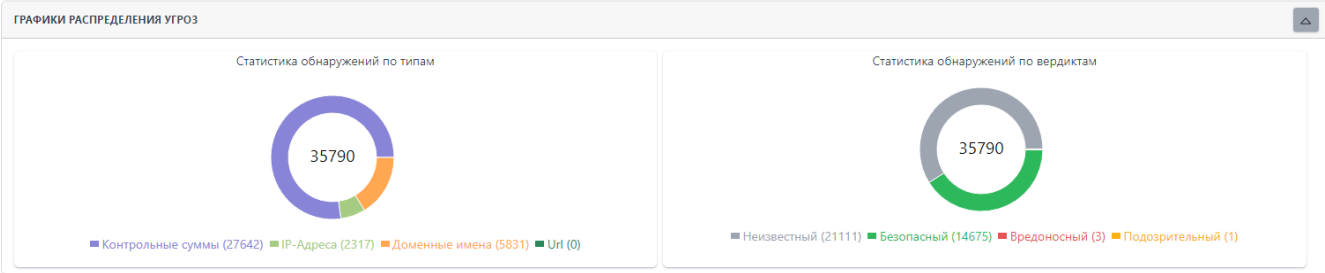


Рисунок 56 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

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** вкладка **Источники данных** 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).

Также имеется система дополнительных фильтров, которые по умолчанию скрыты, но при нажатии по кнопке появляются следующие фильтры, которые представлены на рисунке 57.

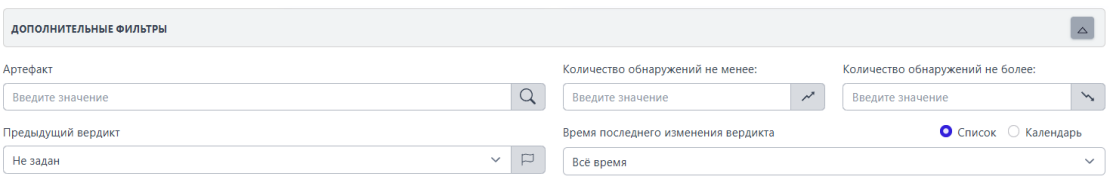


Рисунок 57 – Дополнительные фильтры на странице Активность/ вкладки Источники данных

Дополнительные фильтры представлены согласно следующему списку:

– **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта;**

В фильтре источника данных можно осуществить выборку по критериям согласно следующему списку:

– по одному источнику данных;

– по нескольким источникам данных;

– по всем источникам данных согласно одной категории.

Важно

Следует отметить, что после выставления в фильтре источников данных параметров для фильтрации, в таблице активности будут отображаться артефакты согласно выставленным источникам данных, но основополагающим вердиктом будет вердикт, установленный аналитиком.

При установке галочки напротив надписи **Включить режим агрегации** в фильтре **Источники данных**, появятся два поля, с помощью которых можно производить фильтрацию в таблице активности (см. рисунок 58).

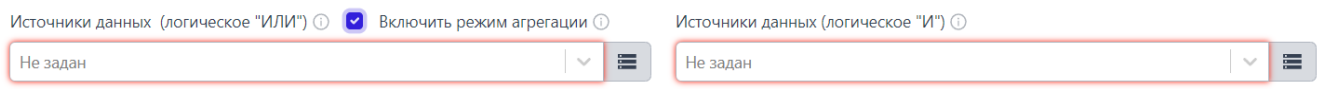


Рисунок 58 – Фильтр по источнику данных на странице Активность

На странице **Активность** вкладки **Источники данных** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 59).

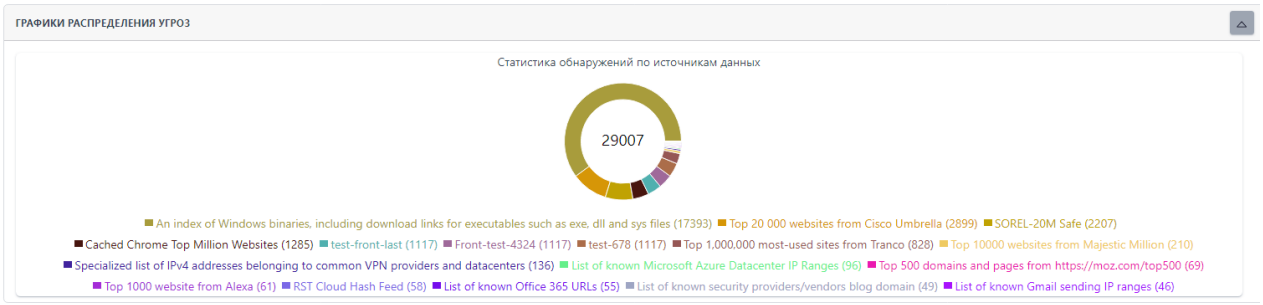


Рисунок 59 – Область графического отображения информации по обнаруженным угрозам вкладка Источники данных

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

– статистика обнаружений по источникам данных.

Для фильтрации информации на странице **Активность** вкладка **Организации и 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);

Так же имеется система дополнительных фильтров, которые по умолчанию скрыты, но при нажатии по кнопке  , появляются следующие фильтры которые представлены на рисунке 60.

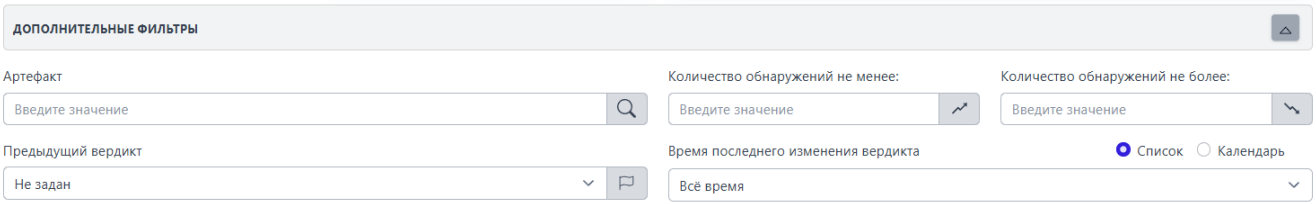


Рисунок 60 – Дополнительные фильтры на странице Активность/Организации и клиенты

Дополнительные фильтры представлены согласно следующего списка:

– **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта;**

– **Организация;**

– **Клиенты.**

На странице **Активность** вкладки **Организации и клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 61).

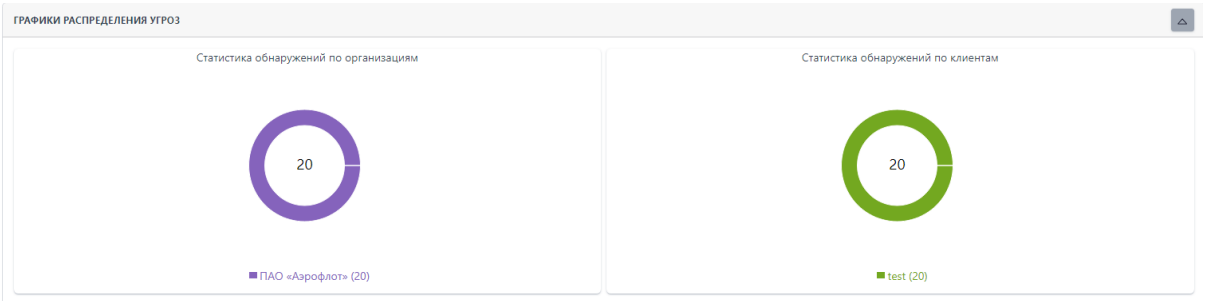


Рисунок 61 – Область графического отображения информации по обнаруженным угрозам вкладка Организации и клиенты

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

– статистика обнаружений по организациям;

– статистика обнаружений по клиентам.

5.5.2. Заключения аналитика

В разделе Заключение аналитика в табличной форме представлена информация о зарегистрированных на портале заключениях аналитика. Общий вид страницы представлен на рисунке 62.

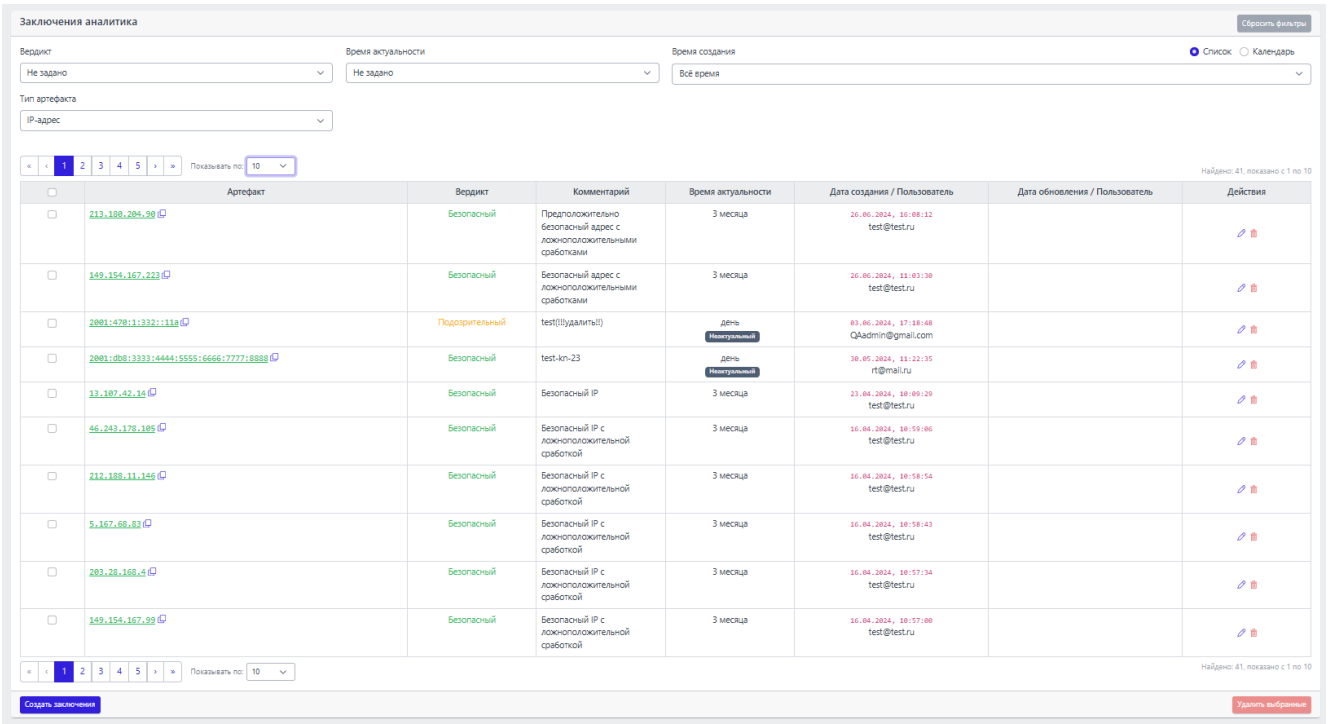


Рисунок 62 – Страница Заключения аналитика

В таблице имеются следующие поля:

– Артефакт (в столбце отображается артефакт, для которого имеется заключение аналитика);

– Вердикт (в столбце отображается вердикт для артефакта);

– Комментарий;

– Время актуальности (отображается время, показывающее, сколько будет актуален вердикт (заключение аналитика) по данному артефакту;

– Дата создания/Пользователь;

– 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);

– Время создания (возможно задать начальную и конечную дату, а также, время создания заключения);

– Тип артефакта (файл, ip-адрес, доменное имя, URL, Email).

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

– 630ae106a99ae7da5d8dd33e7704b27701f69 – 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 63.

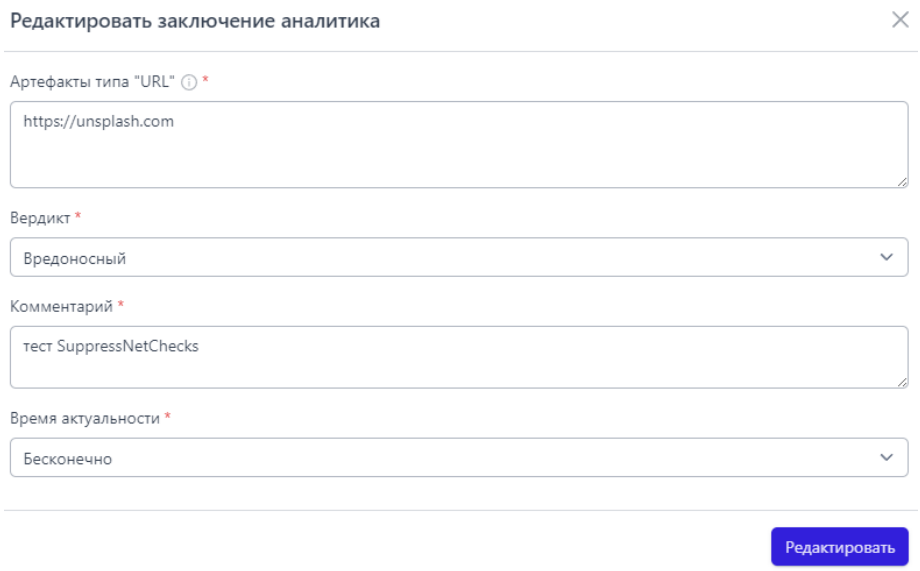


Рисунок 63 – Окно редактирования заключения аналитика

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 64).

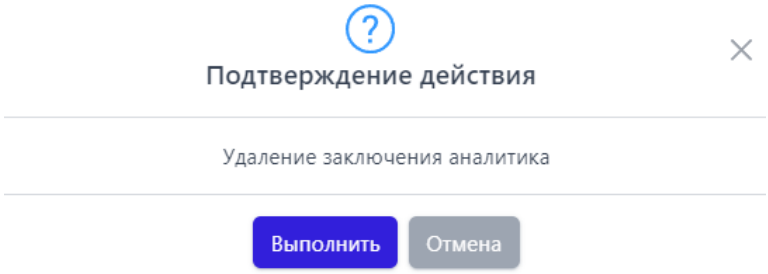
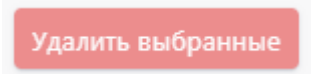
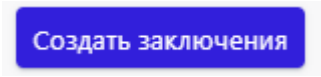


Рисунок 64 – Окно подтверждения действия удаления заключения аналитика

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 65.

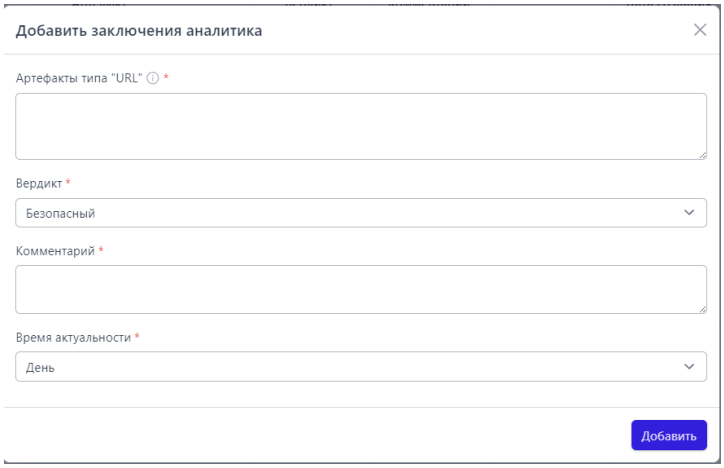


Рисунок 65 – Окно добавления заключения аналитика

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

5.5.3. Отчеты

В разделе **Отчеты** в табличной форме представлена информация о проверенных внешними анализаторами, для которых настроена интеграция, артефактах. Общий вид страницы представлен на рисунке 66.

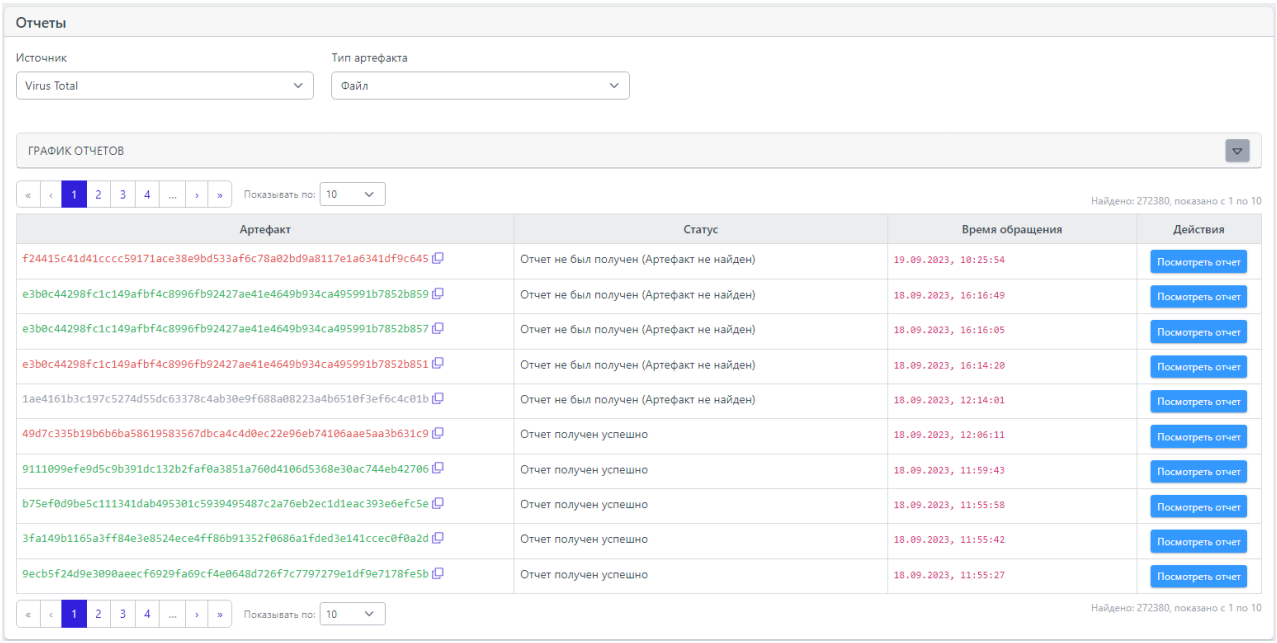


Рисунок 66 – Окно раздела «Отчеты»

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);

– **Статус** (в столбце отображается информация о получении отчета (отчет получен успешно, отчет не был получен));

– **Время обращения** (время, в которое был запрошен отчет);

– **Действия** (получить отчет).

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).

Над таблицей для фильтрации информации имеются следующие фильтры:

– **Источник** (Virus Total, Public TI, Athena, RST Cloud);

– **Тип артефакта** (файл, IP-адрес, доменное имя, URL).

Над таблицей для отображения визуальной информации имеется область с графиком полученного числа отчетов за определенный период в зависимости от установленного в фильтре источника данных (рисунок 67).

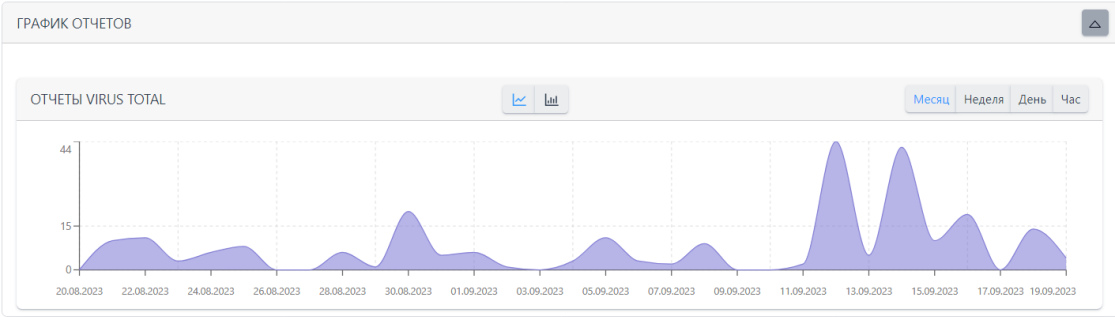
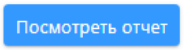


Рисунок 67 – Отчеты Virus Total

Для сворачивания области **График отчетов** требуется нажать по иконке  .

Для просмотра отчета по артефакту нужно нажать по иконке 

.

Страница отчета по артефакту представлена на рисунке 68.

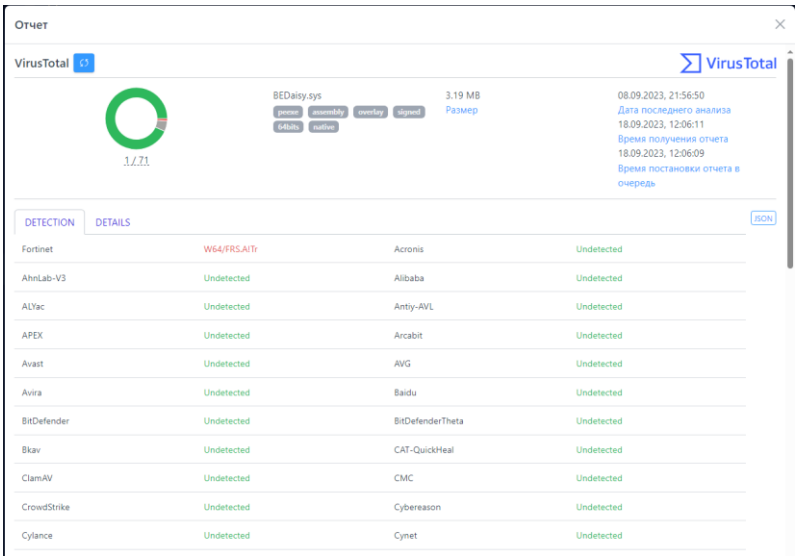


Рисунок 68 – Страница отчета по артефакту от источника Virus Total

5.5.4. Граф связей

Страница «Граф связей» с незаполненным полем артефакта представлена на рисунке 69.

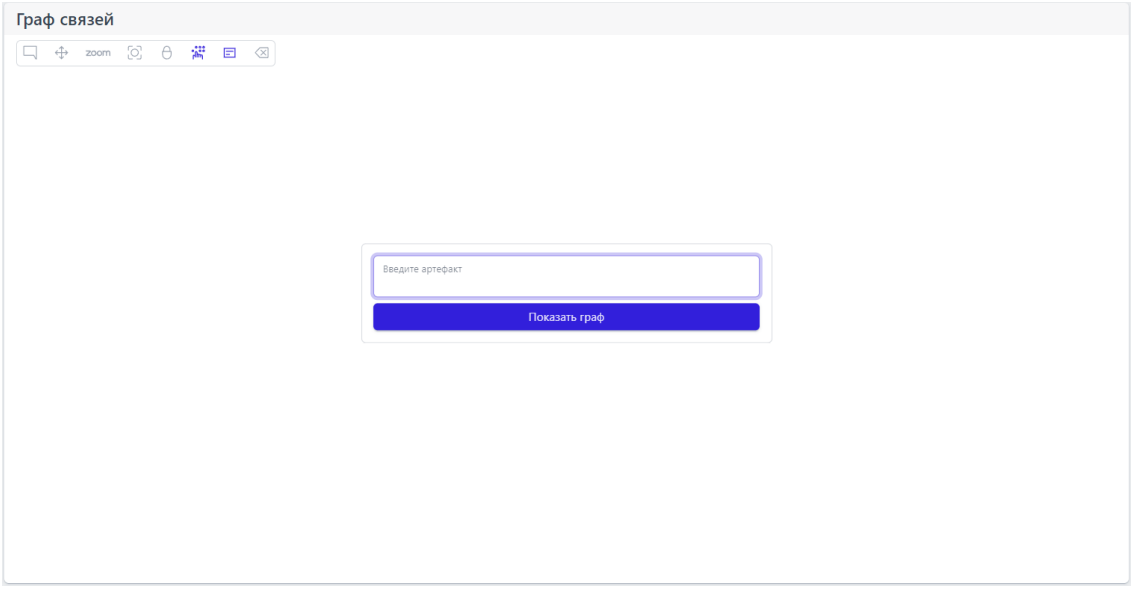


Рисунок 69 – Общий вид пустой страницы «Граф связей»

На странице имеется две области:

– область с иконками-подсказками для управления визуальной частью графа;

– область для введения информации по артефакту, для которого требуется построить граф.

В области управления визуальной частью графа находятся иконки, при наведении на которые указателя мыши появляются всплывающие сообщения (подсказки) для управления графом.

Пример отображения графа после заполнения поля артефакта в виде ip-адреса представлен на рисунке 70.

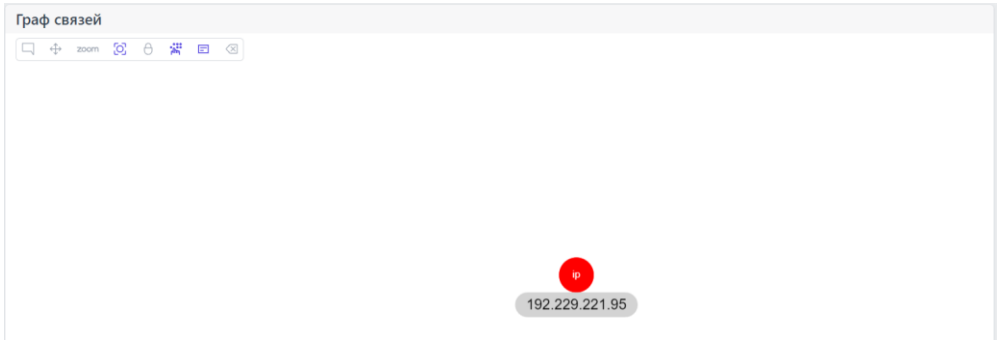


Рисунок 70 – Отображение графа связей для артефакта типа ip-адрес

Пример отображения графа связей для артефакта типа домен с привязанными артефактами представлен на рисунке 71.

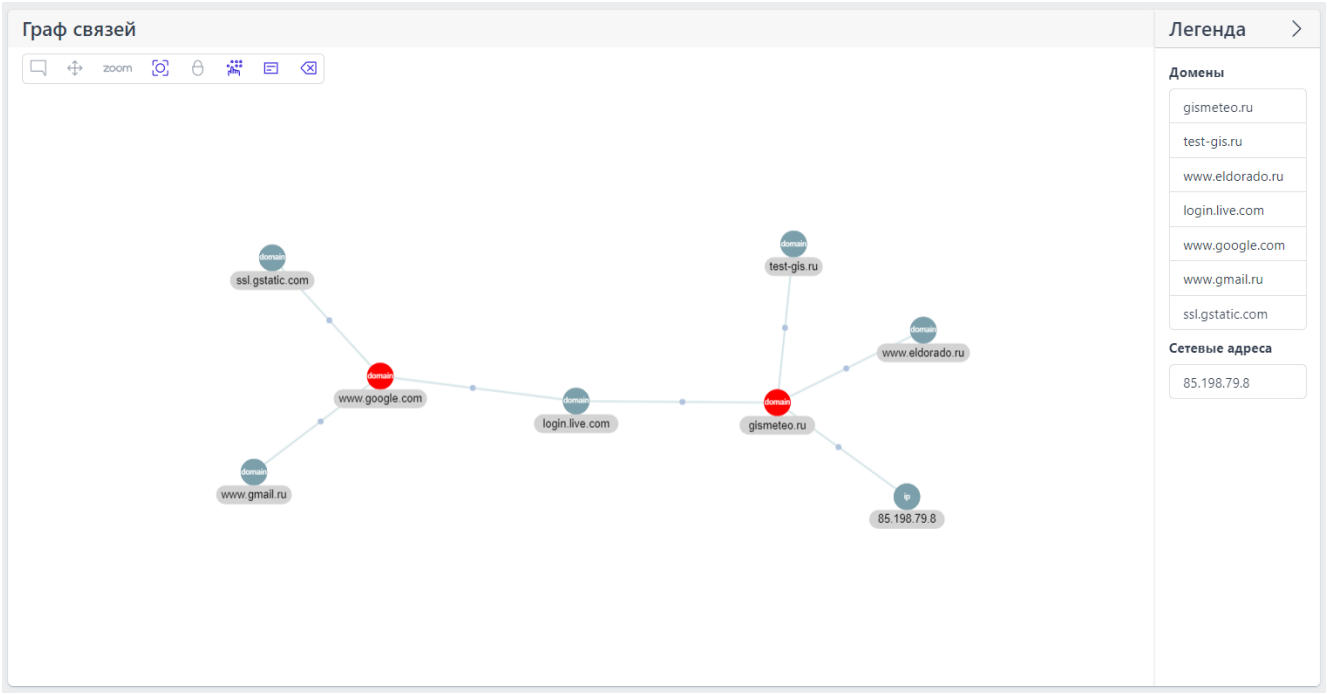


Рисунок 71 – Отображения графа связей для артефакта типа домен, с привязанными артефактами

На данной странице графа в правой части имеется столбец **Легенда**, отображающий связанные с артефактом другие артефакты.

Для того, чтобы скрыть столбец с информацией по привязанным артефактам, следует нажать ЛКМ по иконке  .

При нажатии ЛКМ по круглой области отрисовки графа отображается информация об артефакте (смотри рисунок 72).

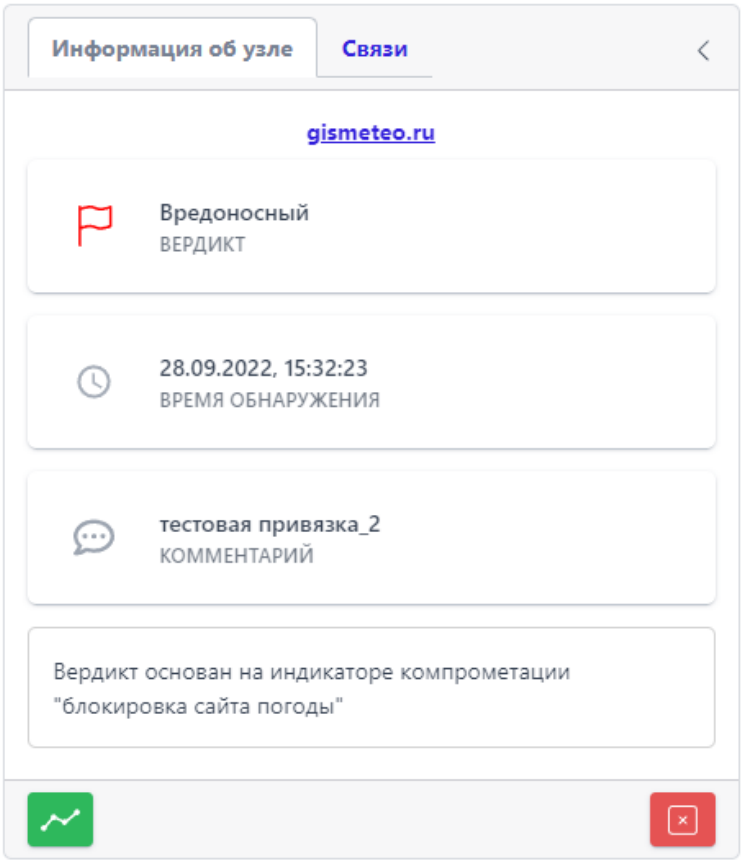


Рисунок 72 – Информация по артефакту

При нажатии по активной области **Связи** появится окно, показывающее список связей данного артефакта (рисунок 73).

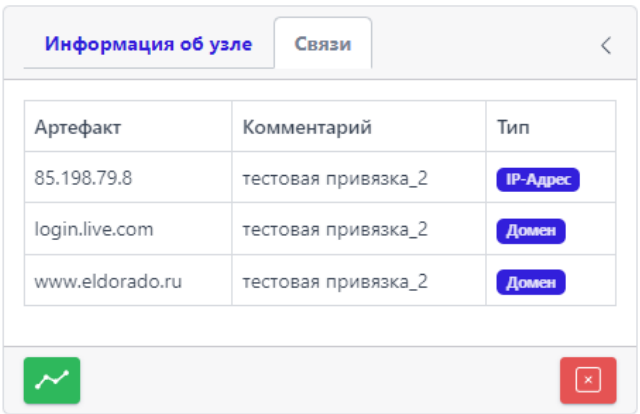


Рисунок 73 – Связи по данному артефакту

При нажатии по иконке, идентифицирующей артефакт, происходит переход на страницу отчета по данному артефакту.

Для привязки нового артефакта к выбранному артефакту следует нажать по иконке  , после чего появляется окно для внесения информации по привязанному артефакту, представленное на рисунке 74.

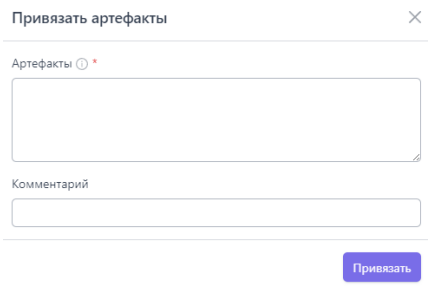


Рисунок 74 – Окно добавления информации для привязывания артефакта

После добавления информации в данном окне следует нажать по иконке **Привязать.** Привязанный артефакт будет отображаться на странице **Граф связей.**

Для удаления связи между двумя артефактами из привязанных артефактов следует нажать по иконке  , после чего появится окно указания того, какую связь и для какого узла требуется удалить (рисунок 75).

Рисунок 75 – Удаление связей между артефактами

Для подтверждения удаления связи требуется нажать по иконке **Удалить.**

5.5.5. 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. 76) 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.**

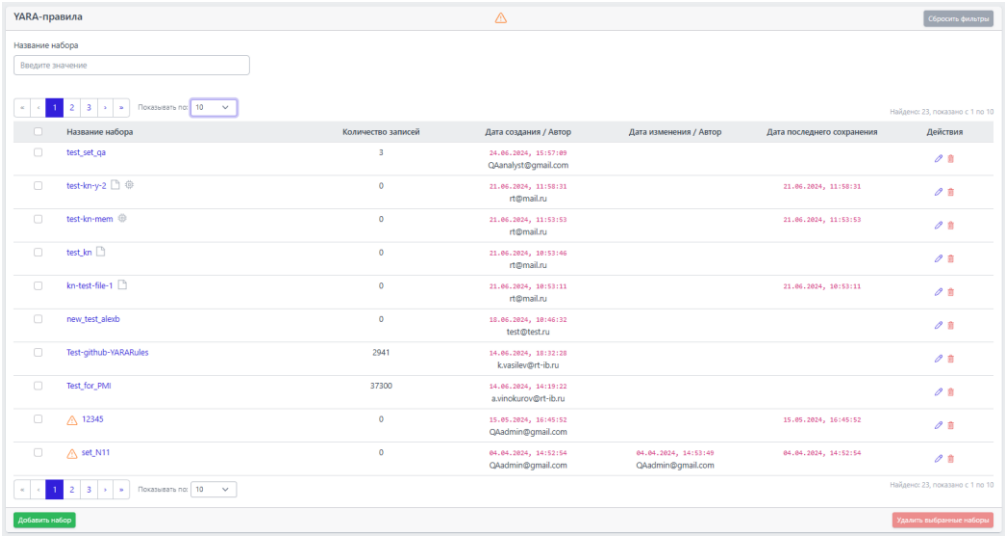


Рисунок 76 – Наборы Yara-правил

Наборы можно искать по названию с помощью фильтра **Название набора**.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Создать набор** (см. рисунок 77) 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.

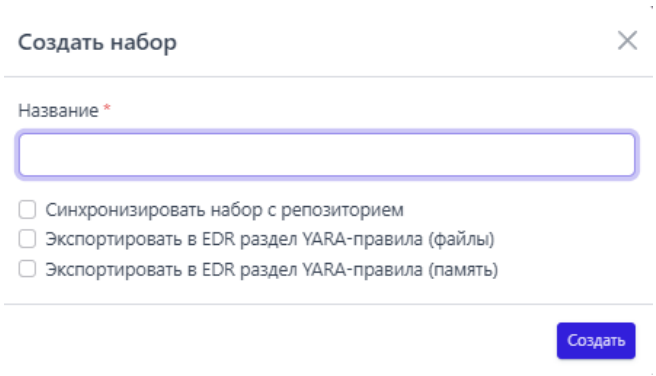


Рисунок 77 – Создать набор YARA-правил

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 ЛКМ на имени набора открывается страница **YARA-правила** для выбранного набора (рис. 78).

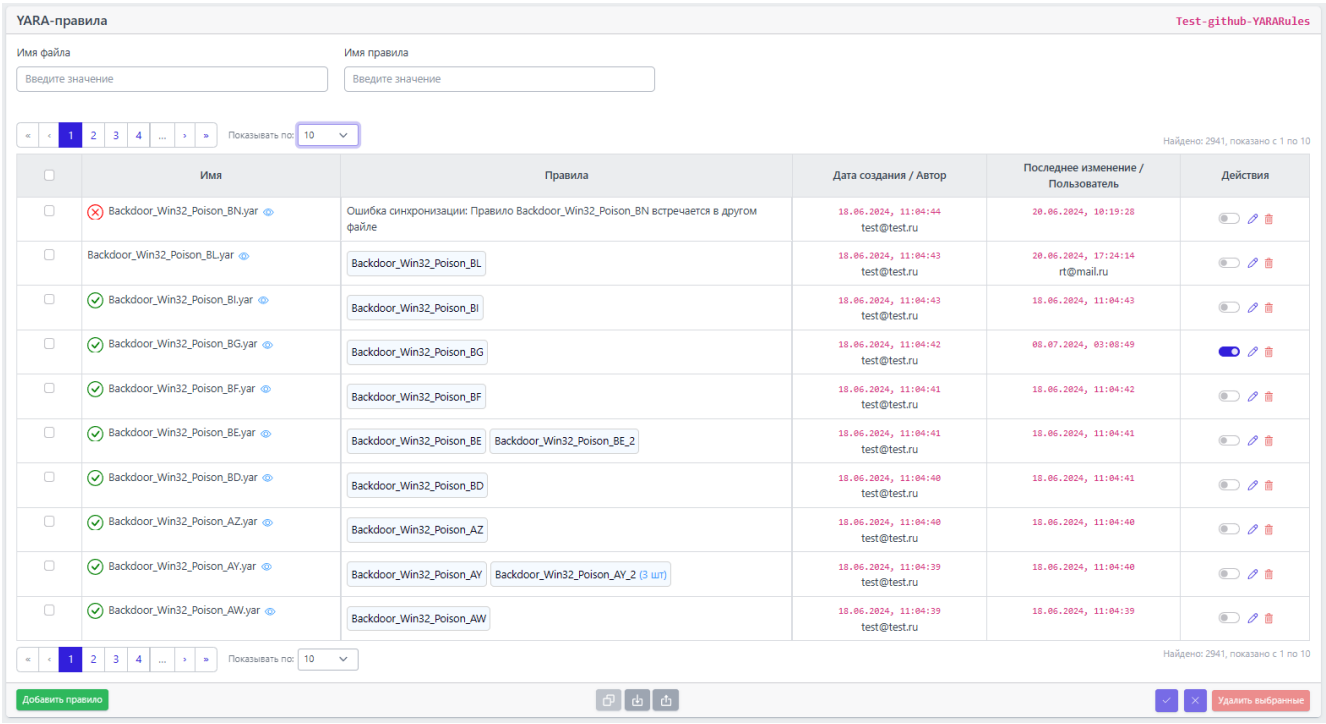


Рисунок 78 – YARA-правила

Страница «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:

– имя файла;

– имя правила.

Для добавления нового правила необходимо нажать кнопку **Добавить правило**, после чего откроется окно **Добавить правило** (рисунок 79), 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 80.

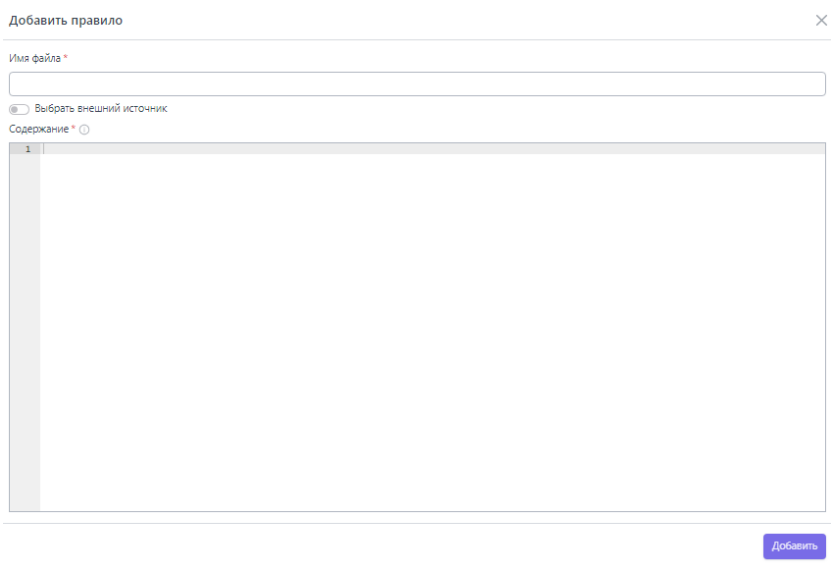


Рисунок 79 – Окно добавления правила

```
rule CobaltStrike__Resources_Artifact32_and_Resources_Dropper_v1_49_to_v3_14
{
meta:
        desc="Cobalt Strike's resources/artifact32{.exe,.dll,big.exe,big.dll} and resources/dropper.exe signature for versions 1.49 to 3.14"
        rs1 = "40fc605a8b95bbd79a3bd7d9af73fbeebe3fada577c99e7a111f6168f6a0d37a"
    author = "gssincla@google.com"


strings:
  // Decoder function for the embedded payload
    $payloadDecoder = { 8B [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

condition:
        any of them
}
```

Рисунок 80 – 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 81.

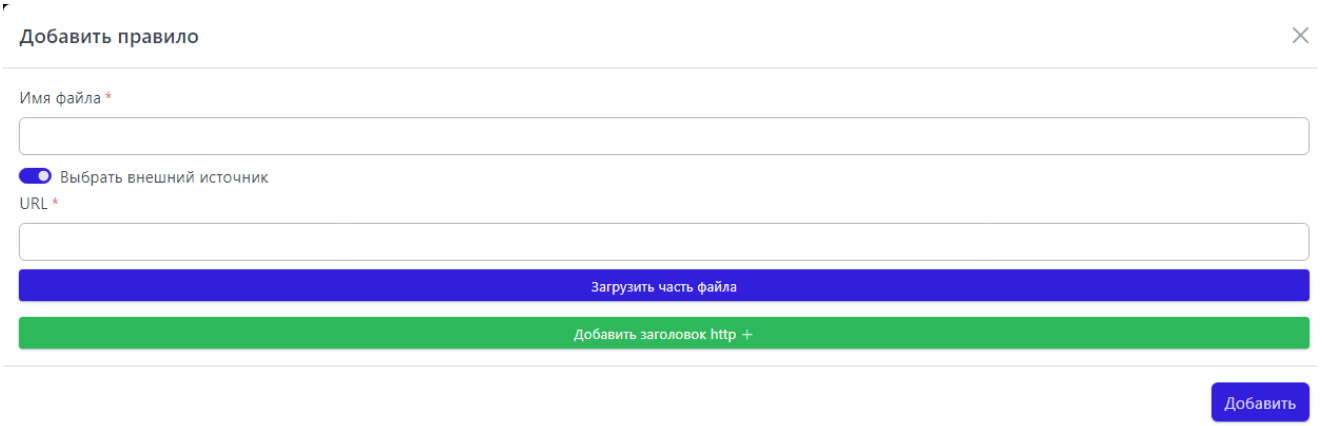


Рисунок 81 – Окно добавления правила из внешнего источника

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.

5.5.6. Распространяемая аналитика

Общие сведения

Распространяемая аналитика позволяет определить артефакты, в автоматическом режиме распространяемые на всех клиентов, взаимодействующих с TI, если они поддерживают соответствующий формат данных. Аналитика основана на концепции «теневых наборов». Подробнее о «теневых наборах» смотри в пункте 5.5.8.

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 82.

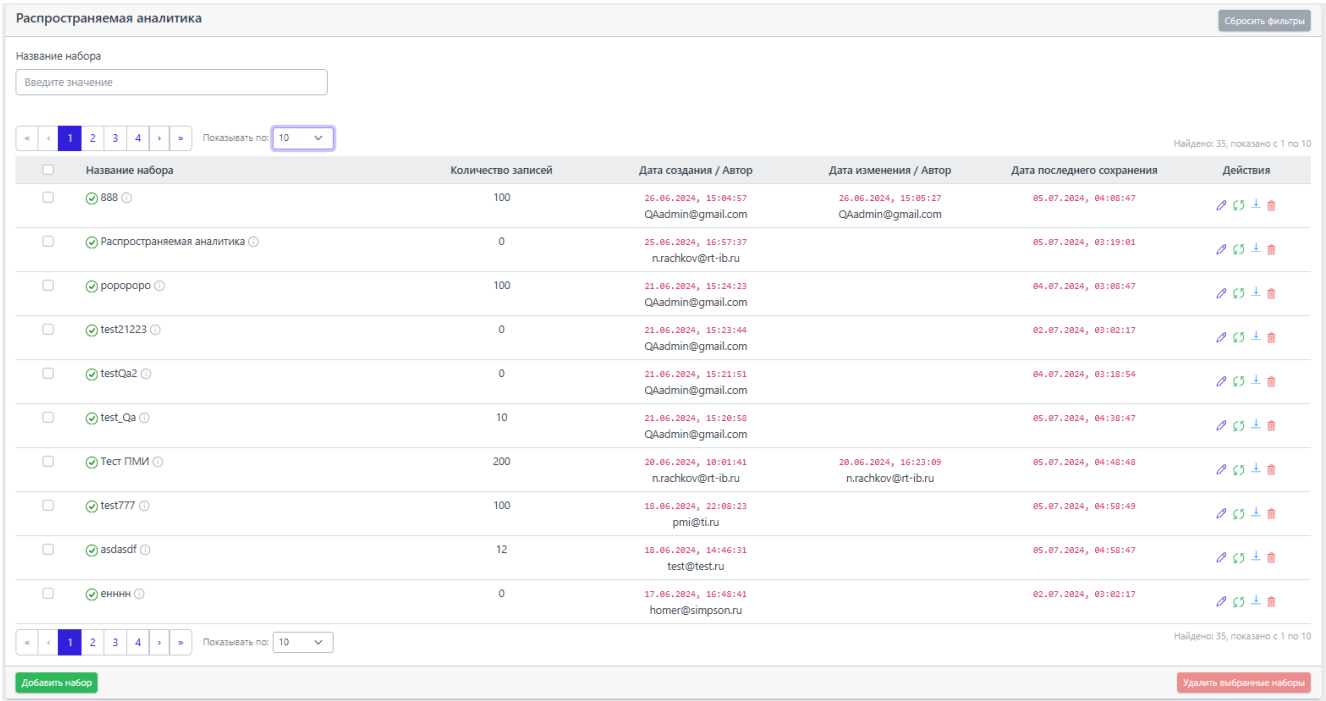


Рисунок 82 – Страница раздела «Распространяемая аналитика»

Страница представлена в виде таблицы с наборами аналитических данных.

В таблице имеются следующие поля:

– название набора;

– количество записей;

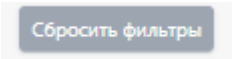
– дата создания/автор;

– дата последнего изменения/автор;

– дата последнего сохранения;

– действия.

Для фильтрации информации в таблице имеется фильтр **Название набора**.

В верхней часть страницы имеется иконка 

, чтобы отменять примененные для фильтрации настройки.

Для навигации на странице имеется стандартный элемент пагинатор.

Действия, возможные над наборами:

–  (редактирование набора);

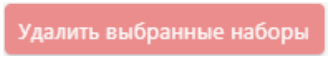
–  (принудительная синхронизация);

–  (скачивание набора);

–  (удаление набора);

– 

(добавление нового набора);

– 

(удалить выбранные наборы).

При нажатии по иконке 

появится окно, представленное на рисунке 83.

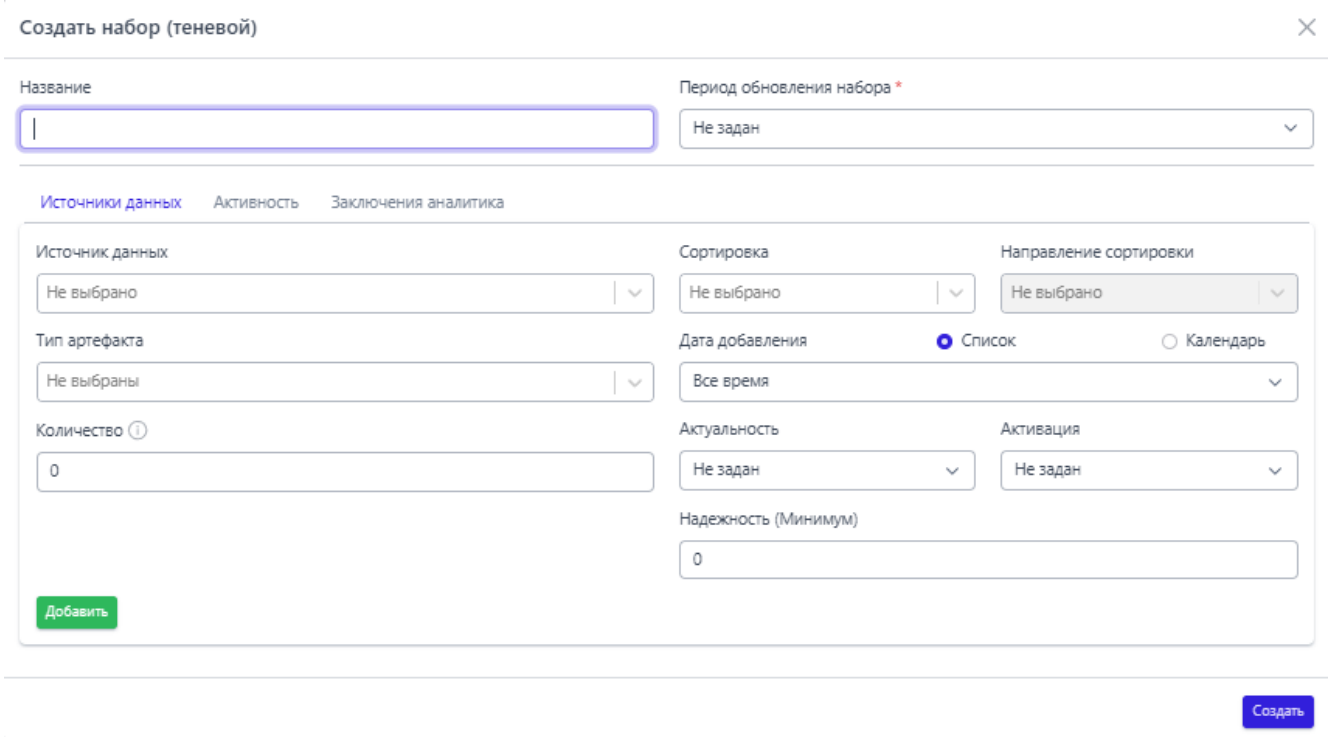


Рисунок 83 – Окно создания набора

В данном окне для создания набора требуется ввести в соответствующих полях 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 84.

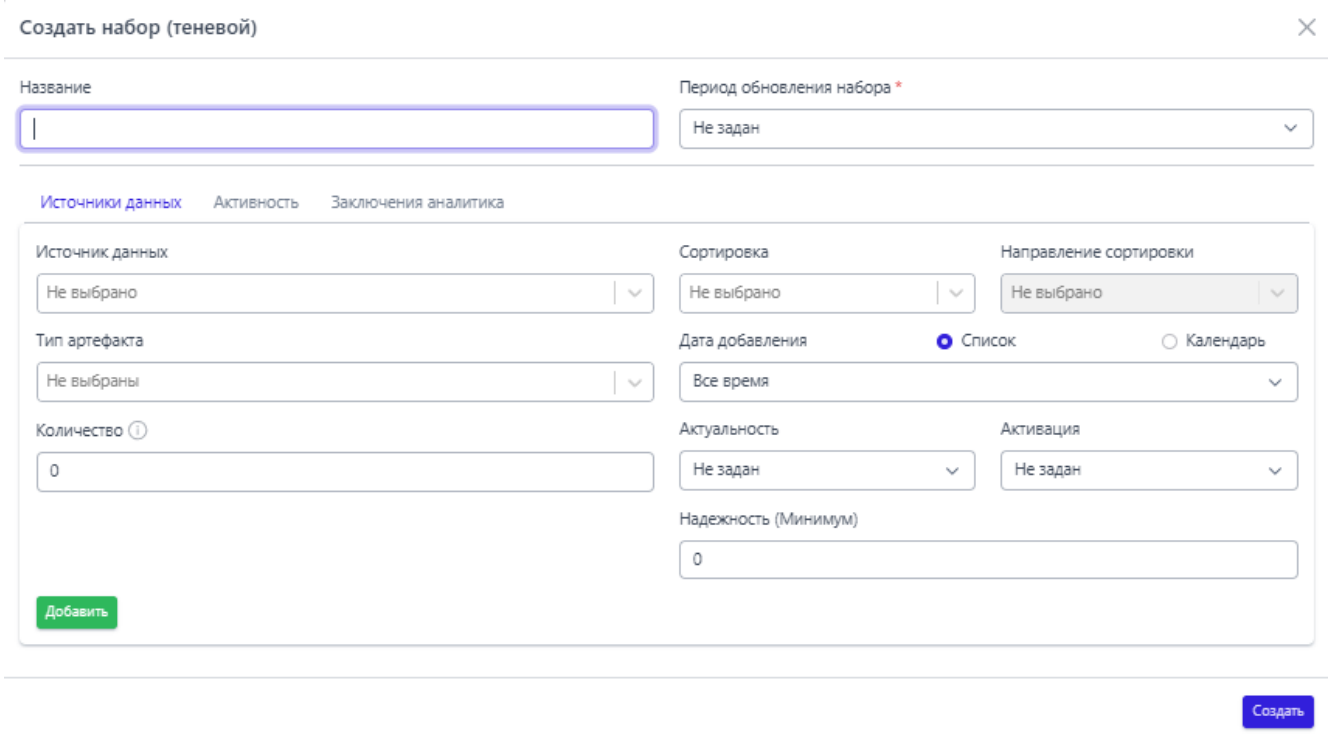


Рисунок 84 – Настройка полей выбранной вкладки «Источники данных»

По данной вкладке можно настроить следующие параметры:

– Количество (количество получаемых элементов для каждого выбранного типа артефакта);

– 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);

– Надежность (задается минимальное значение надежности для артефактов по источнику).

После выставления настроек, требуется нажать по иконке Добавить, после чего появится поле с зафиксированными настройками конфигурации источника данных (рисунок 85).

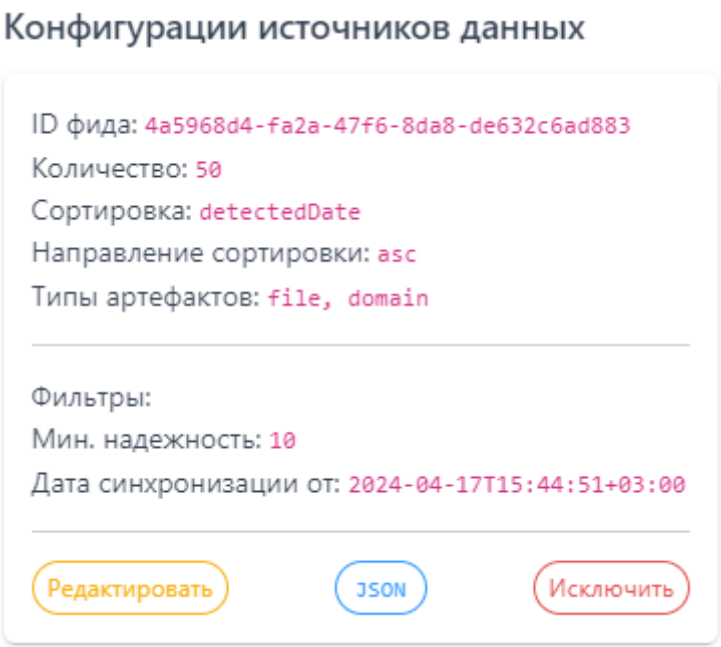


Рисунок 85 – Настройки конфигурации источника данных

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

При нажатии по иконке Редактировать имеется возможность редактирования настроенной конфигурации.

При нажатии по иконке JSON / HTML имеется возможность просмотра настроенной конфигурации в соответствующем формате.

При нажатии по иконке Исключить происходит удаление настроек параметров в конфигурации.

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

Поля настройки по выбранной вкладке **Активность** представлены на рисунке 86.

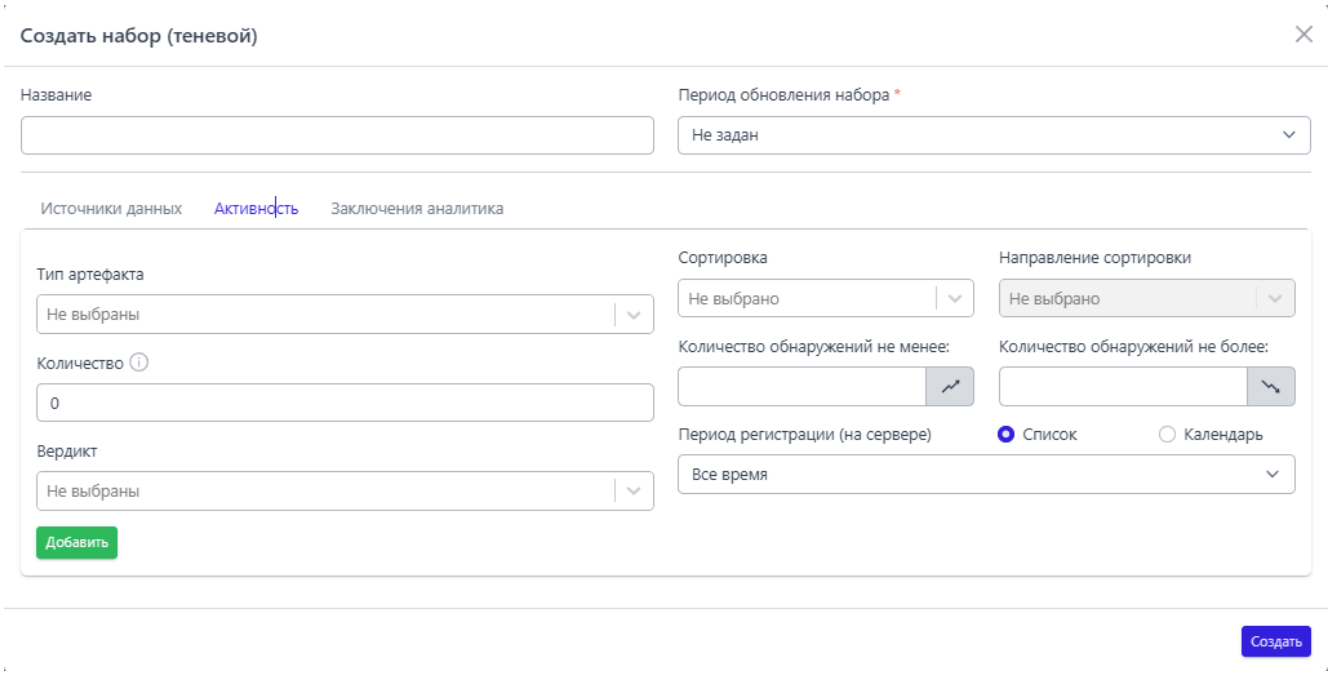


Рисунок 86 – Настройка полей выбранной вкладки «Активность»

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 менее;

– Период регистрации (на сервере) (начальная и конечная даты).

Поля настройки по выбранной вкладке **Заключения аналитика** представлены на рисунке 87.

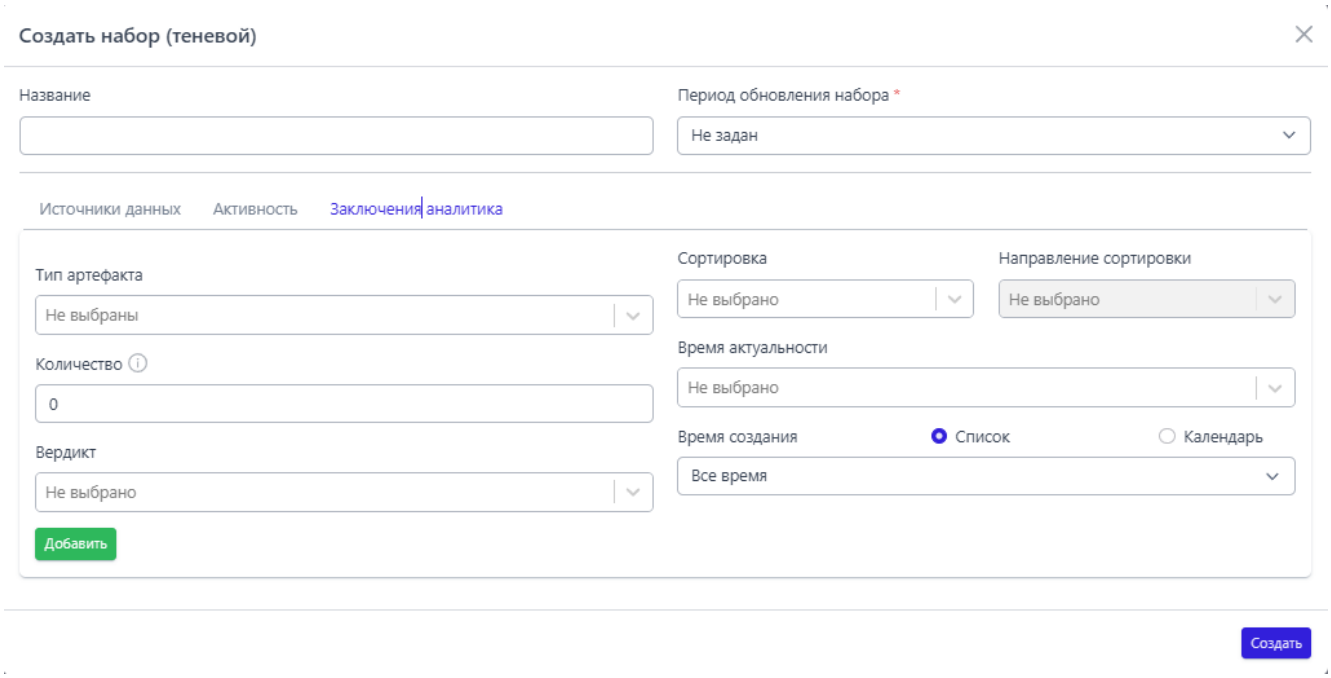


Рисунок 87 – Настройка полей выбранной вкладки «Заключение аналитика»

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

– Количество (количество записей артефактов по выбранному набору, отображающихся на странице Заключение эксперта);

– 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).

5.5.7. Алгоритм вынесения вердикта в TI

При вынесении вердикта TI действует пошагово. Если на текущем шаге имеется информация для вынесения вердикта, то вердикт выносится и следующие шаги не выполняются.

Алгоритм для типа артефакта - Файлы

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется наличие индикатора компрометации. Если он есть, и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

3) Проверяется наличие артефакта в источниках данных. Анализируются только актуальные записи (в которых время жизни артефакта больше, чем время с последней синхронизации). Из всех источников выбирается источник с самым большим приоритетом. Если таких источников несколько, приоритет отдается безопасному источнику. Выносится тот вердикт, который указан в настройках выбранного источника данных.

4) Проверяется наличие для файла отчета по собственному YARA-движку. Если в отчете имеется хотя бы одно сработавшее правило, то выносится вердикт «Вредоносный».

5) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, PT Sandbox, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

6) Проверяется наличие для файла отчета PT Sandbox (PT Multiscanner). Вердикт выносится на основании поля verdict отчета.

7) Проверяется наличие для файла отчета Virus Total. Вердикт выносится на основании вердиктов доверенных вендоров в отчете Virus Total. Если хотя бы

два доверенных вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе вердикт «Безопасный».

Список доверенных вендоров («TrustedFileVendors»):

– CrowdStrike;

– FireEye;

– McAfee;

– TrendMicro;

– Kaspersky;

– Microsoft;

– Sophos;

– Symantec;

– BitDefender;

– Malwarebytes;

– SentinelOne;

– Paloalto.

8) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

9) Если ни на одном предыдущем шаге не удалось вынести вердикт, то вердикт определяется как «Неизвестный».

Нужно отметить, что на текущий момент на вердикт не влияют отчеты остальных анализаторов: Athena, RST Cloud.

Алгоритм для типа артефакта - IP-адреса

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется, что IP находится в приватном диапазоне. Если это так, то выносится вердикт «Безопасный».

3) Проверяется наличие индикатора компрометации. Если он есть и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

4) Проверяется наличие артефакта в источниках данных. Подробнее см пункт 3 в разделе «Файлы».

5) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

6) Проверяется наличие для файла отчета Virus Total. Если хотя бы два любых вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе вердикт определяется как «Безопасный».

7) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

8) Если ни на одном предыдущем шаге не удалось определить вердикт, то выносится вердикт «Неизвестный».

Алгоритм для типа артефакта - Доменные имена

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется наличие индикатора компрометации. Если он есть и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

3) Проверяется наличие артефакта в источниках данных. Подробнее см. пункт 3 в разделе «Файлы».

4) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

5) Проверяется наличие для файла отчета Virus Total. Если хотя бы два любых вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе вердикт определяется как «Безопасный».

6) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

7) Если ни на одном предыдущем шаге не удалось определить вердикт, то выносится вердикт «Неизвестный».

Алгоритм для типа артефакта - URL

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется наличие индикатора компрометации. Если он есть и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

3) Проверяется наличие артефакта в источниках данных. Подробнее см пункт 3 в разделе «Файлы».

4) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

5) Проверяется наличие для файла отчета Virus Total. Если хотя бы два любых вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе присваивается вердикт «Безопасный».

6) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

7) Если ни на одном предыдущем шаге не удалось вынести вердикт, то присваивается вердикт «Неизвестный».

5.5.8. Теневые наборы

В разделах **Распространяемая аналитика**, **Индикаторы компрометации**, **Исключения для файлов** и **Сетевые исключения** присутствуют наборы с артефактами, которые обозначаются как «теневые». Теневые наборы являются основой распространяемой TI-аналитики, но для работы с EDR выделены

отдельные теневые наборы, формат данных которых совпадает с форматом данных EDR.

Теневые наборы – это наборы артефактов, автоматически переопределяемые на основе указанных аналитиком или администратором параметров. Эти параметры задаются администратором или аналитиком при формировании теневого набора.

Теневые наборы формируются на основе трех конфигураций с параметрами:

1) Источники данных (конфигурация набора на основе одного или несколько источников из таблицы артефактов «Источники данных» со своими определенными настройками, в соответствии с которыми артефакты будут отбираться в набор);

2) Активность (конфигурация набора на основе артефактов таблицы «Активность» со своими определенными настройками, в соответствии с которыми артефакты будут отбираться в набор);

3) Заключение аналитика (конфигурация набора на основе артефактов таблицы **Заключение аналитика** со своими определенными настройками, в соответствии с которыми артефакты будут отбираться в набор).

В результате конфигурирования появляется набор, который позволяет в автоматическом режиме отслеживать изменения в таблицах артефактов в соответствии с выбранными параметрами и применять эти изменения для аналитики, распространяемой на EDR, или общей распространяемой аналитики для любых клиентов TI-платформы.

В качестве примера можно рассмотреть такой «теневой набор» (см. рисунок 88).

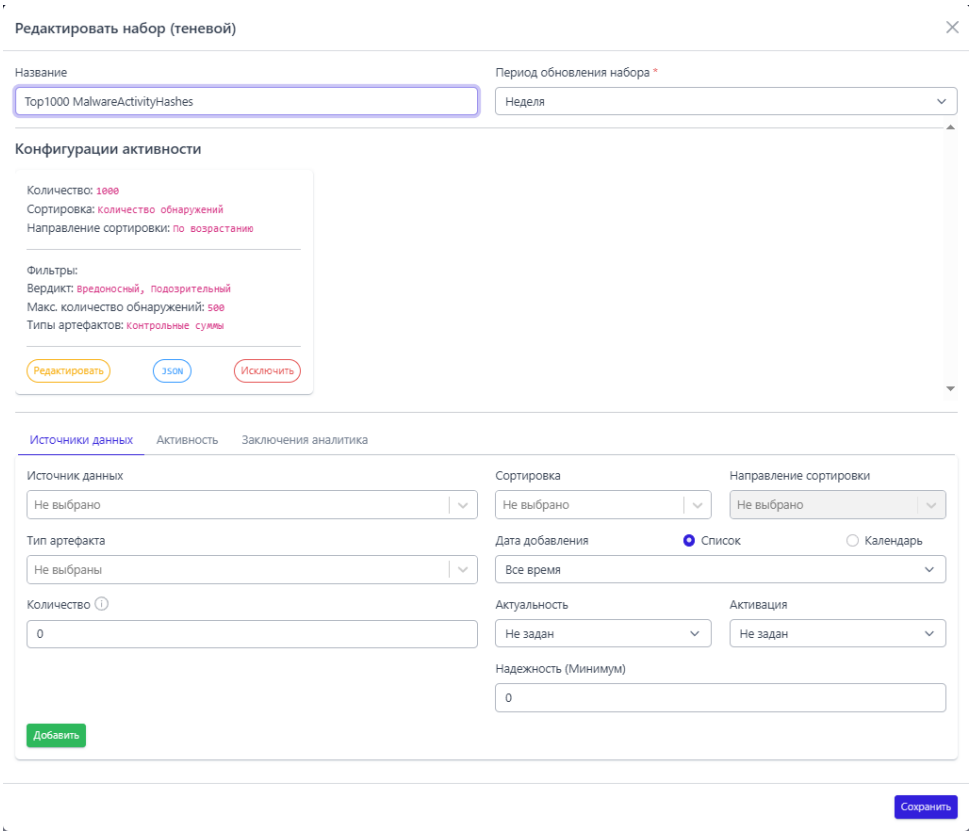


Рисунок 88 – Пример теневого набора

Здесь можно увидеть, что в качестве вредоносных и подозрительных артефактов типа «Файл» в набор будут попадать 1000 файловых артефактов таблицы **Активность,** встречавшиеся менее 500 раз за последнюю неделю в этой таблице. Файлы будут сортироваться по количеству обнаружений от малого числа к большему.

При обнаружении артефакта из списка такого теневого набора на клиенте (EDR, SIEM и т.д.) будет предпринято запрограммированное на клиенте же действие, соответствующее вердикту.

В теневых наборах можно смешивать конфигурации в любых сочетаниях. Подробнее о конфигурациях и параметрах настройки см. пункт 5.5.6.

5.6 Аналитика EDR

5.6.1. 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 выполниться 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-правила 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» (rul) которого будет указано имя индикатора, а в полях «Критичность» (svrt), «Действие» (act) и «MITRE» (mitre) будут перенесены значения соответствующих полей индикатора (см. ниже). Полный перечень доступных типов ИА в системе RT Protect EDR представлен в пункте **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**.

Синтаксис и семантика условных выражений индикаторов атак

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

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 (**exclf**) и расшифровки для них представлены в таблице 7.

Таблица 7 – Флаги исполняемого файла процесса

Наименование флага	Расшифровка
PartialName	Неполное имя исполняемого модуля
TaskSheduler	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 Prefetchera Windows
ControlPanel	Панель управления Windows
ScriptEngine	Скриптовый движок
ImageWow64	Компонент имеет 32-х битную и 64-х битную версию
HostProcess	Хост-процесс
WhoAmI	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
Icacls	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
DotNetNativeImage	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 msiexec
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
DoSpoofParentId	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_flagso, 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
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	*

Имя	Тип поля	Тип ИА	Нативное имя
		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 LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	fprod
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	*

Имя	Тип поля	Тип ИА	Нативное имя
		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 ACCESS	name
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
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

Наименование поля	Расшифровка
Cpath	Полное имя процесса-инициатора операции
Prot	Уровень защиты процесса
Base	Базовый адрес образа
Isize	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
Imgf	Флаги образа
Ldf	Флаги операции загрузки образа
Tpath	Полное имя целевого процесса
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

Наименование поля	Расшифровка
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. 89) включает в себя следующие структурные элементы:

– Фильтры **Название набора** и **Показывать по;**

– таблица с наборами индикаторов атак;

– кнопка **Добавить набор;**

– кнопка **Удалить выбранные наборы;**

– кнопка **Сбросить фильтры.**

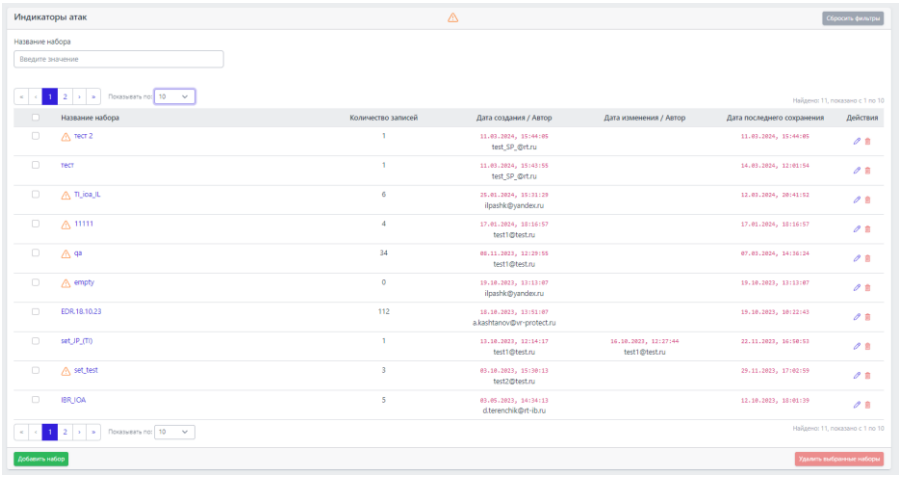


Рисунок 89 – Наборы индикаторов атак

В таблице с наборами индикаторов содержатся следующие поля:

– **Название набора**;

– **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**).

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. 90).

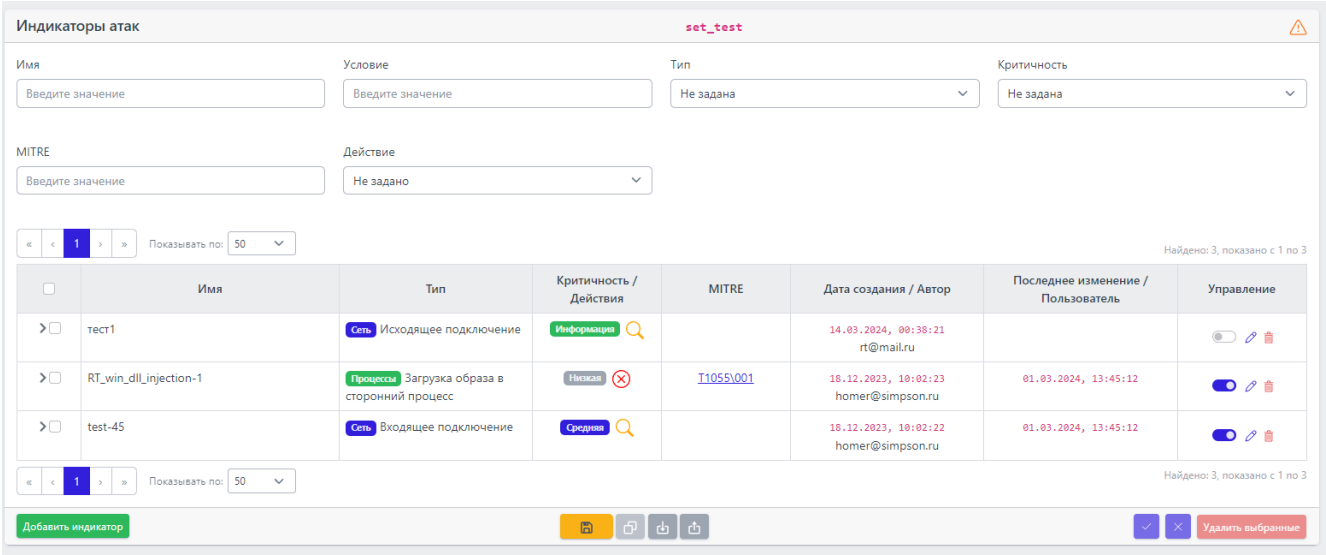


Рисунок 90 – Индикаторы атак

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. 91) следует прописать условия, на основании которых будет срабатывать правило.

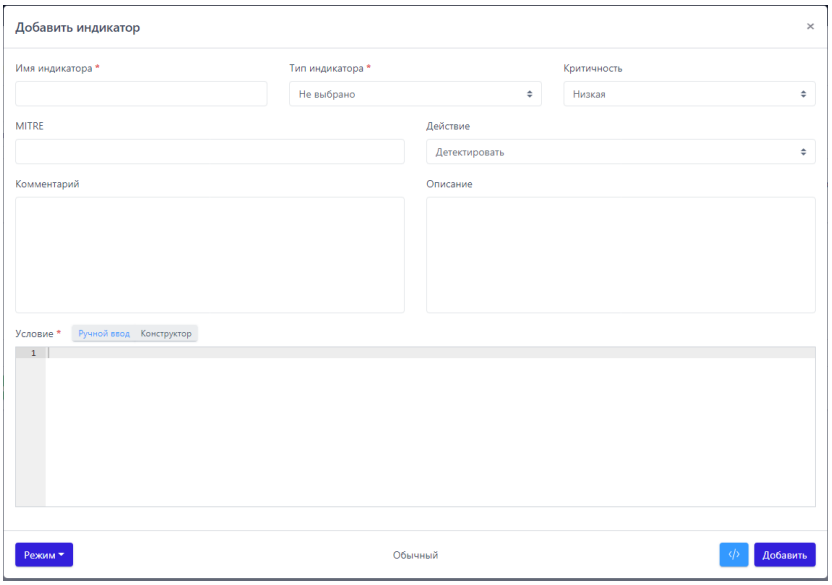


Рисунок 91 – Добавление индикатора

После написания условия необходимо нажать кнопку Добавить. В нижней части страницы появится сообщение о добавлении нового правила (рис. 92).

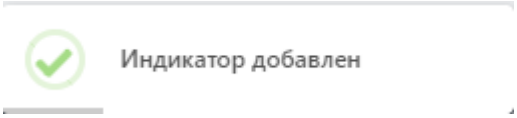


Рисунок 92 – Сообщение о добавлении индикатора атаки

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.93).

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

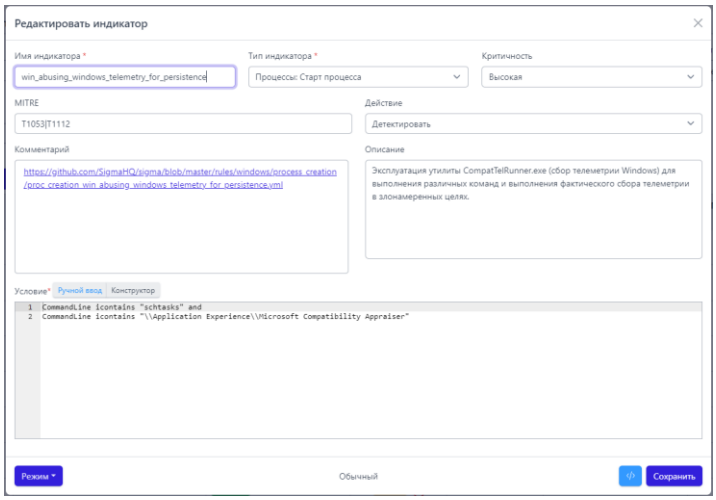


Рисунок 93 – Редактирование индикатора атаки

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении правила (рис. 94).

Рисунок 94 – 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**.

5.6.2. 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, хеш-сумма которого совпадает с хеш-суммой, указанной в индикаторе компрометации, обращение блокируется, а в модуле администрирования формируется (или дополняется) инцидент, объединяющий в себе все события, соответствующие индикатору. Эти события могут иметь разный тип в зависимости от выполняемой операции: открытие файла, чтение, удаление, а также могут относиться к разным процессам в системе. 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).

Страница **Индикаторы компрометации** представлена на рисунке 95. На странице отображаются наборы с индикаторами компрометации, сохраненные на сервере аналитики.

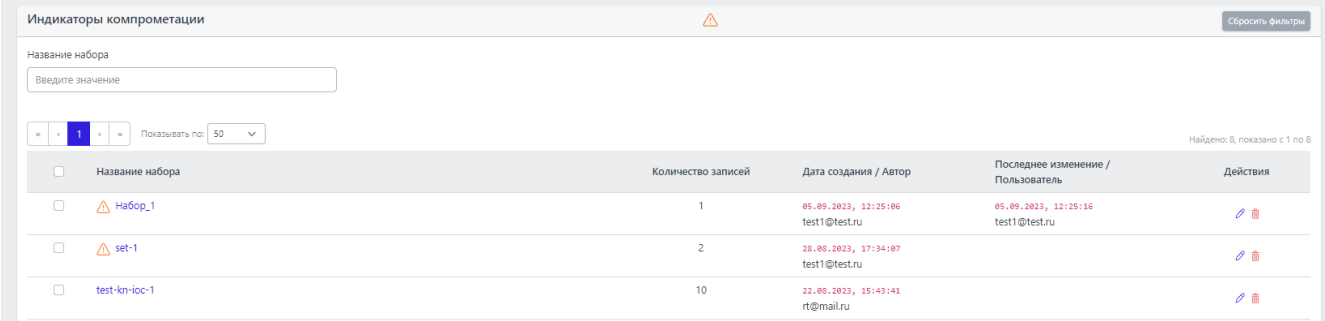


Рисунок 95 – Наборы индикаторов компрометации

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

1) Кнопка выбора (отмечена элементом ▢);

2) **Название набора;**

3) **Количество записей;**

4) **Дата создания/Автор** (показывает, когда и кто создал набор);

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

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

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. 96) в строке **Название** ввести название нового набора.

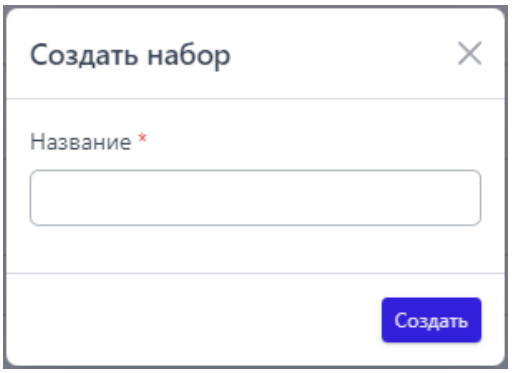


Рисунок 96 – Окно «Создать набор»

Для завершения операции добавления необходимо нажать кнопку **Создать**, после чего в нижней части страницы появится сообщение о добавлении набора (рис. 97), а строка с новым набором появится в таблице.

Рисунок 97 – 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;

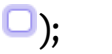
– импортировать данные из файла в набор индикаторов;

– 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**;

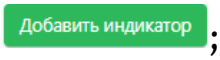
5) **Комментарий**;

6) **Дата создания/Автор**;

7) **Последнее изменение/Пользователь**;

8) **Действия** (в поле содержатся кнопки активации/деактивации индикатора, кнопки **Редактировать** и **Удалить**).

В нижней части таблицы индикаторов находятся кнопки операций с индикаторами:

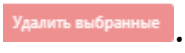
1) 

;

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 Добавить индикатор. Далее в открывшемся окне **Добавить индикатор** (рис. 98) следует заполнить поля, обязательными для заполнения из которых являются поля **Имя индикатора**, **Тип индикатора** и **Артефакт**, после чего нажать кнопку Добавить.

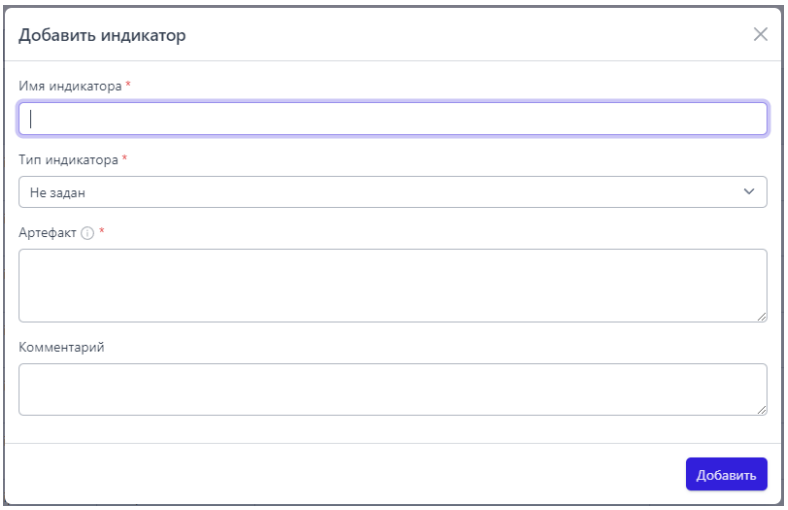


Рисунок 98 – Окно «Добавить индикатор»

В нижней части страницы появится сообщение о добавлении индикатора компрометации (рис. 99).

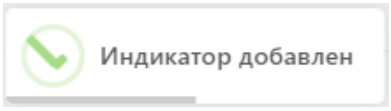


Рисунок 99 – Сообщение о добавлении индикатора

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.

5.6.3. Журналы Windows

Общая информация

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

Наборы с журналами Windows

Страница с наборами журналов Windows (рис. 100) открывается при выборе на панели слева раздела **Журналы Windows** и включает в себя следующие структурные элементы:

– кнопка **Сбросить фильтры**;

– фильтры **Название набора** и **Показывать по**;

– таблица с наборами журналов Windows;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**.

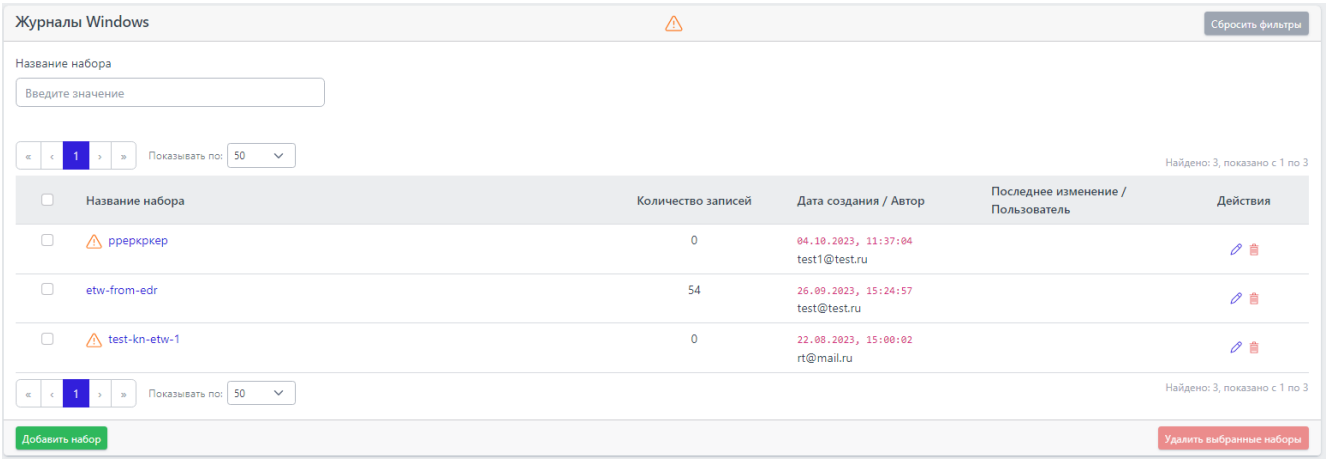


Рисунок 100 – Наборы с журналами Windows

Наборы можно искать по названию с помощью фильтра **Название набора.**

Для добавления нового набора необходимо нажать кнопку **Добавить набор,** после чего в окне **Создать набор** ввести название нового набора журналов Windows. 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 Windows** для выбранного набора (рис. 101).

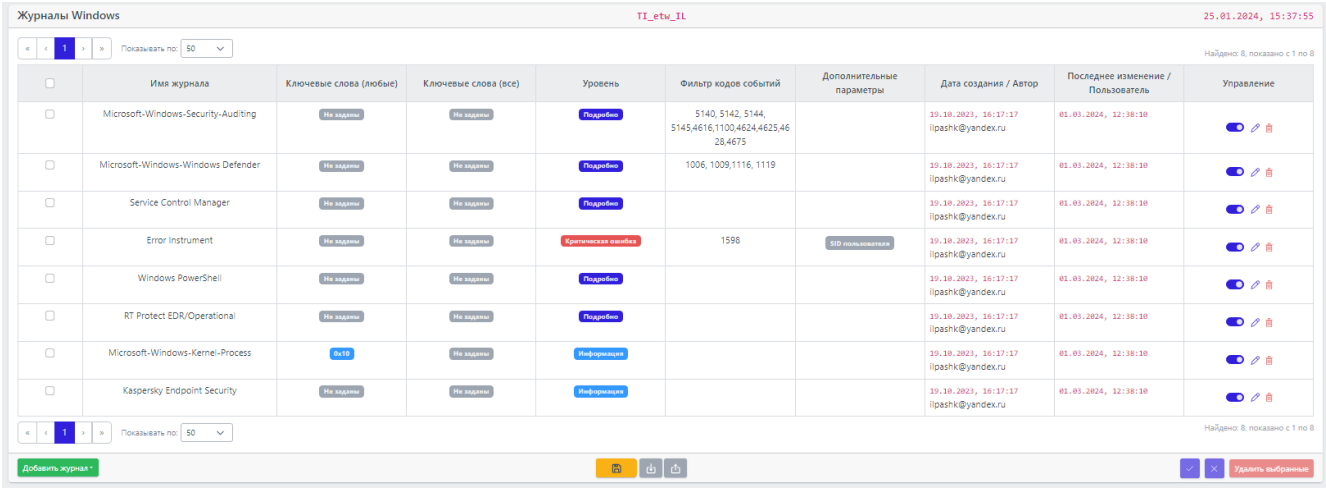


Рисунок 101 – Страница «Журналы Windows»

На странице **Журналы Windows** 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.

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**.

5.6.4. 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. 102) включает в себя следующие структурные элементы:

– таблица с наборами YARA-правил;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**.

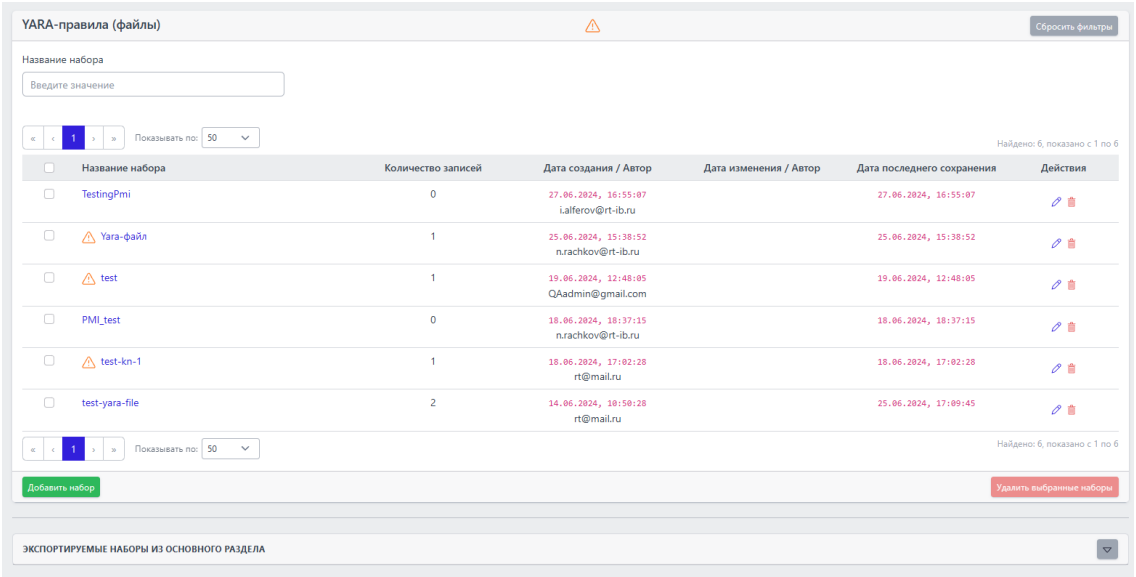


Рисунок 102 – Наборы YARA-правил (файлы)

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.**

Страница «YARA-правила (файлы)»

При нажатии ЛКМ по имени набора открывается страница **YARA-правила** для выбранного набора (рис. 103).

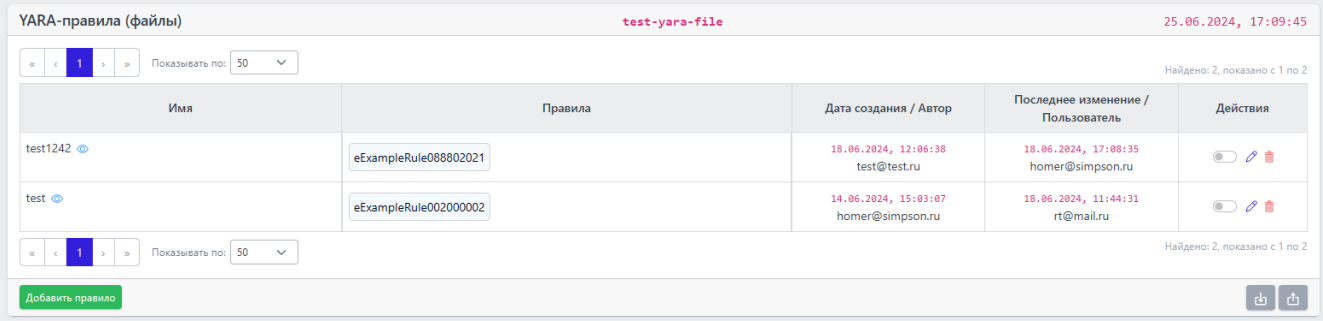


Рисунок 103 – YARA-правила

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 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 104.

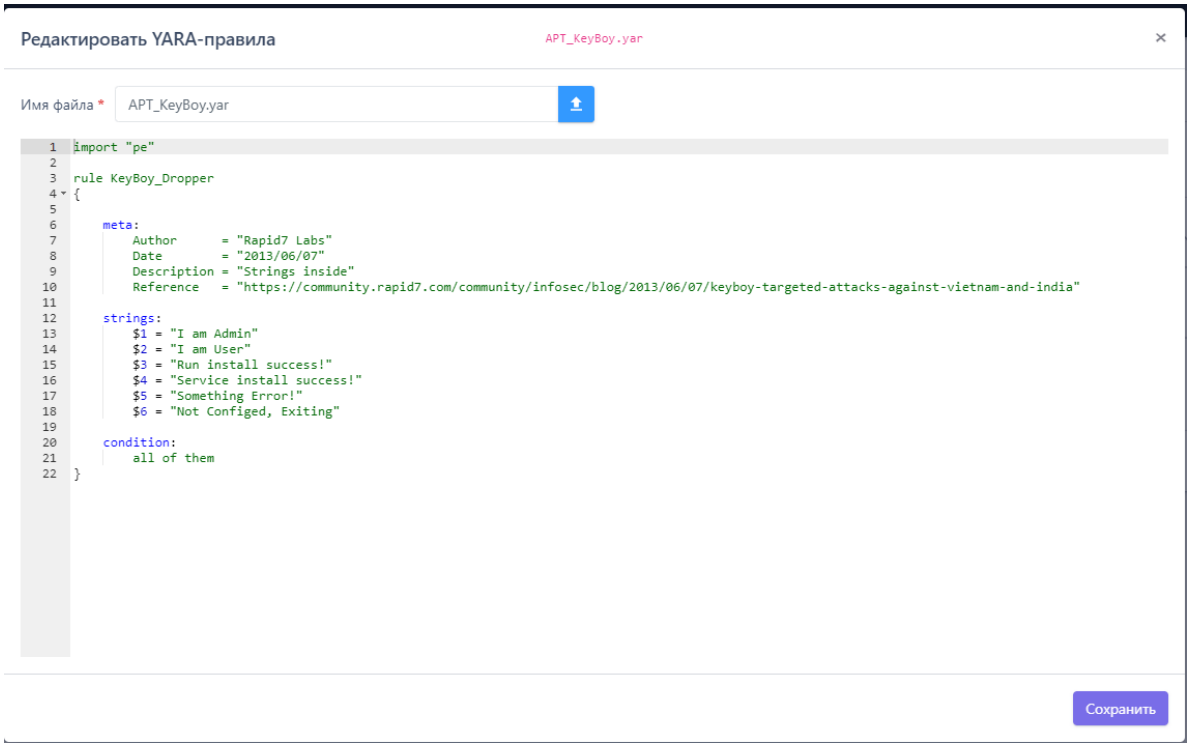


Рисунок 104 – Пример правила YARA

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.

5.6.5. 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 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 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.

5.7 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.

5.7.1. Исключения для программ

Общая информация

На странице с наборами исключений для программ (рис. 105) 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.

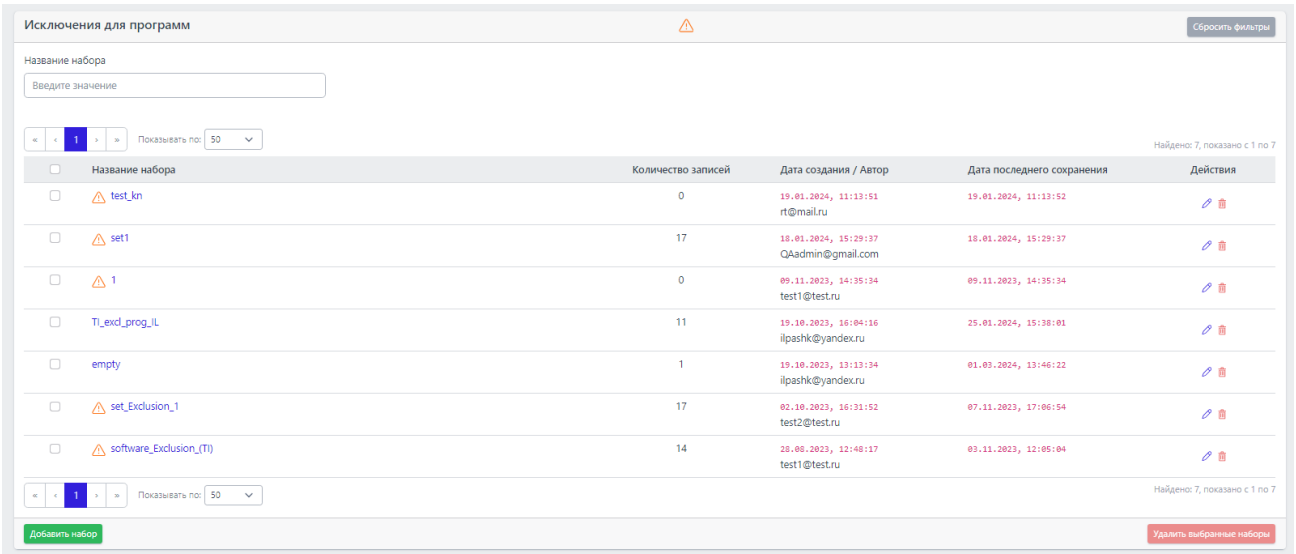


Рисунок 105 – Наборы исключений для программ

Наборы исключений для программ

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

– кнопка **Сбросить фильтры;**

– фильтры **Название набора** и **Показывать по**;

– таблица с наборами исключений для программ;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**.

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. 106) 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.

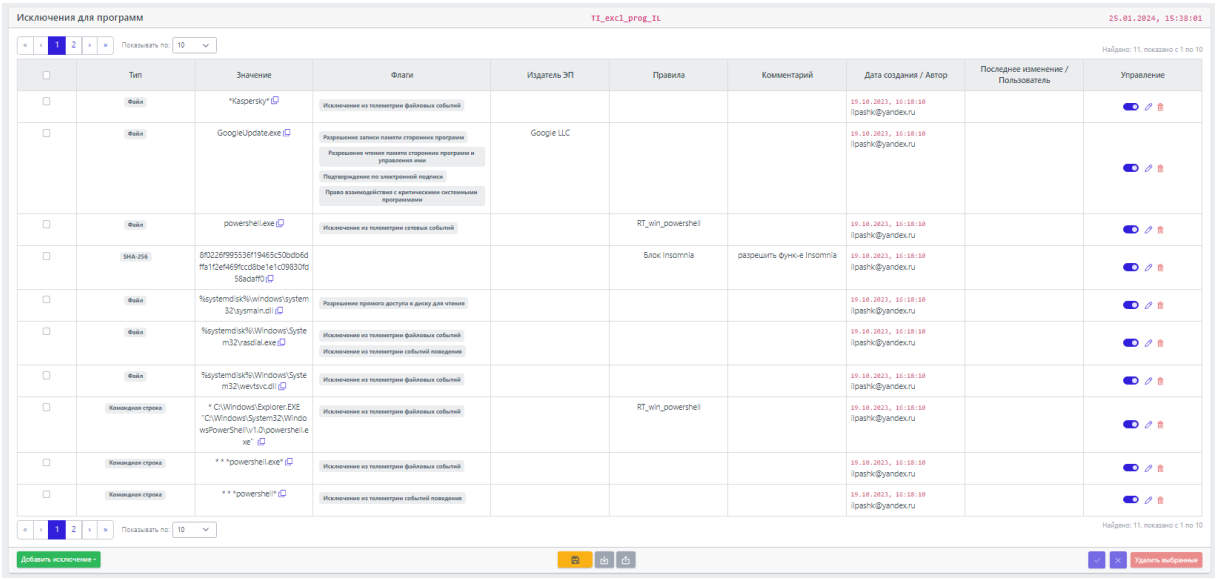


Рисунок 106 – Исключения для программ

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. 107).

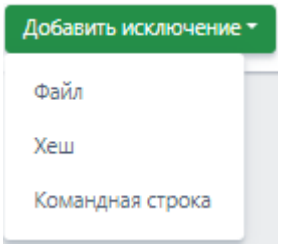


Рисунок 107 – Добавить исключение для программ (выбор типа)

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. 108).

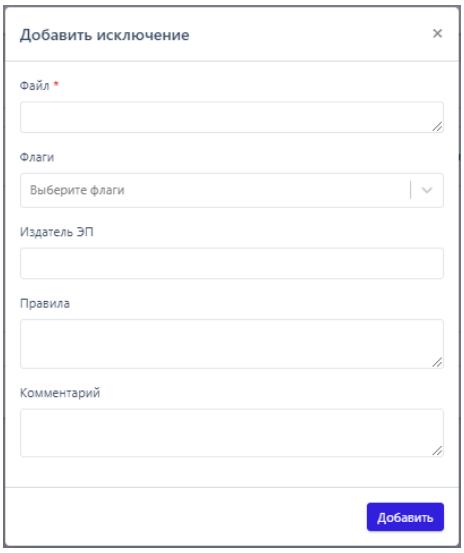


Рисунок 108 – Добавление исключения для программы (тип «Файл»)

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы, Хеш-сумма, Флаги, Издатель ЭП, Правила, Комментарий** (рис. 109).

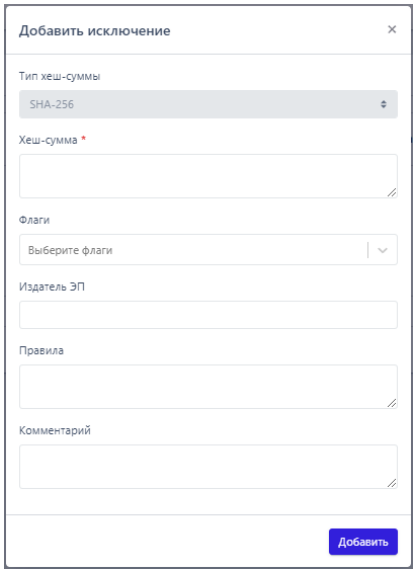


Рисунок 109 – Добавление исключения для программы (тип «Хеш»)

Для типа исключений **Командная строка** необходимо определить следующие параметры: **Командная строка прародителя, Командная строка родителя, Командная строка процесса, Флаги, Издатель ЭП, Правила, Комментарий** (рис. 110).

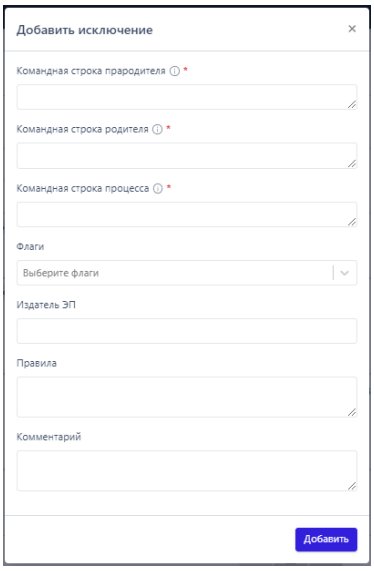


Рисунок 110 – Добавление исключения для программы (тип «Командная строка»)

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** ().

5.7.2. Исключения для файлов

Общая информация

На странице **Наборы исключений для файлов** (рис. 111) содержится список файлов, исполнение которых должно быть разрешено или блокировано (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.

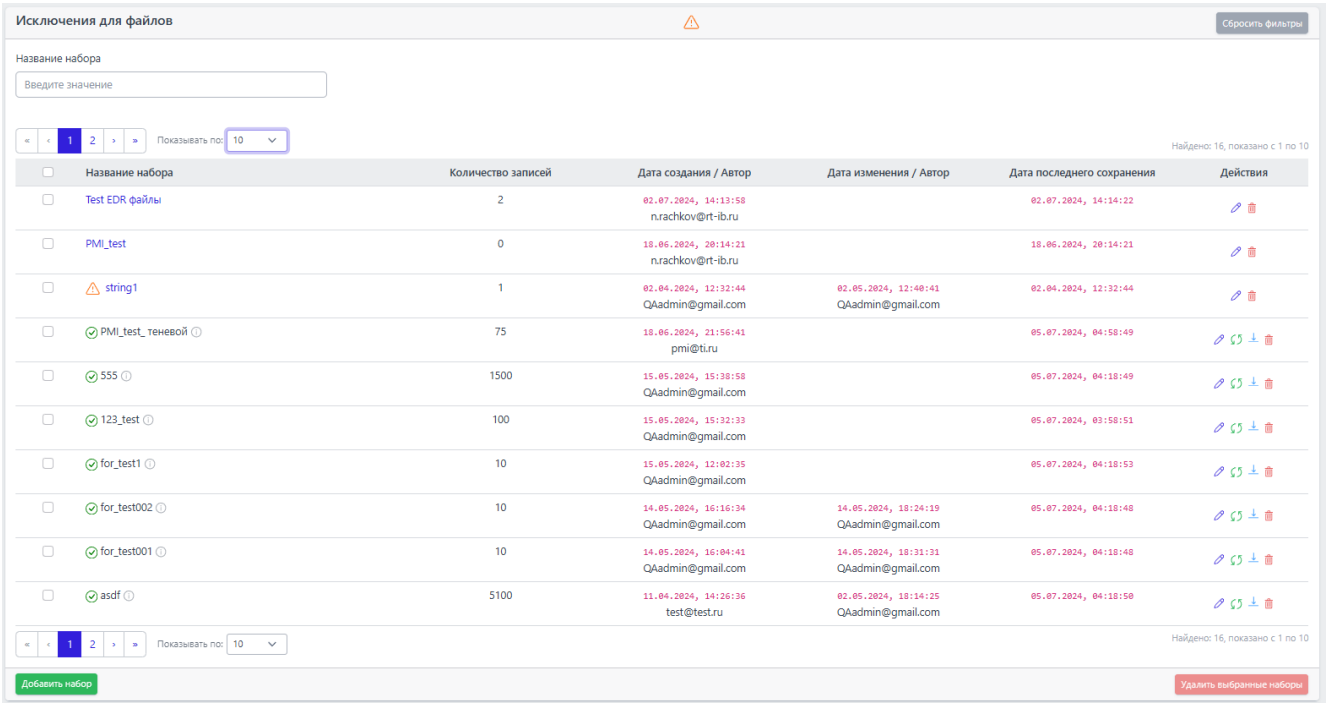


Рисунок 111 – Наборы исключений для файлов

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.**

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. 5.5.8. 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. 112) 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.

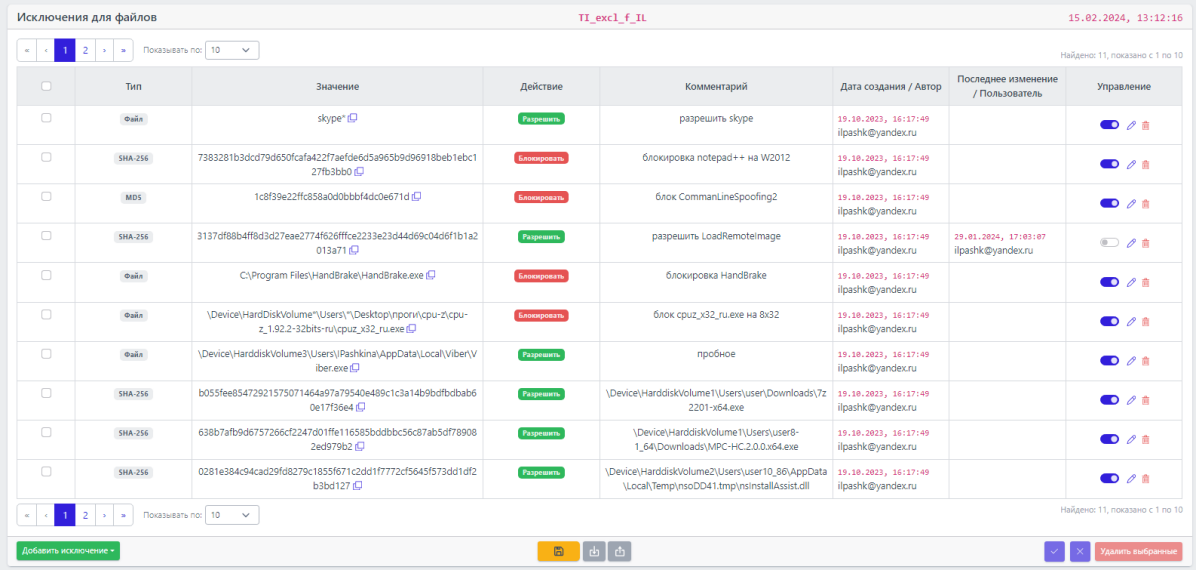


Рисунок 112 – Исключения для файлов

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. 113).

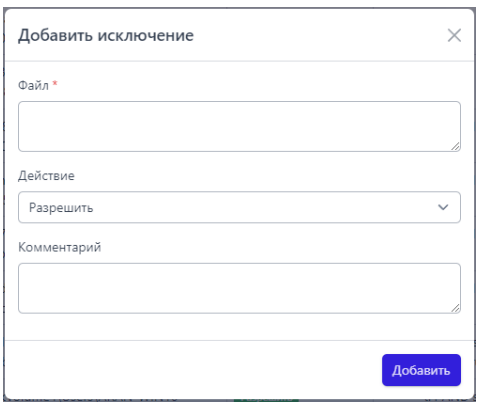


Рисунок 113 – Добавление исключения для файла (тип «Файл»)

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. 114).

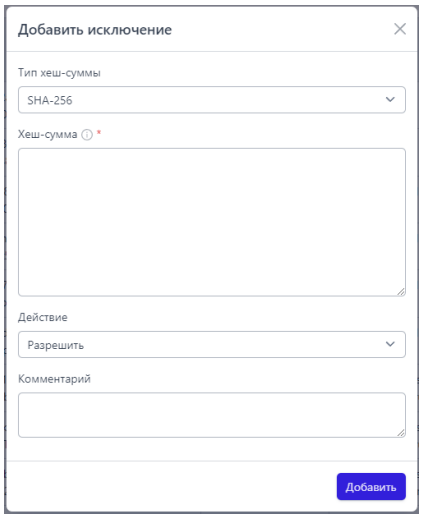


Рисунок 114 – Добавление исключения для файла (тип «Хеш»)

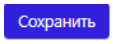
Файл – в поле прописываются имена исполняемых файлов, которые необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** в поле **Значение**, а в поле **Тип** будет указан тип исключения.

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 

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** ().

5.7.3. 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. 115):

– таблица с наборами сетевых исключений;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**.

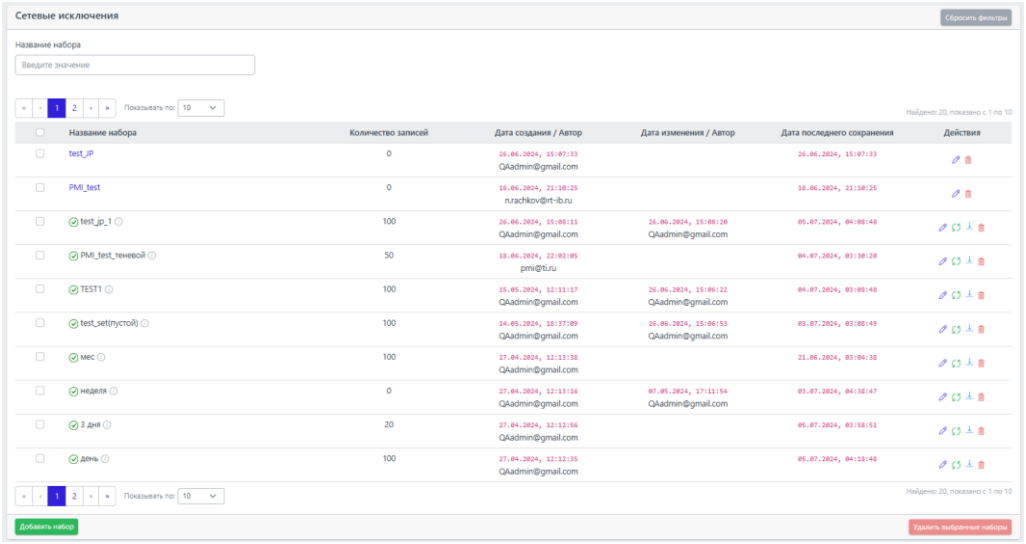


Рисунок 115 – Страница наборов сетевых исключений

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. 5.5.8 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. 116) 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.

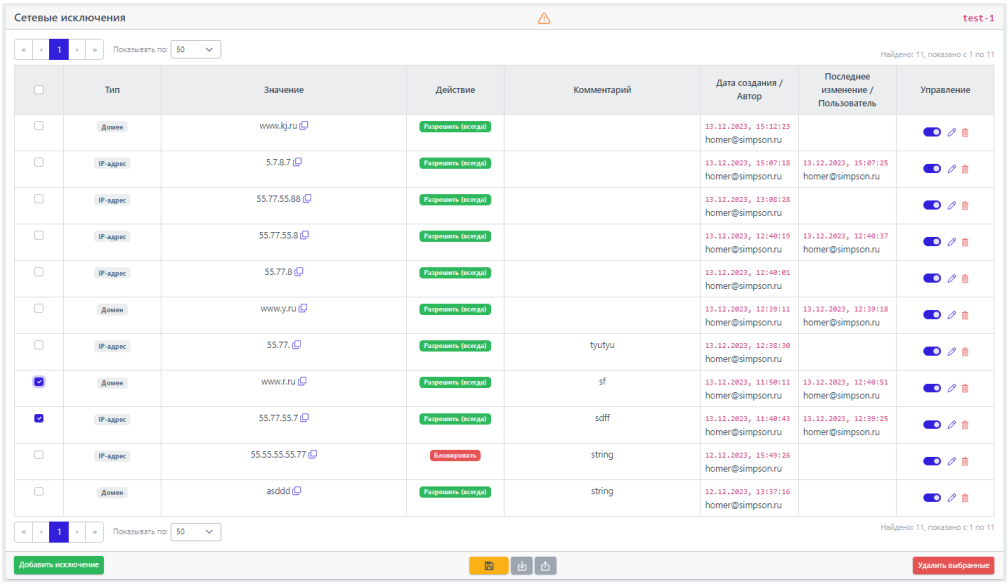


Рисунок 116 – Страница «Сетевые исключения»

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения.

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

5.7.4. 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. 117):

– таблица с наборами исключений для индикаторов атак;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

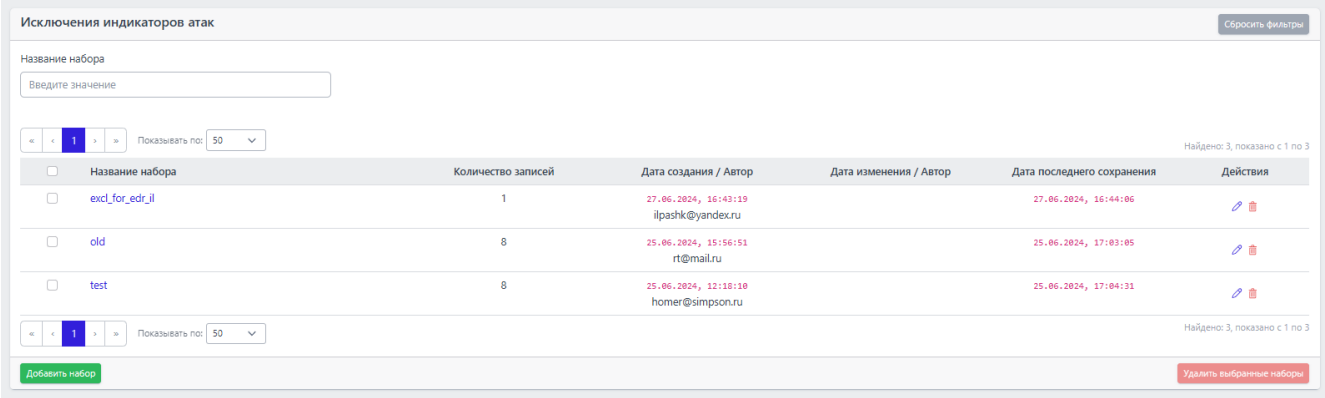


Рисунок 117 – Страница «Наборы исключений индикаторов атак»

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**.

Страница «Исключения индикаторов атак»

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 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 Добавить.

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключений индикаторов атак** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** (). Далее выбрать набор, в который будет копироваться выбранный элемент.

Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** (). Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** (). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

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

активацию/деактивацию с помощью кнопок **Активировать выбранные элементы**/**Деактивировать выбранные элементы** ()

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

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».