

RT Protect EDR

Руководство оператора поиска угроз

Версия 1.0.13 от 15 октября 2024

Разработано компанией АО «РТ-Информационная безопасность»



RT
Protect

1. Общие положения	4
1.1 Идентификация документа	4
1.2 Аннотация документа	4
1.3 Термины и определения.....	4
1.4 Условные обозначения	5
2. Общие сведения	7
2.1 Общие сведения о Программе	7
3. Описание принципов безопасной работы Программы.....	8
3.1 Общая информация	8
3.2 Компрометация паролей	9
4. Основные операции в Программе.....	10
4.1 Просмотр состояния защищаемой инфраструктуры	10
4.2 Работа с панелью управления	12
4.3 Работа с инцидентами	14
4.3.1. Страница «Инцидент»	17
4.4 Работа с деревом процессов	18
4.4.1. Вкладка «Информация»	20
4.4.2. Вкладка «Файлы»	22
4.4.3. Вкладка «Сеть».....	23
4.4.4. Вкладка «Реестр»	24
4.4.5. Вкладка «Процессы».....	25
4.4.6. Вкладка «Загруженные DLL/SO»	26
4.4.7. Вкладка «Точки автозапуска»	27
4.4.8. Вкладка «Распространенность»	28

4.4.9. Вкладка «Событие старта»	28
4.4.10. Вкладка «Правила/MITRE»	29
4.5 Проактивный поиск угроз.....	29
4.5.1. Просмотр графиков активности	40
4.5.2. Создание инцидента на странице «Активность».....	40
4.6 Проверка артефактов с помощью TI-платформы	41
4.7 Проверка распространенности программы в агентской сети.....	41
4.8 Действия с агентами	43
4.8.1. Сканирование уязвимостей на странице «Агент»	Ошибка! Закладка не определена.
4.9 Просмотр конфигураций	45
4.10 Просмотр графиков.....	45
4.11 Просмотр информации об уязвимостях.....	Ошибка! Закладка не определена.
4.11.1. Формирование отчетности на странице с уязвимостями	Ошибка! Закладка не определена.
4.11.2. Распространенность уязвимости в защищаемой инфраструктуре	Ошибка! Закладка не определена.
4.11.3. Изучение сведений об уязвимости.....	Ошибка! Закладка не определена.
4.12 Просмотр исключений	52
4.13 Просмотр профилей безопасности агента	54
4.14 Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения	56
5. Модель данных, обнаруживаемых агентом	57
5.1 Общие сведения	57
5.2 События монитора сети	67
5.3 События монитора файловых операций.....	68
5.4 События монитора реестра	71
5.5 События системного журнала Windows (ETW)	72
5.6 События монитора процессов	73

5.7 События монитора системы	75
5.8 События пользовательских сессий	78
5.9 События монитора вызовов.....	79
5.10 События модуля контроля USB	80
5.11 События статистики	81
5.12 События anti-ransomware-модуля	81
6. Перечень сокращений	83
7. Перечень терминов и определений	84
8. Заключение	88

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect EDR» Руководство оператора поиска угроз
Версия документа	Версия 1.0.13 (актуально для версии агента 2.0.173.2673, версии фронтенда 2.40.8, версии бекенда 1.21.1-23)
Идентификация программы	«RT Protect EDR»
Идентификация разработчика	АО «РТ-Информационная безопасность»
Уровень доверия	Оценочный уровень доверия 4 (ОУД4)
Идентификация ПЗ	Профиль защиты систем обнаружения вторжений уровня узла типа «У» четвертого класса защиты. ИТ.СОВ.У4.ПЗ. Утвержден ФСТЭК России от 3.02.2012г. Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты ИТ.СКН.П4.ПЗ (утвержден ФСТЭК России от 01.12.2014)
Идентификация ОК	«Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
Ключевые слова	Система обнаружения вторжений, СОВ, ОУД4

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей, осуществляющих функции оператора поиска угроз и взаимодействующих с программой «RT Protect EDR» (далее Программа) с целью обеспечения ИБ.

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 – Основные термины

Термин	Расшифровка
Администратор программы	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию программы.
Задание по безопасности	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретной программы.
Политика безопасности	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых программой.
Профиль защиты	Совокупность требований безопасности для программы.
Разработчик	АО «РТ-Информационная безопасность»
Угроза безопасности информации	Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.
Функции безопасности программы	Совокупность всех функций безопасности программы, направленных на осуществление политики безопасности (ПБ).
Инцидент информационной безопасности	Единовременное событие или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации бизнес-информации и угрозы информационной безопасности.
Событие информационной безопасности	Идентифицированный случай состояния системы, сервиса или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности.

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, названия кнопок меню модуля администрирования программы.
	Обозначения кнопок меню, операций модуля администрирования программы.
Times New Roman/Times New Roman	Перечисление альтернативных вариантов, путь меню, путь файла.
 Примечание	Информация, требующая внимания пользователя

Важно	Информация, связанная с важными конфигурационными настройками и особенностями работы EDR
---	---

2. Общие сведения

2.1 Общие сведения о Программе

RT Protect EDR – это программа, которая позволяет обнаруживать целенаправленные атаки (APT) и другую вредоносную активность на конечных точках (хостах) и реагировать на обнаружение соответствующим образом: изоляция хоста, отправка команды с помощью терминала, блокирование вредоносной активности и т.д.

Программа имеет клиент-серверную архитектуру.

Программа не содержит в своем составе заимствованных компонентов без исходного кода. Все компоненты собираются из исходного кода. Программа предназначена для обработки информации, не являющейся секретной.

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

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



Примечание

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

Клиент проводит мониторинг системной активности, чтобы выявлять вредоносное поведение согласно правилам, полученным от сервера поведенческого анализа. Клиент собирает статистику системной активности и периодически отправляет ее на сервер. Взаимодействие с сервером происходит по протоколу HTTPS.

3. Описание принципов безопасной работы Программы

3.1 Общая информация

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

- необходимо соблюдать парольную политику;
- пароль не должен включать в себя легко вычисляемые сочетания символов;
- личный пароль пользователь не имеет права сообщать никому;
- при вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами

и техническими средствами;

- пароль должен соответствовать требованиям, описанным в пункте 6.2.2 документа «Руководство администратора RT Protect EDR».



Важно

Если в течение 12 часов пользователь с ролью **Оператор поиска угроз** выполнит 20 или более неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор Программы.

При эксплуатации Программы запрещено:

- оставлять без контроля незаблокированные программные средства;
- разглашать пароли, выводить пароли на дисплей, принтер или иные средства отображения информации.

Эксплуатация Программы должна осуществляться пользователями, прошедшими проверку на благонадежность и компетентность. Пользователи Программы должны действовать согласно правилам и процедурам, установленным в настоящем руководстве и внутренних документах организаций, эксплуатирующих Программу.

3.2 Компрометация паролей

Под компрометацией паролей следует понимать следующее:

- физическую утерю носителя с парольной информацией;
- передачу идентификационной информации по открытым каналам связи;
- перехват пароля при распределении идентификаторов;
- сознательную передачу информации постороннему лицу.

При компрометации пароля пользователь обязан незамедлительно оповестить администратора Программы.

4. Основные операции в Программе

Оператору поиска угроз доступны следующие возможности Программы:

- 1) Управление собственным профилем пользователя;
- 2) Просмотр в графическом виде параметров состояния защищаемой инфраструктуры;
- 3) Просмотр всех инцидентов;
- 4) Создание инцидентов и добавление событий в свои ранее созданные инциденты;
- 5) Просмотр событий на странице **Активность**;
- 6) Создание поисковых DSL-запросов на странице **Активность**;
- 7) Просмотр активных процессов и модулей;
- 8) Просмотр списка агентов и параметров агентов;
- 9) Создание поисковых DSL-запросов на странице **Агенты**;
- 10) Просмотр графиков работы агентов;
- 11) Просмотр наборов исключений и списка исключений, входящих в каждый набор;
- 12) Просмотр наборов с профилями и самих профилей безопасности агента.



Примечание

Основная функция оператора поиска угроз в Программе – это поиск аномалий в событиях, поступающих с агентов. События приходят на страницу **Активность**, соответственно большую часть времени оператор должен проводить, создавая поисковые DSL-запросы, позволяющие найти необычные для защищаемой инфраструктуры события.

4.1 Просмотр состояния защищаемой инфраструктуры

На главной странице оператор поиска угроз может просмотреть текущее состояние защищаемой инфраструктуры. Информация об инфраструктуре включает в себя следующие области:

- 1) Агенты;
- 2) Инциденты;
- 3) События;

- 4) Последние обнаруженные процессы и модули;
- 5) Текущее значение EPS (на всех агентах и в среднем на одном агенте);
- 6) Среднее за неделю EPS;
- 7) Динамика инцидентов;
- 8) Критичность инцидентов;
- 9) Топ 10 правил в инцидентах;
- 10) Топ 10 техник MITRE в инцидентах
- 11) Информация об уязвимостях.

В области **Агенты** оператор может просмотреть данные об общей численности агентов в защищаемой инфраструктуре, количестве активных агентов и их процентном соотношении к общему количеству, а также количество изолированных агентов (изолированным называется агент, сетевая активность которого полностью остановлена, кроме взаимодействия с сервером EDR). Каждая из представленных в инфографике цифр позволяет перейти на страницу **Агенты** с соответствующей фильтрацией агентов.

В области **Инциденты** оператор может просмотреть общее количество инцидентов, зарегистрированное в защищаемой инфраструктуре, а также количество открытых в данный момент инцидентов. Цифры инфографики позволяют перейти на страницу **Инциденты** с соответствующей фильтрацией инцидентов.

В области **События** оператор может просмотреть общее количество событий, зарегистрированных в защищаемой инфраструктуре в течение последних пятнадцати минут, а также общее количество за день. Цифры инфографики позволяют перейти на страницу **Активность** с соответствующей фильтрацией событий.

В области **Последние обнаруженные процессы и модули** оператор может просмотреть программы, которые работали в защищаемой инфраструктуре в последнее время, имя такой программы является ссылкой для перехода на страницу **Активность** с выполненным соответствующим запросом на языке DSL (отображаются все события, в которых фигурирует выбранная программа).

В области **Текущее значение EPS** (Events per Second) оператор может просмотреть количество событий в секунду, фиксируемое на активных агентах, а также в среднем на одном агенте. Информация показана в виде графика, на котором можно отследить количество событий в пятисекундном интервале, пришедшие на сервер за последнюю минуту.

В области **Среднее за неделю EPS** оператор может просмотреть среднее количество событий в секунду, фиксируемое на активных агентах за последнюю неделю. Информация показана в виде графика, на котором можно отследить общее количество событий за день на недельном интервале времени.

В области **Динамика инцидентов** оператор может просмотреть количество инцидентов за последний день, неделю или месяц, представленное в виде графиков. Каждый график соответствует инцидентам, распределенным по степени критичности.

В области **Критичность инцидентов** оператор может просмотреть распределение инцидентов, зарегистрированных на агентах, по критичности. Графики можно переключать, отображая инциденты, зарегистрированные в течение дня, недели или месяца.

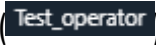
В области **Топ 10 правил в инцидентах** оператор может просмотреть на диаграмме распределение по самым часто встречающимся инцидентам. Диаграмму можно переключать, отображая данные за день, неделю или месяц.

В области **Топ 10 техник MITRE** в инцидентах оператор может просмотреть на диаграмме распределение по самым часто встречающимся техникам Mitre. Диаграмму можно переключать, отображая данные за день, неделю или месяц.

В области **Уязвимости** показана информация о последних инцидентах с трендовыми уязвимостями, а также инфографика с количеством программ, в которых содержатся и отсутствуют уязвимости, количеством уязвимостей по степени критичности и количеством агентов, в которых содержатся и отсутствуют уязвимости.

4.2 Работа с панелью управления

Панель управления находится в верхней части главного окна Программы и содержит следующие кнопки:

- 1) Кнопка для сворачивания/разворачивания панели с разделами Программы ();
- 2) Кнопки включения/отключения светлой и темной темы (/);
- 3) Кнопка управления профилем пользователя (.

Кнопка управления пользователем профиля позволяет сделать изменения в профиле или выйти из текущей учетной записи. Страница редактирования профиля разделена на две области:

- 1) Профиль пользователя;

2) Сессии и устройства.

В области **Профиль пользователя** можно изменить имя, фамилию и e-mail текущего пользователя, включить или отключить возможность получать уведомления о новых инцидентах на электронную почту, а также включить и отключить двухфакторную аутентификацию. Кроме того, пользователь может изменить пароль своей учетной записи, нажав кнопку **Сменить пароль**, после чего откроется окно смены пароля, в котором необходимо ввести текущий пароль, новый пароль, а также повтор нового пароля. Пароль должен соответствовать требованиям, указанным в пояснительной информации в нижней части открывшегося окна:

- пароль не должен совпадать с именем пользователя или другой персональной информацией или быть слишком похожим на нее;
- пароль должен содержать как минимум 12 символов;
- пароль не может быть одним из широко распространенных паролей;
- пароль не должен состоять только из цифр.

Для включения двухфакторной аутентификации или возможности получения уведомлений об инцидентах на почту оператору необходимо установить соответствующие флажки на странице **Профиль пользователя** и нажать кнопку **Сохранить**. После этого кроме ввода пароля при входе в учетную запись Программа потребует ввода числового кода, который отправляется на указанную в профиле электронную почту. Числовой код действителен в течение двух минут. Информация об инцидентах также будет приходить на электронную почту, указанную в профиле оператора.

В области **Сессии и устройства** на странице **Профиль пользователя** отображается информация о запущенных сессиях текущего пользователя. Представлены следующие данные для каждой отдельной сессии:

- 1) Время создания;
- 2) IP-адрес;
- 3) Браузер;
- 4) ОС;
- 5) User agent (имеется в виду строка, которая идентифицирует браузер для веб-сервера).

Оператор может выйти не только из учетной записи на текущем устройстве, но и на всех устройствах (если сессий несколько) одновременно. Для этого предусмотрена кнопка **Выйти на всех устройствах**.

Для выхода из учетной записи текущего пользователя необходимо открыть меню **Пользователь** и нажать кнопку **Выход**.

Если оператор забудет пароль для входа в свою учетную запись, он может воспользоваться кнопкой **Сбросить пароль** на экране входа в Программу. Откроется окно, в котором необходимо будет написать свой логин и нажать кнопку **Отправить запрос**, после чего на почту, указанную при регистрации, будет выслана ссылка для изменения пароля оператора.

4.3 Работа с инцидентами

Для просмотра инцидентов оператору необходимо перейти в раздел **Инциденты** на главной панели Программы слева. Кроме просмотра инцидентов оператор может закрыть инциденты, ранее созданные им же. Для инцидентов, которые создавали другие пользователи, операция **Закрыть выбранные** будет недоступна, как и любые другие действия с инцидентами.



Примечание

Инцидентом называется событие, которое сообщает о возможной угрозе для защищаемой инфраструктуры. Автоматически в инциденты попадают события с уровнем критичности **Средняя** и выше.

Информация об инцидентах представлена в виде таблицы, в которой содержатся следующие поля:

- 1) Критичность (показывает уровень критичности инцидента);
- 2) Название (содержит название инцидента, которое является активной ссылкой для перехода на страницу **Инцидент**);
- 3) Время регистрации (показывает время регистрации инцидента на сервере);
- 4) Время действия (показывает, в течение какого времени длился инцидент);
- 5) Агенты (показывает, на каком агенте инцидент возник, имя агента является активной ссылкой для перехода на страницу **Агент**);
- 6) Кол-во событий (показывает количество входящих в инцидент событий);
- 7) Ответственный (содержит имя пользователя, ответственного за решение инцидента).

В левой части таблицы находятся кнопка для выбора одного или нескольких инцидентов и кнопка раскрытия дополнительной информации об инциденте (>). При нажатии кнопки > оператор может просмотреть краткую информацию о событиях, входящих в инцидент:

- 1) Время регистрации события;
- 2) Критичность события;
- 3) Действие, связанное с событием;
- 4) Краткое описание сути события;
- 5) Имя процесса, с которым связано событие.

Для некоторых инцидентов будут показаны идентификатор MITRE и имя правила, в соответствии с которым событие попало в инцидент.

Информацию об инцидентах можно фильтровать с помощью следующих фильтров:

- 1) Показывать по (показывает на странице 10, 20, 50, 100 или 500 инцидентов);
- 2) Группа (фильтрует инциденты по группам агентов);
- 3) Агент (фильтрует инциденты по выбранному агенту);
- 4) Критичность (фильтрует инциденты по уровню критичности);
- 5) Ответственный (фильтрует инциденты по выбранному пользователю, ответственному за решение инцидента);
- 6) Создатель (фильтрует инциденты, созданные вручную по имени создавшего их пользователя);
- 7) Период регистрации (фильтрует инциденты по временному периоду из списка или заданному с помощью календаря);
- 8) Статус (фильтрует инциденты по статусам **Новый**, **Закрыт**, **Назначен**);
- 9) Правило (фильтрует инциденты в соответствии с именем правила, применение которого привело к возникновению инцидента, например, **SuspiciousFile**);
- 10) MITRE (фильтрует инциденты по идентификатору TTP);
- 11) Полное имя исполняемого модуля процесса (фильтрует инциденты по имени программы, работа которой привела к созданию инцидента).

Оператор может просмотреть информацию об инцидентах в графическом виде. Чтобы на странице отобразились графики, показывающие динамику инцидентов, необходимо нажать кнопку **Показать графики** (▼). Графики могут отображаться в линейном или столбчатом виде (рис.1 - 2).

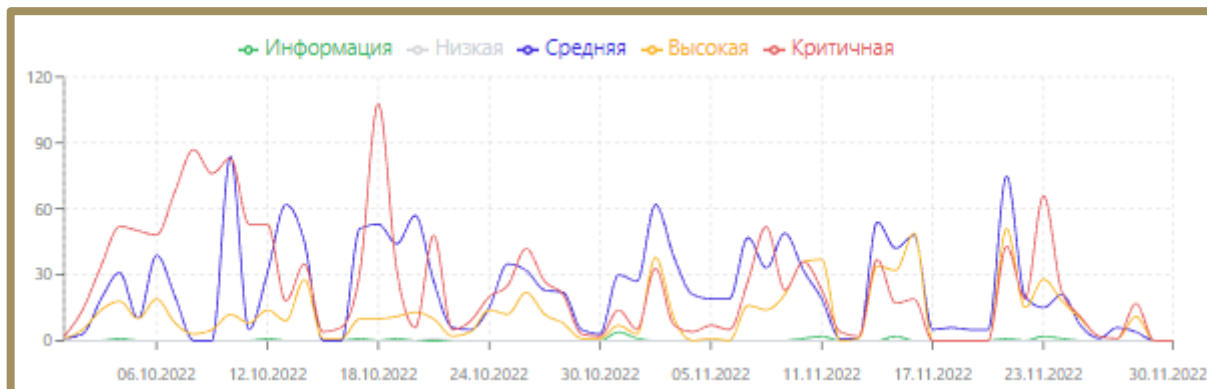


Рисунок 1 – Линейный график



Рисунок 2 – Столбчатый график

Чтобы закрыть инцидент, оператор должен выполнить следующие действия:

- 1) Установить флаг для соответствующей выбранному инциденту кнопки выбора;
- 2) Нажать кнопку **Закреть выбранные**;
- 3) В открывшемся окне изменить текст комментария или оставить комментарий по умолчанию и нажать кнопку **Отправить**.



Важно

Операция доступна только для инцидента, созданного этим же оператором поиска угроз.

Оператор также может удалить созданный им инцидент. Для этого нужно выполнить следующие действия:

- 1) Установить флаг для соответствующей удаляемому инциденту кнопки выбора;
- 2) Нажать кнопку **Удалить выбранные**, откроется окно **Удаление инцидентов**;
- 3) Нажать кнопку **Начать удаление** (удаление инцидентов можно прервать, если операция занимает слишком много времени, для этого необходимо нажать кнопку **Прервать удаление**);
- 4) В открывшемся окне подтвердить операцию, нажав кнопку **Выполнить**;
- 5) После завершения действия нажать кнопку **Заккрыть**.

4.3.1. Страница «Инцидент»

Переход на страницу **Инцидент** выполняется при нажатии имени инцидента. Редактирование инцидента оператором поиска угроз возможно только для инцидентов, созданных этим же оператором. При этом операция комментирования доступна для всех инцидентов.

На странице отображаются следующие области с информацией:

- 1) Инцидент (содержит информацию об инциденте);
- 2) Комментарии;
- 3) Обнаружения.

В области **Инцидент** представлены такие данные:

- 1) Название инцидента;
- 2) Критичность инцидента;
- 3) Ответственный за решение инцидента;
- 4) Статус инцидента;
- 5) Агент, на котором инцидент возник;
- 6) Время регистрации инцидента;
- 7) Время действия инцидента;
- 8) Описание.

Оператор может выполнить несколько операций с инцидентом, созданным им же самим:

- 1) Сохранить изменения на странице инцидента;

- 2) Закрыть инцидент;
- 3) Удалить инцидент.

Каждое из указанных действий требует подтверждения в отдельном окне. Кроме того, оператор может сохранить на свой компьютер отчет об инциденте в формате pdf ().

В области **Комментарии** отображаются ранее сохраненные комментарии, а также присутствует возможность создавать новые комментарии с помощью кнопки **Создать комментарий**.

В области **Обнаружения** содержится таблица с событиями-обнаружениями, входящими в инцидент. Оператор может исключать события из инцидента, если инцидент создан этим же оператором. Во всех остальных случаях кнопка **Исключить выбранные** становится неактивной.

Таблица с событиями в области **Обнаружения** содержит следующие поля:

- 1) Регистрация на сервере (показывает, когда событие было зарегистрировано на сервере);
- 2) Группа/Имя агента (показывает в какую группу входит агент, на котором было зафиксировано событие, и имя этого агента);
- 3) Описание (содержит краткое описание сути события);
- 4) Процесс (содержит имя процесса, работа которого послужила возникновению события, имя является активной ссылкой для перехода на страницу **Процесс**);
- 5) Информация (показывает критичность события в виде флага соответствующего цвета, действие, предпринятое Программой по отношению к событию, имя и номер правила, в соответствии с которым событие попало в инцидент, а также идентификатор TTP MITRE, который является активной ссылкой для перехода к соответствующей TTP на сайте attack.mitre.org).

4.4 Работа с деревом процессов

Страница с деревом процесса открывается при нажатии имени процесса на страницах, связанных с инцидентами, и странице **Активность**.

Дерево процессов – это графическое отображение запуска программ на агенте. Дерево состоит из родительских и дочерних процессов. Если у родительского процесса количество дочерних процессов превышает удобное для просмотра количество процессов, то в правом верхнем углу области отображения появится кнопка  для загрузки оставшихся процессов в область отображения.

Рядом с кнопкой загрузки дополнительных дочерних процессов показано количество отображаемых дочерних процессов и общее количество дочерних процессов для выбранного родительского процесса (Показано 5 дочерних процессов из 127 ).



Примечание

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

Для детального рассмотрения дерева процессов и изменения его расположения, необходимо использовать кнопки  (**Изменить ориентацию дерева**) и  (**Изменить размер области дерева**). После нажатия кнопок окно отображения дерева процессов увеличится в масштабе и дерево процессов поменяет пространственную ориентацию.

Снизу от области отображения дерева процессов находится область с подробной информацией о выделенном в данный момент родительском или дочернем процессе.

Вкладки, которые включают большое количество элементов, могут подгружать информацию в течение некоторого времени, в этот момент рядом с именем вкладки отобразится мигающий значок  (к примеру, **Реестр** ). После завершения загрузки информации рядом с названием вкладки отобразится количество элементов, на которые так или иначе повлиял процесс, выбранный ранее (к примеру, **Реестр (154)**). В таблице отображаются следующие вкладки:

- 1) Информация;
- 2) Файлы;
- 3) Сеть;
- 4) Реестр;
- 5) Процессы;
- 6) Загруженные DLL;
- 7) Точки автозапуска;

- 8) Распространенность;
- 9) Событие старта;
- 10) Правила/MITRE.

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

- [Все события процесса](#) ;
- [Ключевые события процесса \(1\)](#) ;

Все события процесса – при нажатии кнопки [Все события процесса](#) происходит переход к странице **Активность**, на которой будут представлены все дочерние процессы выбранного родительского процесса.

Ключевые события процесса – при нажатии кнопки [Ключевые события процесса \(1\)](#) происходит переход на страницу **Активность**, на которой отображаются важные события (инциденты или события с уровнем критичности от уровня «Низкая» и выше), связанные с процессом. При этом отображаемые события должны подчиняться логике DSL-запроса, указанного в строке **Запрос на языке DSL** (рис. 3).

The screenshot shows the 'Активность' (Activity) page with various filters and a table of events. A red box highlights the 'Запрос на языке DSL' (DSL query) field, which contains the query: `uuid:8db667ba-db8f-01d7-0700-000000000000 AND (svrt[1 TO *] OR (svrt[0 AND (rul:* OR act[0])])`. Below the filters, a table displays event details.

Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Критичность	Действие	Инцидент
17.11.2021, 11:46:09	17.11.2021, 11:46:09	Gr_Илья / Ag_for_lla_W8.1_64	Создан новый ключ \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VirpSvc	services.exe (688)	Низкая		

Рисунок 3 – Ключевые события процесса

4.4.1. Вкладка «Информация»

В таблице раздела отображается общая информация о процессе. Чтобы просмотреть общие данные о процессе, оператор может изучить следующие поля (рис. 4):

- 1) Исполняемый модуль;

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

Исполняемый модуль	\Device\HarddiskVolume8\Users\Yulia\AppData\Roaming\Telegram Desktop\Telegram.exe
Командная строка	"C:\Users\Yulia\AppData\Roaming\Telegram Desktop\Telegram.exe" -noupdate
Время старта / завершения	14.04.2023, 14:58:49 / Процесс запущен
Имя пользователя (SID)	Yulia (S-1-5-21-4150296239-652914265-3817714726-1001)
SHA-256	d3edc61b3c09e4a7746971b3014768bc4b0e7173186ac77833f480f1fac6b578
Цифровая подпись	Telegram FZ-LLC
Флаги исполняемого модуля	Нет данных
Поведенческие признаки	Событие создания синтезировано (Synthetic) Основные системные модули загружены (LaterStage) Показать все...
Распространенность	12 (3.08 %) * WORK / alexb 22.03.2023, 10:20:29

Рисунок 4 – Общая информация о процессе

Исполняемый модуль – в поле отображается имя модуля исполняемого файла, который инициировал запуск процесса. Имя является активной ссылкой, которая позволяет перейти на страницу **Активность** с событием старта процесса для выбранного модуля.

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

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

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

SHA-256 – в поле отображается хеш-сумма исполняемого файла, запустившего процесс. При нажатии ЛКМ на значение хеш-суммы пользователю показывается всплывающее окно с кратким отчетом сервера аналитики об исполняемом файле. В зависимости от статуса артефакт будет отображаться разным цветом

(зеленый – безопасный файл, красный – вредоносный, оранжевый – подозрительный, синий означает, что файл проверяется в данный момент, а серый, что данные о файле отсутствуют). Рядом с хеш-суммой отображаются две кнопки. Первая кнопка позволяет скопировать хеш в буфер обмена (📋). Вторая позволяет перейти на страницу **Процессы и модули** для выбранной хеш-суммы (📄).

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

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

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

Распространенность – в поле отображается, на каком количестве агентов был обнаружен процесс, также просчитано процентное соотношение таких агентов к их общему количеству. Помимо этого, показан агент, на котором процесс был обнаружен впервые и время, когда это было сделано.

4.4.2. Вкладка «Файлы»

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

Для	фильтрации	файлов	предусмотрена	система	флажков
☒ Создан	☒ Переименован	☒ Удален	☒ Модифицирован	☒ Прочитан	☒ Зарезервирован

. Файл, соответствующий выбранному параметру, при снятии флажка не будет отображаться в таблице.

Если среди действий с файлом, присутствующим в списке, было удаление, то он помечается значком

❗. При наведении курсора мыши на значок оператору выводится предупреждающее сообщение (рис. 5).

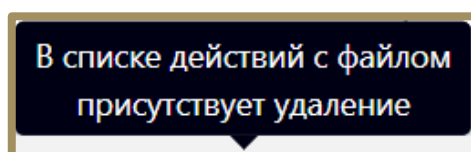


Рисунок 5 – Сообщение о присутствии в списке удаления файла

4.4.3. Вкладка «Сеть»

Во вкладке **Сеть** отображается информация о сетевых подключениях процесса (рис. 6):

- 1) Входящие подключения;
- 2) Исходящие подключения;
- 3) DNS-запросы.

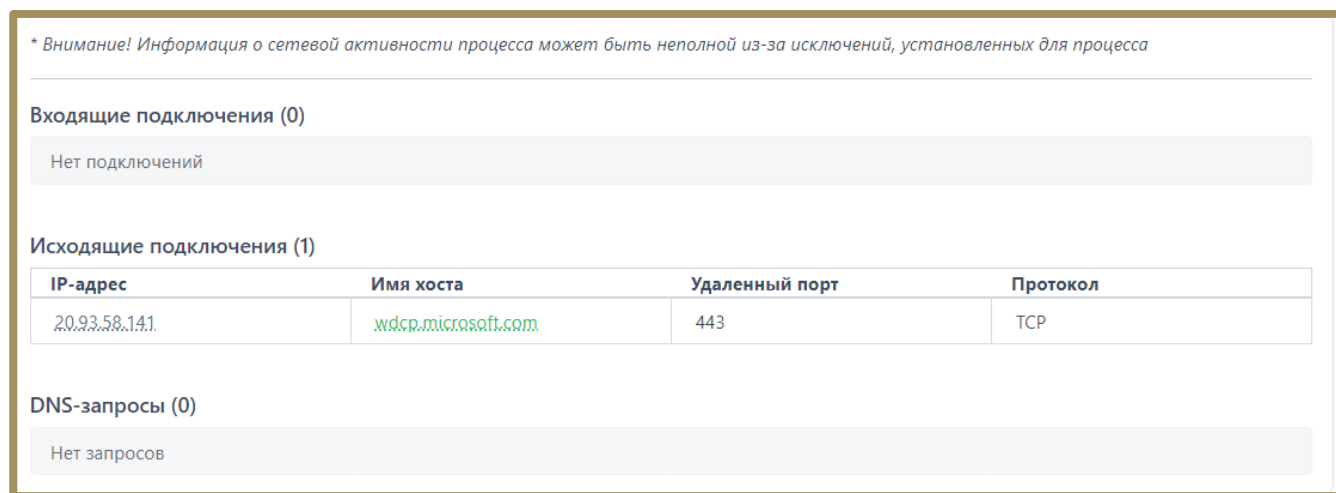


Рисунок 6 – Информация о сетевых подключениях процесса

Информация о сетевых подключениях представлена в табличном виде. Таблица для каждого типа подключения включает в себя следующие поля:

- 1) IP-адрес;
- 2) Имя хоста;
- 3) Удаленный порт;
- 4) Протокол.

IP-адрес – показывает сетевой адрес соответствующего сетевого подключения, при нажатии ЛКМ на значение адреса всплывает окно с кратким отчетом об объекте, полученным от сервера аналитики. В зависимости от статуса артефакт будет отображаться разным цветом (зеленый – безопасный ip-адрес, красный – вредоносный, оранжевый – подозрительный, синий означает, что ip-адрес проверяется в данный момент, а серый, что данные об ip-адресе отсутствуют). При необходимости оператор может перейти на страницу с полным отчетом, нажав кнопку **Перейти к отчету**.

Имя хоста – в поле отображается доменное имя конечной точки, с которой осуществлялось сетевое соединение, доменное имя также автоматически проверяется сервером аналитики, при нажатии ЛКМ на

значение имени оператор может просмотреть отчет сервера. Цветовая дифференциация такая же, как и у других артефактов (файлы, ip-адреса). При необходимости оператор может перейти на страницу с полным отчетом, нажав кнопку **Перейти к отчету**.

Удаленный порт – в поле отображается номер порта, по которому осуществлялось сетевое соединение, для входящего подключения кроме удаленного порта указывается еще и локальный порт.

Протокол – в поле отображается сетевой протокол, по которому осуществлялось сетевое соединение.

4.4.4. Вкладка «Реестр»

Во вкладке **Реестр** отображается информация о ключах реестра, с которыми производил действия выбранный процесс.

☒ Создан	☒ Переименован	☒ Удален	☒ Модифицирован
Ключ реестра	Значение	Действие	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BITS	Start	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc		Создан новый ключ	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	DisplayName	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	ErrorControl	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	ImagePath	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	ObjectName	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	Start	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	Type	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\TrustedInstaller	Start	В значение ключа записаны данные	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\GoogleChromeElevationService	ImagePath	В значение ключа записаны данные	

Рисунок 7 – Ключи реестра, на которые действовал процесс

Информация о ключах реестра представлена в таблице, в которой присутствуют следующие столбцы:

- 1) **Ключ реестра** – в поле прописывается путь ключа реестра, с которым выбранный процесс производил те или иные действия;
- 2) **Значение** – в поле отображается значение, которое было внесено выбранным процессом в ключ реестра;

3) **Действие** – в поле отображается действие, которое совершил выбранный процесс с ключом реестра: это может быть внесение данных в значение ключа, удаление ключа, создание нового ключа и т.д.

4.4.5. Вкладка «Процессы»

Во вкладке **Процессы** отображается информация о процессах, взаимодействовавших или взаимодействующих с выбранным процессом.

Информация разбита на две информационные области **Доступ к процессу** и **Доступ к нити процесса** (рис. 8).

Доступ к процессу (6)			
Имя исполняемого образа	Запрошенные права	Предоставленные права	Кол-во событий
C:\Windows\System32\smss.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	4
C:\Windows\System32\autochk.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\csrss.exe	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	2
C:\Windows\System32\wininit.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\winlogon.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\svchost.exe	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	1
Доступ к нити процесса (4)			
Имя исполняемого образа	Запрошенные права	Предоставленные права	Кол-во событий
C:\Windows\System32\smss.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	2
C:\Windows\System32\autochk.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1
C:\Windows\System32\wininit.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1
C:\Windows\System32\winlogon.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1

Рисунок 8 – Информация на вкладке «Процессы»

Информация представлена в таблице, которая содержит следующие поля:

- **Имя исполняемого образа;**
- **Запрошенные права;**
- **Предоставленные права;**
- **Кол-во событий.**

В области **Доступ к процессу** показана информация о том, к каким процессам в системе выбранный процесс осуществлял доступ, и какие права при предоставлении доступа были запрошены и предоставлены этому процессу.

В области **Доступ к нити процесса** показана информация о том, к каким нитям выбранный процесс осуществлял доступ, и какие права при предоставлении доступа были запрошены и предоставлены.

4.4.6. Вкладка «Загруженные DLL/SO»

Во вкладке **Загруженные DLL/SO** отображается информация о нативных и .Net-библиотеках DLL, используемых выбранным процессом (рис. 9).

Нативные (показано 27 из 27)	Размер файла	Подпись	Размещение	Хеш (SHA-256)
> \Device\HarddiskVolume4\Windows\System32\winmr.dll	31232		0x00007FFC97060000 - 0x00007FFC9706E000	0ce5de9525699efa35d7378472391be583e3cb160557eb5908fdd5f6a38324f9  
> \Device\HarddiskVolume4\Windows\System32\wshbth.dll	64000		0x00007FFC96760000 - 0x00007FFC96775000	5e6d0f371594b4388c51d5153d7209ef9a8e691e669c6a6499c97ec33b290fd4  
> \Device\HarddiskVolume4\Windows\System32\wpnapps.dll	1348608		0x00007FFC82F70000 - 0x00007FFC8308E000	58f7d01809188e2e13c977b2bfc4680a4c55677ff75dd1f2f352165f103d7043  
> \Device\HarddiskVolume4\Windows\System32\netprofm.dll	229376		0x00007FFC9E3F0000 - 0x00007FFC9E42D000	f03f71d6a6507a364a5789ecd78220b8e586ab6a619bc83d5c75cca1c3ca15e8  
> \Device\HarddiskVolume4\Windows\System32\npmproxy.dll	45056		0x00007FFC9C2C0000 - 0x00007FFC9C2D0000	8d10f12787c97ce4c91a4bb6584bacc21d0d1d19f30c4012784749f1266ff2a65  
.NET (показано 0 из 0)	Размер файла	Подпись	Размещение	Хеш (SHA-256)
Нет загруженных DLL				

Рисунок 9 – Список загруженных библиотек DLL

Информация о загруженных DLL разделена на две таблицы для нативных и .Net-библиотек, которая включает в себя следующие данные:

- 1) Имя библиотеки (полный путь);
- 2) Размер (в байтах);
- 3) Подпись;
- 4) Размещение;

5) Хеш (SHA-256), хеш является ссылкой на отчет сервера аналитики, рядом с хеш-суммой содержится кнопка **Копировать в буфер обмена** (📄) и кнопка для перехода на страницу **Процессы и модули** (🔗).

Рядом с названием библиотеки находится кнопка раскрытия дополнительной информации о событии, связанном с библиотекой (➤). При нажатии ЛКМ на кнопку открывается карточка событий, связанная с рассматриваемым процессом и библиотекой. Для процесса **%SYSTEM%** будет представлен список драйверов, дополнительная информация о которых также становится доступной при нажатии кнопки ➤.

4.4.7. Вкладка «Точки автозапуска»

Во вкладке **Точки автозапуска** отображается информация о точках автозапуска, созданных рассматриваемым процессом в реестре (рис. 10).

Реестр (21)		
Ключ реестра	Значение	Тип данных
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	DependOnService	REG_MULTI_SZ
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	ImagePath	REG_EXPAND_SZ
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	ErrorControl	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	Type	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ObjectName	REG_SZ
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	DisplayName	REG_SZ
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ImagePath	REG_EXPAND_SZ
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ErrorControl	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	Start	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	Type	REG_DWORD
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc		
➤ \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc		

Рисунок 10 – Точки автозапуска

Информация представлена в виде таблицы, в которой содержатся следующие поля:

- 1) Ключ реестра;
- 2) Значение;
- 3) Тип данных.

Рядом с названием точки автозапуска в таблице находится кнопка раскрытия дополнительной информации о событии, связанном с этой точкой (>). При нажатии ЛКМ на кнопку открывается карточка событий, связанная с ключами реестра, с помощью которых процессом создавались точки автозапуска.

4.4.8. Вкладка «Распространенность»

Во вкладке **Распространенность** отображается информация о распространении выбранного процесса в агентской сети (рис. 11).

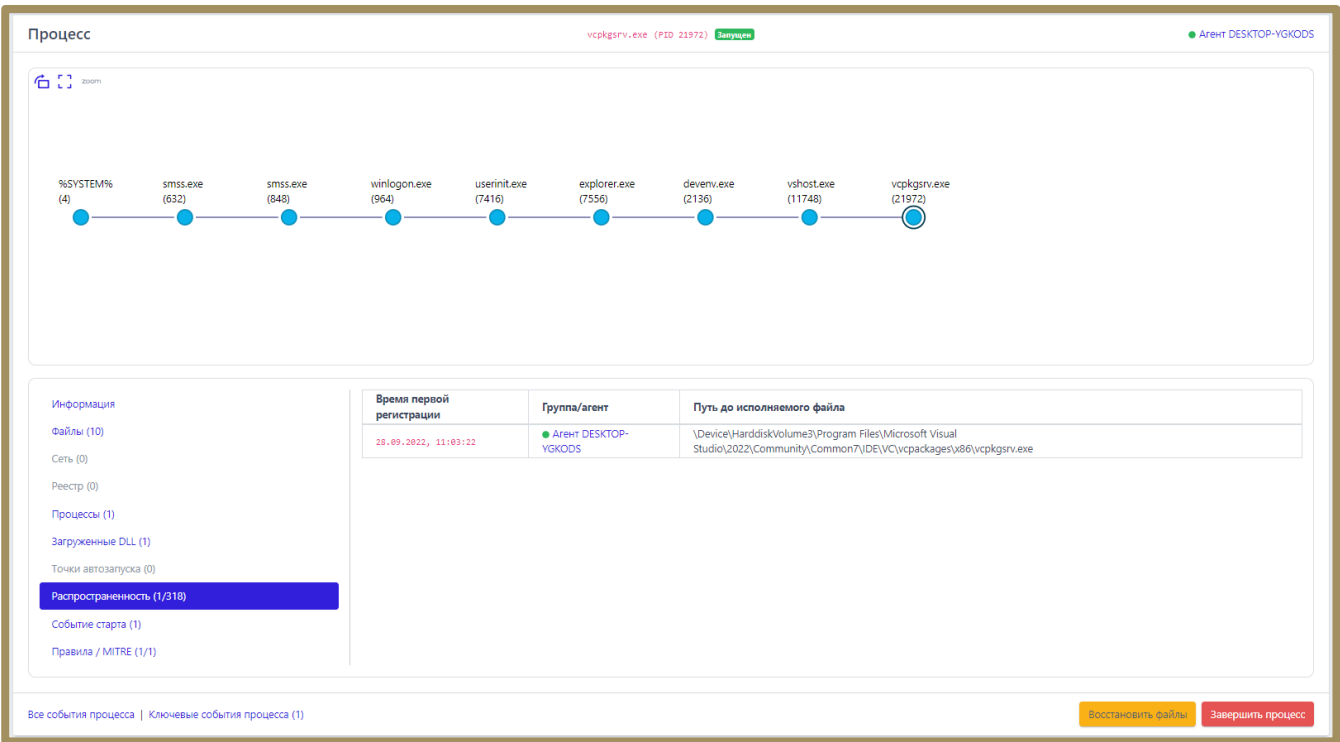


Рисунок 11 – Вкладка «Распространенность»

При этом оператору показывается, когда процесс был впервые зарегистрирован, на каком агенте это произошло и путь до исполняемого файла. Цифры в названии вкладки показывают, на каком количестве агентов присутствует выбранный модуль. Имя агента является ссылкой на страницу **Агент**. Рядом с именем отображается значок, показывающий, активен или не активен агент в данный момент (● \ ○).

4.4.9. Вкладка «Событие старта»

Во вкладке «Событие старта» показана карточка события для старта процесса (рис. 12).

Информация	
Файлы (10)	
Сеть (0)	
Реестр (0)	
Процессы (1)	
Загруженные DLL (1)	
Точки автозапуска (0)	
Распространенность (1/318)	
Событие старта (1)	
Правила / MITRE (1/1)	

Время регистрации на сервере	18.10.2022, 15:32:14
Время регистрации события (UTC)	18.10.2022, 15:32:06
Тип события	Процессы
Подтип события	Старт процесса
Критичность (уровень важности) события	Информация
Агент	Агент DESKTOP-YGKODS
Уникальный идентификатор агента	78a6e5dff3c3a0db2d1198e4e9b283ba7a
Полное имя исполняемого модуля процесса	\\Device\\HarddiskVolume3\\Program Files\\Microsoft Visual Studio\\2022\\Community\\Common7\\IDE\\VC\\vcpackages\\x86\\vcpgksrv.exe ↓
Идентификатор процесса на агентской системе	21972
Идентификатор родительского процесса на агентской системе	11748

Рисунок 12 – Событие старта

Кроме информации со страницы **Процесс** оператору может быть интересна дополнительная информация о событии или событиях инцидента. Для ее просмотра необходимо вернуться со страницы выбранного процесса на страницу **Инцидент**. Для этого оператору достаточно нажать кнопку возврата на предыдущую страницу в браузере.

4.4.10. Вкладка «Правила/MITRE»

Во вкладке **Правила/MITRE** содержится информация о срабатываниях действующих в EDR правил, а также техник MITRE для выбранного процесса.

4.5 Проактивный поиск угроз

Расследование – это определение и изучение оператором поиска угроз событий, связанных с возможной или уже существующей нелегитимной активностью внутри защищаемого периметра.

Современные АPT-атаки могут проводиться таким образом, что явных инцидентов, указывающих на вредоносную активность на конечных точках, возникать не будет. Зачастую такие атаки скрываются под легитимными процессами, используют легитимное ПО, которое является нативным для ОС Windows.

Активный поиск угроз позволяет на ранней стадии выявлять новые и сложные угрозы и рассматривается как дополнение к имеющейся защите информационных систем организации, а не как ее замена. От традиционных методов защиты threat hunting отличает именно проактивность.



Примечание

Активный поиск угроз (threat hunting) – это процесс проактивного (то есть упреждающего) обнаружения вредоносной деятельности в компьютерных сетях.

Поскольку проникновение в систему может произойти в любой момент, поиск угроз – это непрерывный процесс, условно этот процесс можно разбить на 3 шага:

1) Формулирование гипотезы. На этом этапе специалисты строят предположения о том, где следует искать угрозы. Источником информации для выдвижения гипотезы могут служить как внутренние данные компании (сведения о состоянии IT-инфраструктуры, результаты тестов на проникновение и так далее), так и внешние (тактики и техники Mitre Att&ck, отчеты разведки киберугроз, новости безопасности и так далее). Например, если в свежем отчете приводится анализ ранее неизвестного вредоносного ПО, можно предположить, что этот зловард мог проникнуть в инфраструктуру компании.

2) Проверка гипотезы посредством поиска угроз. После формулирования гипотезы ее тестируют. Например, анализируют данные с конечных точек на предмет наличия индикаторов компрометации, связанных с новым вредоносным ПО.

3) Улучшение автоматического анализа. Для этого могут использоваться индикаторы компрометации или индикаторы атак. Успешная охота должна завершаться обогащением возможностей автоматического обнаружения. Если в процессе охоты обнаруживается индикатор или паттерн, который может циркулировать в системе, необходимо автоматизировать его обнаружение, чтобы можно было сосредоточиться на поиске новых угроз.

Чтобы предотвратить целенаправленные атаки, необходимо искать аномалии в работе защищаемой инфраструктуры. Для этого оператор по поиску угроз должен определить, какая активность будет нормой для защищаемых конечных точек или инфраструктуры целиком. Определив нормальное состояние, оператор сможет начать искать отклонения от нормы, чтобы выяснить, являются ли эти отклонения следствием вредоносной активности или нет.

Если обнаруженная аномальная активность не укажет на APT-атаку, результаты поиска все равно могут быть полезны. Положительным эффектом выявления аномалий может стать определение слабых мест защищаемой инфраструктуры или возможностей для улучшения ее защиты. Чем больше аналитик будет знать

о защищаемой системе, тем лучше он сможет ее оборонять от возможных атак и проникновений злоумышленников.

Страница **Активность** позволяет аналитику проводить проактивные расследования и выявлять отклонения от нормы в событиях, поступающих от конечных точек. Кроме большого количества фильтров, позволяющих сортировать телеметрические события по множеству различных параметров, **Активность** предоставляет возможность аналитику использовать строку DSL-запросов на языке Elasticsearch Query DSL.

Для написания запросов необходимо знать структуру событий, отправляемых агентами на сервер, и сам язык запросов. Полное описание полей всех событий расположено в разделе 5.

Описание языка запросов представлено на официальном сайте elasticsearch(<https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html>).

Далее приведено собственное описание языка запросов с примерами.

В общем виде запрос представляет собой поиск некоторого заданного значения в БД событий по определенному временному срезу. Поддерживается как поиск значения вне зависимости от его семантики (принадлежности определенному полю), так и поиск значений среди заданных полей. Пример первого варианта представлен на рисунке 13.

The screenshot shows the 'Активность' (Activity) page in the RT Protect EDR interface. At the top, there are filters for 'Показывать по' (Show by) set to 50, 'Группа' (Group) set to 'Не выбрана' (Not selected), and 'Источник события' (Event source) set to 'Все' (All). Below these, there are options for 'Период регистрации (на сервере)' (Registration period (on server)) set to '15 минут' (15 minutes) and 'Подтип события' (Event subtype) set to 'Не выбран' (Not selected). A red box highlights the 'Запрос на языке DSL' (DSL query) field, which contains the text '*svchost.exe'. To the right of this field is a button 'Отправить' (Send). Below the query field, there are more filters: 'Агент' (Agent) set to 'Не выбран' (Not selected), 'Платформа' (Platform) set to 'Не задана' (Not specified), 'Критичность (не менее)' (Criticality (not less)) set to 'Не задана' (Not specified), and 'Действие, связанное с событием' (Action related to the event) set to 'Не задано' (Not specified). Below the filters, there is a section 'ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ' (Event distribution graphs) with a 'Тип графика' (Chart type) dropdown set to 'Распределение' (Distribution). Below the graphs, there is a table with columns: 'Регистрация на сервере' (Registration on server), 'Регистрация на агенте' (Registration on agent), 'Группа / Имя агента' (Group / Agent name), 'Описание' (Description), 'Процесс' (Process), and 'Информация' (Information). The table shows three rows of events, all with the process 'svchost.exe (76)'. At the bottom left, there is a button 'Добавить в инцидент' (Add to incident).

Рисунок 13 – Запрос вне семантики

Результатом строки запроса **svchost.exe* являются все события, в которых есть поля, значения которых оканчиваются на подстроку *svchost.exe*. Это может быть имя исполняемого файла при запуске нового процесса или имя файла в событии создания нового файла и др.



Примечание

Если DSL-запрос не является оптимальным с точки зрения нагрузки на поисковую систему базы данных, то сверху строки с запросом появляется значок ⌚. Если навести на него курсор мыши, то пользователю будет показана информация о том, что запрос желательно изменить с примером того, как это можно сделать.

Если же требуются именно события процессов с исполняемым файлом *svchost.exe*, в запросе необходимо указать имя поля, для которого будет выполнен поиск. Пример такого запроса представлен на рисунке 14.

The screenshot shows the 'Активность' (Activity) section of the RT Protect EDR interface. At the top, there are filters for 'Показывать по' (Show by), 'Группа' (Group), 'Источник события' (Event source), 'Период регистрации' (Registration period), and 'Подтип события' (Event subtype). Below these, there is a search bar labeled 'Запрос на языке DSL' (DSL query) with the text 'app:svchost.exe' entered. To the right of the search bar is a button 'Отправить' (Send). Below the search bar, there are more filters for 'Агент' (Agent), 'Платформа' (Platform), 'Критичность' (Criticality), and 'Действие, связанное с событием' (Action related to the event). Below the filters, there is a section 'ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ' (Event distribution graphs) with a dropdown for 'Тип графика' (Graph type) set to 'Распределение' (Distribution). Below the graphs, there is a table of events. The table has columns: 'Регистрация на сервере' (Registration on server), 'Регистрация на агенте' (Registration on agent), 'Группа / Имя агента' (Group / Agent name), 'Описание' (Description), 'Процесс' (Process), and 'Информация' (Information). The table shows three rows of events, all related to 'svchost.exe'.

Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
25.05.2023, 13:58:31	25.05.2023, 13:58:29	юля-тест / WIN_8_x32	Система WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_PageFileSetting"	svchost.exe (1080)	🔍
25.05.2023, 13:58:31	25.05.2023, 13:58:29	юля-тест / WIN_8_x32	Система WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_PageFileUsage"	svchost.exe (1080)	🔍
25.05.2023, 13:58:31	25.05.2023, 13:58:29	юля-тест / WIN_8_x32	Система WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_PageFileUsage"	svchost.exe (1080)	🔍

Рисунок 14 – Поиск по заданному полю

Формат запроса с учетом семантики значения имеет вид: **<имя_поля>:<искомое_значение>**. В случае, если искомое значение представляет собой некоторую подстроку, необходимо использовать регулярные выражения. На рисунке, приведенном выше, результатом запроса будут все события, в которых есть поле *app*, и значение этого поля оканчивается на *svchost.exe* (при этом возможно, что значение поля будет в точности равно искомому выражению).

Стоит отметить, что поиск значения ведется с учётом регистра символов. Для того, чтобы регистр не учитывался, к имени поля необходимо указать спецификатор *lower*. Пример запроса без учета регистра приведен на рисунке 15.

Активность

Сбросить фильтры

Показывать по: 50

Группа: Не выбрана

Источник события: Все

Период регистрации (на сервере): 15 минут

Подтип события: Не выбран

Запрос на языке DSL: **app.lower:*svchost.exe**

Агент: Не выбран

Платформа: Не задана

Критичность (не менее): Не задана

Действие, связанное с событием: Не задано

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ

Тип графика: Распределение

Выбрано: 0 из 4548

Найдено: 4548, показано: с 1 по 50

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
>	25.05.2023, 13:59:38	25.05.2023, 13:59:36	WORK / KAA_WORK_MARKS	Сеть DNS-запрос А к 192.168.1.1:53 на имя onedscolorpeus12.eastus.cloudapp.azure.com размером 60 байт	svchost.exe (2420)	
>	25.05.2023, 13:59:35	25.05.2023, 13:59:34	юля-тест / Windows_10_x32 (new)	Система WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root/cimv2 : Win32_PageFileUsage"	svchost.exe (1260)	

Добавить в инцидент

Рисунок 15 – Запрос без учета регистра



Важно

Имя поля всегда указывается с учетом регистра. В RT Protect EDR принято соглашение, что названия полей содержат только строчные буквы, поэтому имена полей в запросе должны состоять только из строчных букв.

Язык Elasticsearch Query DSL позволяет осуществлять сложные запросы, состоящие из объединения простых запросов, рассмотренных ранее, с помощью логических операторов: И, ИЛИ, НЕ. Логические операторы задаются с помощью ключевых слов: AND, OR, NOT. Ключевые слова записываются с учетом регистра символов, т.е. And, and не являются логическими операторами. Для группировки результатов выполнения подзапросов используются круглые скобки. Пример сложного запроса представлен на рисунке 16.

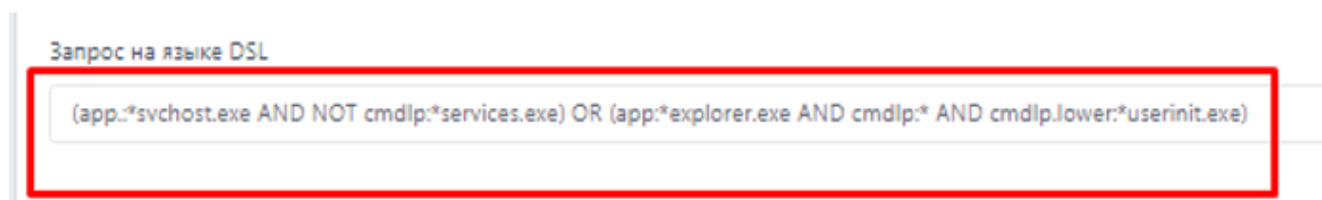


Рисунок 16 – Сложный DSL-запрос

С помощью приведенного запроса выполняется поиск событий запуска подозрительных процессов svchost.exe и explorer.exe. Для этого проверяется командная строка родительских процессов. В основном экземпляры штатных процессов svchost запускаются процессом services.exe, а explorer.exe – процессом userinit.exe. Дополнительное условие для проверки командной строки родительского процесса «*cmdlp:**» необходимо для случаев установки агента «на горячую». Агент устанавливается на работающую систему и сразу начинает отправлять события. В этой ситуации агент для консистентности представления информации формирует синтетические события запуска процессов. Но получить информацию о родительском процессе для синтетического события запуска не всегда возможно, в частности для explorer.exe это невозможно, поскольку его родительский процесс userinit.exe уже завершен. В результате выполнения запроса выявлен запуск svchost.exe антивирусом Microsoft Defender.

Для удобства помимо фильтрации событий на основе запросов с помощью языка Elasticsearch Query DSL на форме **Активность** представлены поля для фильтрации. Фильтры в представлении страницы **Активность** по умолчанию позволяют сортировать события по следующим критериям:

- 1) Количество отображаемых событий на странице;
- 2) Группа (на странице отобразятся события, пришедшие от агентов выбранной группы);
- 3) Тип события (на странице отобразятся события, соответствующие выбранному источнику: сеть, файлы, реестр и т.д.);

- 4) Период регистрации событий на сервере;
- 5) Подтип события;
- 6) Агент;
- 7) Платформа (ОС Windows или Linux);
- 8) Критичность (на странице отобразятся события с критичностью не ниже выбранной);
- 9) Действие, связанное с событием.

Таким образом на странице **Активность** можно составлять запросы тремя способами:

- только с помощью языка запросов (все поля фильтрации сброшены);
- только с помощью полей фильтрации, с заполнением их соответствующими значениями (строка запроса при этом пустая);
- комбинированным — используются и поля фильтрации, и текст запроса.

Комбинированный способ удобен, когда наряду с несколькими односложными условиями (например, требуется поиск по конкретному единственному типу события и на конкретном агенте) события фильтруются на основе целого набора возможных значений некоторого поля.

Наиболее простым примером использования раздела **Активность** является ретроспективный анализ на предмет выявления артефактов «свежих» угроз. Например, в одном из контуров агентской сети было проведено расследование некоторого инцидента, в результате которого были выявлены: хэши, ip-адреса, DNS-имена, имена исполняемых файлов, связанные с этим инцидентом. Далее обычно происходит поиск в других контурах, с целью определения факта компрометации других агентов. Пример такого запроса представлен на рисунке 17.

Запрос на языке DSL

```
sha256:0ad37dc6b692903c4e129b1ad75ee8188da4b9ce34c309fed34a25fe86fb176d OR r_ip:142.149.1.99 OR dnsq_h:tracker.justseed.it OR app.lower:*beacon.exe
```

Рисунок 17 – Пример запроса для ретроспективного анализа угроз

В результате выполнения запроса было выявлено обращение по DNS-имени, связанному с вредоносной активностью.

Для полей событий с числовыми значениями возможно использование операторов сравнения значений (>, <, >=, <=). Пример запроса для вывода сетевых событий, у которых размер сетевого пакета превышает 100 байт, представлен на рисунке 18.

Активность

Сбросить фильтры

Показывать по

50

Группа

Не выбрана

Источник события

Все

Период регистрации (на сервере)

15 минут

Подтип события

Не выбран

Запрос на языке DSL

size:>=100

Отправить

Агент

Не выбран

Платформа

Не задана

Критичность (не менее)

Не задана

Действие, связанное с событием

Не задано

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ

Тип графика: Распределение Динамика

Выбрано: 0 из 2096

Найдено: 2096, показано: с 1 по 50

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
>	25.05.2023, 14:55:53	25.05.2023, 14:55:51	ila_group / Ag_for_ila_WS2012	Сеть DNS-ответ со статусом 9501 на запрос А к 194.85.252.62:53 на имя ns2.spektr-orel.ru размером 994 байт	dns.exe (1400)	
>	25.05.2023, 14:55:53	25.05.2023, 14:55:50	ila_group / Ag_for_ila_WS2012	Сеть DNS-ответ со статусом 9501 на запрос А к 8.8.8.8:53 на имя ns1.homelink.ru размером 108 байт	dns.exe (1400)	

Добавить в инцидент

Рисунок 18 – Пример запроса с числовым значением

Также допускается фильтрация для диапазона значений. Пример фильтрации событий, связанных с входящими сетевыми подключениями для диапазона сетевых портов [1080;1800], представлен на рисунке 19.

Активность

Сбросить фильтры

Показывать по

50

Группа

Не выбрана

Источник события

Все

Период регистрации (на сервере)

15 минут

Список

Календарь

Подтип события

Не выбран

Запрос на языке DSL

r_ip:[1080 TO 1800]

Примеры запросов

Отправить

Агент

Не выбран

Платформа

Не задана

Критичность (не менее)

Не задана

Действие, связанное с событием

Не задано

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ

Тип графика:

Распределение

Динамика

« 1 2 3 4 ... »

Выбрано: 0 из 323

Найдено: 323, показано: с 1 по 50

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
> ☐	25.05.2023, 14:57:04	25.05.2023, 14:56:59	WORK / ANPG_WORK_10	Сеть SSL HELLO (rtk1.pass.xzvpn.net) с rtk1.pass.xzvpn.net (178.62.202.111:443) размером 517 байт	chrome.exe (10516)	☐
> ☐	25.05.2023, 14:57:04	25.05.2023, 14:56:59	WORK / ANPG_WORK_10	Сеть Исходящее подключение к rtk1.pass.xzvpn.net (178.62.202.111:443) по TCP	chrome.exe (10516)	☐
> ☐	25.05.2023,	25.05.2023,	WORK /	Сеть Исходящее подключение к mail.vr-protect.ru (178.208.150.156:443) по TCP	chrome.exe (13756)	☐

Добавить в инцидент

Рисунок 19 – Пример запроса с диапазоном значений

Следует отметить, что наиболее частой ошибкой при поиске, например, исполняемого модуля, является указание его названия без расширения. Иллюстрация такой ситуации представлена на рисунках 20 - 21.

Активность

Сбросить фильтры

Показывать по

50

Группа

Не выбрана

Источник события

Все

Период регистрации (на сервере)

15 минут

Список

Календарь

Подтип события

Не выбран

Запрос на языке DSL

r_ip:[1080 TO 1800]

Примеры запросов

Отправить

Агент

Не выбран

Платформа

Не задана

Критичность (не менее)

Не задана

Действие, связанное с событием

Не задано

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ

Тип графика:

Распределение

Динамика

« 1 2 3 4 ... »

Выбрано: 0 из 323

Найдено: 323, показано: с 1 по 50

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
> ☐	25.05.2023, 14:57:04	25.05.2023, 14:56:59	WORK / ANPG_WORK_10	Сеть SSL HELLO (rtk1.pass.xzvpn.net) с rtk1.pass.xzvpn.net (178.62.202.111:443) размером 517 байт	chrome.exe (10516)	☐
> ☐	25.05.2023, 14:57:04	25.05.2023, 14:56:59	WORK / ANPG_WORK_10	Сеть Исходящее подключение к rtk1.pass.xzvpn.net (178.62.202.111:443) по TCP	chrome.exe (10516)	☐
> ☐	25.05.2023,	25.05.2023,	WORK /	Сеть Исходящее подключение к mail.vr-protect.ru (178.208.150.156:443) по TCP	chrome.exe (13756)	☐

Добавить в инцидент

Рисунок 20 – Пример неправильного DSL-запроса

Активность

Сбросить фильтры

Показывать по

50

Группа

Не выбрана

Источник события

Все

Период регистрации (на сервере)

15 минут

Список

Календарь

Подтип события

Не выбран

Запрос на языке DSL

app:*chrome.exe

Примеры запросов

Отправить

Агент

Не выбран

Платформа

Не задана

Критичность (не менее)

Не задана

Действие, связанное с событием

Не задано

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ

Тип графика: Распределение Динамика

«

1

2

3

4

...

»

Выбрано: 0 из 1092

Найдено: 1092, показано: с 1 по 50

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
> ☐	25.05.2023, 15:03:48	25.05.2023, 15:03:44	● lla_group / Ag_for_lla_WS2012	Сеть SSL HELLO (static-cdn.jtvnw.net) с jtvnw.twitchcdn.net (18.165.128.214:443) размером 517 байт	chrome.exe (4792)	🔍
> ☐	25.05.2023, 15:03:48	25.05.2023, 15:03:44	● lla_group / Ag_for_lla_WS2012	Сеть Исходящее подключение к jtvnw.twitchcdn.net (18.165.128.214:443) по TCP	chrome.exe (4792)	🔍

Добавить в инцидент

Рисунок 21 – Исправленный вариант DSL-запроса

С помощью первого запроса не найдено ни одного события, однако после добавления расширения сразу найдены требуемые события. Это связано с тем, что поиск осуществляется не по подстроке, а по строке целиком. Но для гибкости допускается использовать регулярные выражения. Поиск без указания расширения должен выглядеть как на рисунке 22.

Активность Сбросить фильтры

Показывать по: 50 Группа: Не выбрана Источник события: Все

Период регистрации (на сервере): 15 минут Подтип события: Не выбран

Запрос на языке DSL: `app:"chrome"` Примеры запросов Отправить

Агент: Не выбран Платформа: Не задана Критичность (не менее): Не задана Действие, связанное с событием: Не задано

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ Тип графика: Распределение Динамика

« < 1 2 3 4 ... > » Выбрано: 0 из 1038 Найдено: 1038, показано: с 1 по 50

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
> ☐	25.05.2023, 15:05:38	25.05.2023, 15:05:34	юля-тест / WIN_8_x32	Сеть Исходящее подключение к clientservices.googleapis.com (142.251.1.94:443) по UDP	chrome.exe (8996)	🔍
> ☐	25.05.2023, 15:05:38	25.05.2023, 15:05:34	юля-тест / WIN_8_x32	Сеть DNS-ответ со статусом 0 на запрос А к 192.168.47.2:53 на имя clientservices.googleapis.com размером 63 байт, результат: 142.251.1.94;	chrome.exe (8996)	🔍
> ☐	25.05.2023,	25.05.2023,	lla_group /	Сеть SSL HELLO (pubsub-edge.twitch.tv) < pubsub-edge.twitch.tv (44.240.168.143:443)	chrome.exe (4792)	🔍

Добавить в инцидент

Рисунок 22 – Использование регулярных выражений для DSL-запроса

Удобно пользоваться оператором отрицания (NOT). Ниже представлен запрос, с помощью которого можно отфильтровать события создания новых .exe-файлов для всех процессов, кроме svchost.exe (рис. 23).

Активность Сбросить фильтры

Показывать по: 50 Группа: Не выбрана Источник события: Все

Период регистрации (на сервере): 15 минут Подтип события: Не выбран

Поля для отображения: Не выбраны Поля для фильтрации: Агент x Критичность (не менее) x Полное имя исполняемого модуля процесса x

Запрос на языке DSL: `name:".exe" AND NOT app:"svchost.exe"` Примеры запросов Отправить

Агент: Не выбран Критичность (не менее): Не задана Полное имя исполняемого модуля процесса: Введите значение

ГРАФИКИ РАСПРЕДЕЛЕНИЯ СОБЫТИЙ Тип графика: Распределение Динамика

« < 1 > » Выбрано: 0 из 18 Найдено: 18, показано: с 1 по 18

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
> ☐	05.12.2022, 14:16:09	05.12.2022, 14:16:05	JP_WIN_10	Файл Удален файл \Device\HarddiskVolume8\Users\Yulia\AppData\Local\Temp\Rar\$DRa15740.22802\Setup.exe	WinRAR.exe (13476)	🔍

Добавить в инцидент

Рисунок 23 – Пример использования оператора NOT

4.5.1. Просмотр графиков активности

Кроме табличного представления на странице **Активность** оператор может просматривать информацию о событиях в графическом виде. Просмотреть графики можно в области **Графики распределения событий**. Чтобы открыть ее, необходимо нажать кнопку **Показать графики** (▼).

Доступно два основных вида графика (рис. 24 и 25):

- 1) Первый показывает количественное распределение событий по типам и подтипам;
- 2) Второй показывает динамику событий по типам и подтипам (может отображаться в линейном и столбчатом виде).

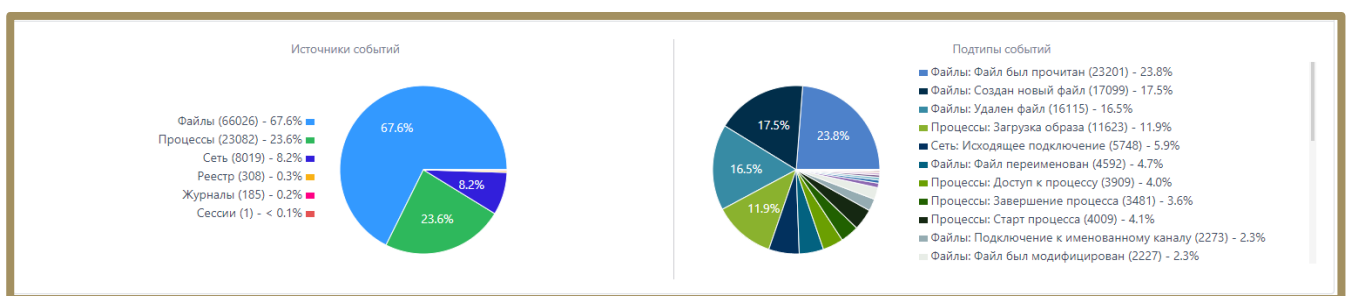


Рисунок 24 – График с распределением событий

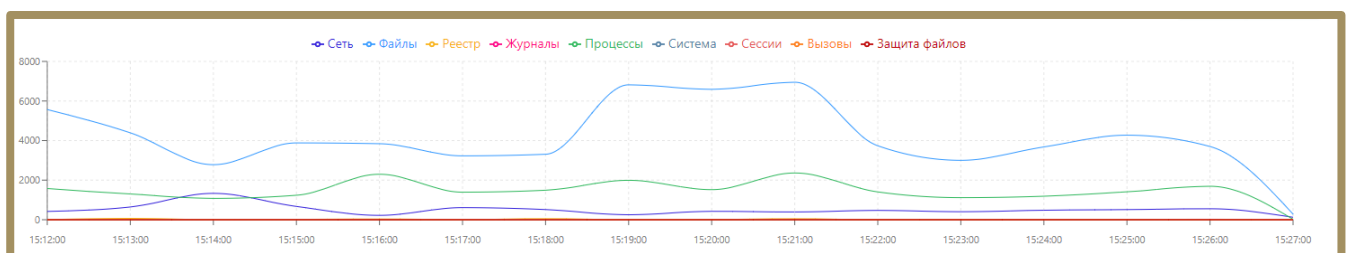


Рисунок 25 – График с динамикой событий

4.5.2. Создание инцидента на странице «Активность»

Оператор в случае обнаружения на странице **Активность** событий, которые указывают на аномалии на конечной точке, может создать инцидент вручную. Чтобы добавить новый инцидент, оператору необходимо выполнить следующие действия:

- 1) Отметить флажком кнопку выбора для соответствующего события;
- 2) Нажать кнопку **Добавить в инцидент**;
- 3) Из выпадающего списка выбрать пункт **Новый**;

4) В открывшемся окне **Добавление событий в новый инцидент** заполнить поля и нажать кнопку **Добавить**.

После добавления вновь созданный инцидент отобразится на странице **Инциденты**. Чтобы добавить события в ранее созданный инцидент, оператору необходимо выполнить следующие действия:

- 1) Отметить флажком кнопку выбора для добавляемого в инцидент события;
- 2) Нажать кнопку **Добавить в инцидент**;
- 3) Выбрать пункт **Существующий**;
- 4) В открывшемся окне выбрать один из ранее созданных инцидентов;
- 5) Если это необходимо, установить флаг **Перейти к инциденту**;
- 6) Нажать кнопку **Добавить**.

4.6 Проверка артефактов с помощью TI-платформы

TI-платформа – это работающий в связке с EDR дополнительный сервис проверки артефактов: хешей, доменных имен, глобальных ip-адресов. На странице **Активность** артефакты можно наблюдать в карточке события, открываемой по кнопке **>**. Кроме того, ссылки на отчеты TI-платформы содержатся на странице **Процесс и Процессы и модули**. Отчеты сервера аналитики содержат вердикт, основанный на информации, полученной из множества различных источников: база данных Virus Total, MalwareBazaar и другие открытые источники информации.

Если хеши исполняемых файлов (PE) определяются TI-платформой, как вредоносные, то запуск таких файлов автоматически запрещается и на сервере управления регистрируется инцидент. Также инцидент регистрируется, если TI-платформа определяет домен или IP-адрес, как вредоносный, при этом обращение к такому домену или адресу не блокируется.

4.7 Проверка распространенности программы в агентской сети

На странице **Процессы и модули** оператор может просмотреть распространенность программы (модуля) в агентской сети, а также узнать вердикт TI-платформы по этой программе (рис. 26). Распространённость программы показывает, на каких агентах появлялся файл с определенной хеш-суммой.

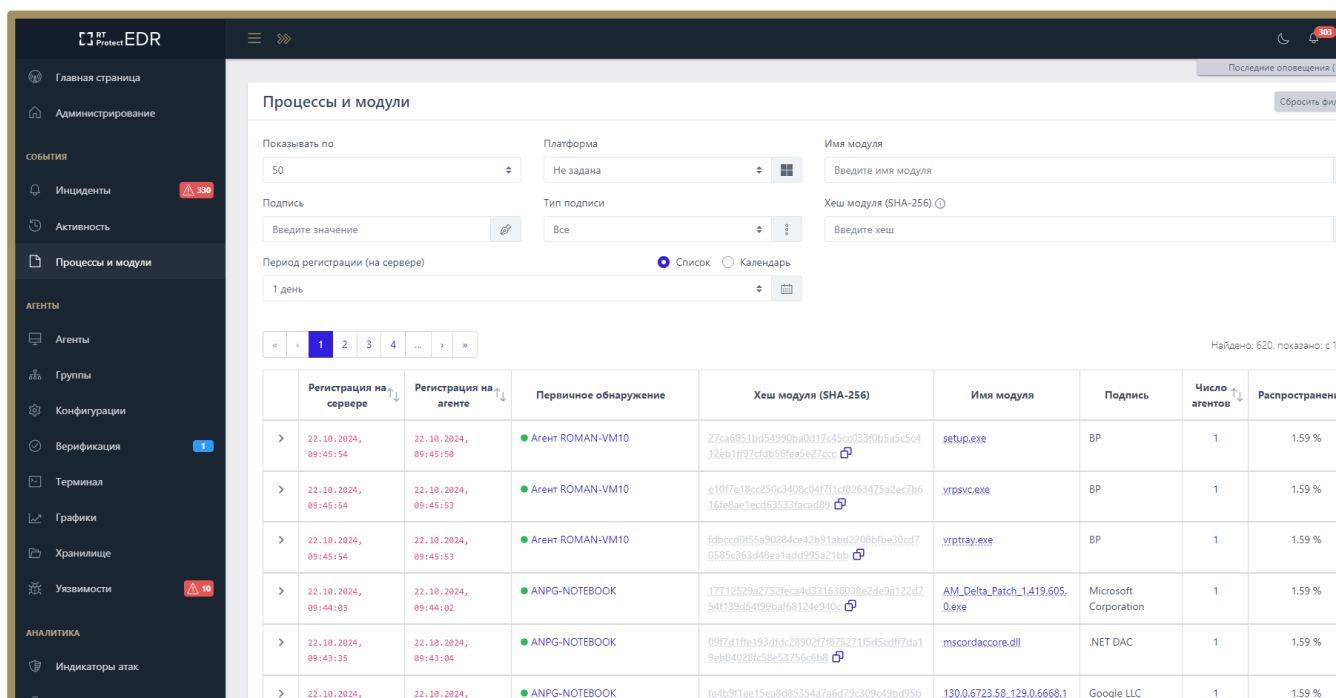


Рисунок 26 – Процессы и модули

Оператор может искать нужную программу с помощью фильтров:

- 1) Показывать по (10, 20, 50, 100 строк в таблице);
- 2) Подпись (фильтры **Все**, **Неподписанные**, **Кроме широко известных**);
- 3) Имя модуля;
- 4) Платформа (Windows, Linux);
- 5) Хеш модуля;
- 6) Период регистрации на сервере.

Вердикт сервера аналитики открывается, если оператор нажмет поле с хеш-суммой. Первоначально открывается краткий отчет. Полный отчет доступен, если нажать кнопку **Перейти к отчету**.

Пользователь может просмотреть дополнительную информацию из карточки события для старта процесса, которая открывается при нажатии кнопки **>**.

В таблице с основной информацией о программе отображаются следующие поля:

- 1) Время регистрации старта процесса на сервере;
- 2) Время регистрации старта процесса на агенте;
- 3) На каком агенте программа была обнаружена впервые;
- 4) Хеш программы;

- 5) Имя файла (имя программы);
- 6) Электронная подпись;
- 7) Число агентов, на которых была обнаружена программа;
- 8) Распространение программы в агентской сети (в процентах от общего числа агентов).

4.8 Действия с агентами

На странице **Агенты** оператор может выполнить следующие действия:

- просмотреть информацию о верифицированных в системе агентах (группа, имя агента, версия агента, значение EPS на агенте (количество событий, происходящих на агенте в секунду), сетевые адреса, домен, имя компьютера, на котором агент установлен, операционная система, часовой пояс, состояние агента и используемые на агенте конфигурационные наборы);
- отфильтровать агентов с помощью представленных на странице фильтров (активность, имя агента, домен, настройки и т.д.);
- выполнить DSL-запрос для фильтрации агентов в соответствии с этим запросом\$
- сохранить отчет об агентах в формате CSV () , отчет содержит информацию согласно выборке на странице **Агенты**, то есть изменяя состояние фильтров можно изменять информацию, которая будет представлена в отчете.

В поле **Состояние** таблицы с агентами могут отображаться значки, указывающие на определенные состояния агента:

 — значок указывает на то, что в составе золотого образа агента (под образом понимается зафиксированный Программой состав ПО, установленного на агенте), произошли изменения (удалены некоторые программы из золотого образа или установлены новые программы, не входящие в состав золотого образа);

 — значок указывает на то, что на агенте установлена парольная защита от удаления, то есть чтобы удалить агента с компьютера, будет необходимо ввести пароль, заданный после включения опции парольной защиты от удаления;

 — значок указывает на то, что на агенте установлена функция отслеживания состава золотого образа, но отличий от золотого образа ПО этого агента нет.

Для перехода к странице **Агент** необходимо кликнуть по имени агента.

На странице **Агент** оператор может выполнить следующие действия:

- скачать полный или краткий отчет об агенте в формате pdf (PDF), полный отчет будет содержать список установленного ПО и установленных драйверов;
- просмотреть информацию о выбранном агенте (версия, часовой пояс, имя и т.д.);
- скопировать в буфер обмена идентификатор агента;
- просмотреть количество событий и инцидентов на агенте за последнее время и за все время с момента его верификации;
- просмотреть информацию о состоянии агента (состояние изоляции, состояние защиты);
- просмотреть информацию о количестве событий на агенте за последние сутки и 15 минут;
- просмотреть информацию о количестве инцидентов, возникших на агенте (общее количество и открытые инциденты);
- просмотреть состояние золотого образа агента (под золотым образом подразумевается зафиксированный список ПО на компьютере с установленным агентом);
- просмотреть информацию о состоянии парольной защиты от удаления агента;
- просмотреть информацию о группе, в которую входит агент;
- просмотреть информацию о количестве событий, приходящих с агента в секунду (EPS) на текущий момент и среднее EPS за последнюю неделю;
- просмотреть информацию о конфигурациях аналитических правил, примененных на агенте;
- просмотреть информацию о системе, в которой установлен агент;
- просмотреть информацию об установленном ПО на машине с агентом;
- сканировать уязвимости в программном обеспечении, установленном на машине с агентом;
- просмотреть информацию об установленных драйверах на машине с агентом;
- назначить или изменить конфигурационный набор с индикаторами или исключениями для агента;
- изменить группу, в которую входит агент;
- просмотреть графики, показывающие статистическую информацию по активности системы за последние 15 минут;



Примечание

В разделах **Обновления системы**, **Установленное ПО** и **Установленные драйверы** оператору будут показаны все установленные программы и драйверы, а также обновления операционной системы, не соответствующие золотому образу (если состояние золотого образа отслеживается и в нем имеются расхождения с текущим состоянием системы). Значок  и зачеркнутое наименование элемента означает, что он был удален с компьютера с установленным агентом, но при этом присутствует в золотом образе. Значок  напротив программы означает, что она была установлена на компьютер с агентом, но при этом в золотом образе эта программа отсутствует. Обновления системы отображаются с теми же особенностями, только вместо значков обновления отображаются в красной и зеленой заливке, где красная заливка и перечеркнутое наименование приравнивается к значку , а зеленая заливка обновления к значку .

4.9 Просмотр конфигураций

В разделе **Конфигурации** оператор может просматривать информацию о конфигурациях аналитических наборов и профилей, назначаемых агентам на этапе верификации.

4.10 Просмотр графиков

На странице **Графики** оператор может просмотреть статистическую информацию о параметрах конечной точки, на которой установлен агент. Для просмотра доступна следующая информация:

- загрузка центрального процессора (в процентах);
- загрузка оперативной памяти (в процентах);
- количество запущенных процессов;
- количество нитей процессов;
- количество дескрипторов;
- загрузка диска в Кб/с (на чтение);
- загрузка диска в Кб/с (на запись);
- загрузка сети в Кбит/с (на передачу);

— загрузка сети в Кбит/с (на прием).

Просмотр графиков доступен только для активных агентов. Чтобы добавить график, необходимо нажать кнопку . Программа показывает графики в соответствии с выбранным временным интервалом.

Доступны следующие интервалы:

- 15 минут;
- 1 час;
- 8 часов;
- 1 день;
- 1 неделя;
- 1 месяц;
- 3 месяца.

4.11 Уязвимости

Уязвимость – это недостаток программы, используя который, можно нарушить ее целостность и вызвать неправильную работу программы.

Управление уязвимостями осуществляется в разделе **Уязвимости**. Сканирование уязвимостей осуществляется ПИ-платформой и позволяет проверить программное обеспечение на конечных точках с установленными агентами и выявить программы, защита которых ослаблена наличием известных и эксплуатируемых уязвимостей.

Сканер способен обнаруживать уязвимости из базы NIST (National Institute of Standards and Technology), а также из базы данных угроз ФСТЭК (БДУ ФСТЭК).



Примечание

Запрос на сканирование программы на наличие уязвимостей отправляется ПИ-платформе в случае обнаружения в RT Protect EDR нового ПО.

Для специалиста, работающего с уязвимостями, важны такие понятия, как инциденты модуля уязвимости и критичность агента. Под инцидентами подразумеваются сущности, возникающие в случае

совпадения двух событий: на агенте присутствует программа, в которой есть «трендовая» уязвимость, а также критичность агента имеет значение «Критичная». Трендовые уязвимости определяются аналитиками на TI-платформе, а критичность агента устанавливается аналитиками RT Protect EDR. Критичным может быть агент, установленный на важном хосте: контроллер домена, сервер с важной базой данных и т.д. Трендовая уязвимость в Программе помечается соответствующим значком (🔥). Обычно под трендовыми подразумеваются такие уязвимости, которые активно используются злоумышленниками в данный момент времени и поэтому требуют особого внимания к себе со стороны сотрудников информационной безопасности.

Страница **Уязвимости** содержит диаграммы, на которых можно видеть результаты сканирования обнаруженных в защищаемой инфраструктуре программ, количество выявленных уязвимостей с разбивкой по критичности, а также покрытие агентов по наличию на них уязвимостей. Записи диаграмм **Программы** и **Уязвимости** кликабельны и позволяют перейти во вкладку **Программы** с соответствующей настройкой фильтрации полей.

Информация во вкладке **Инциденты** представлена в таблице, которая содержит следующие поля:

- 1) Инцидент (содержит название инцидента и CVE-идентификатор уязвимости);
- 2) Агент (показывает имя критичного агента, на котором содержится программа с трендовой уязвимостью);
- 3) Статус инцидента (активен, завершен автоматически или завершен вручную);
- 4) Программное обеспечение (название программы, в которой обнаружена трендовая уязвимость);
- 5) Время обнаружения;
- 6) Действия (содержит кнопку **Заккрыть инцидент** ).

Инциденты можно искать с помощью фильтров: **Статус**, **Агент**, **Группа**. Клик по имени инцидента приводит к переходу на страницу, содержащую сведения об инциденте, сведения о программе, в которой найдена трендовая уязвимость, и сведения об этой уязвимости. В области **Сведения об инциденте** содержится кнопка **Заккрыть инцидент**. При закрытии инцидента необходимо указывать причину его закрытия, это может быть изменение критичности агента, обновление программы, закрывающее уязвимость или снятие с уязвимости аналитиком TI-платформы статуса трендовой.

Информация во вкладке **Программы** представлена в таблице, которая содержит следующие поля:

- 1) Имя;

- 2) Издатель;
- 3) Версия;
- 4) Агенты;
- 5) Уязвимости.

Программы в таблице можно фильтровать с помощью следующих фильтров:

- 1) Статус;
- 2) Агент;
- 3) Платформа (Windows или Linux);
- 4) Имя;
- 5) Издатель;
- 6) Критичность (не менее);
- 7) Признак трендовой уязвимости (трендовая или обычная);
- 8) Группа агентов;
- 9) Оценка CVSS (от 0 до 10);
- 10) Значение CVE.

Клик по имени программы в таблице вкладки **Программы** приводит к переходу на страницу, содержащую сведения о программе, в том числе об агентах, на которых эта программа присутствует, а также сведения обо всех обнаруженных в программе уязвимостях. Уязвимости отмечаются значками, показывающими степень критичности ( – критичная,  – высокая,  – средняя,  – ниже среднего,  – низкая).

Клик по идентификатору CVE-уязвимости в таблице вкладки **Программы** приводит к переходу на страницу, содержащую сведения об уязвимости, в том числе список относящихся к ней CVE и количество программ, в которых уязвимость присутствует.



Примечание

В отличие от CVE, идентификатор CWE указывает не на конкретную уязвимость, а на общую проблему или недочет в программном обеспечении.

Кроме сведений об уязвимости страница содержит критерии соответствия уязвимости, ее описание, рекомендации по устранению.

4.11.1. Формирование отчетности на странице с уязвимостями

Аналитик может сформировать отчет о найденных на агентах уязвимостях и сохранить этот отчет на компьютер, с которого осуществляется доступ к серверу управления. Отчет формируется на странице **Управление уязвимостями** во вкладке **Программы**. Чтобы сохранить отчет в формате csv, необходимо нажать кнопку , после чего отчет будет доступен в папке **Загрузки** или в другой папке, указанной в настройках браузера. Для формирования отчета необходимо использовать кнопку .

В отчете отображается полный список ПО на просканированных агентах, в котором присутствуют программы с найденными уязвимостями. Отчет формируется с учетом применяемых на странице фильтров.

4.11.2. Распространенность программы с уязвимостью в защищаемой инфраструктуре

Чтобы получить информацию о распространении программы с уязвимостью в защищаемой EDR инфраструктуре, аналитику необходимо перейти в раздел **Программы** страницы **Управление уязвимостями**, после чего кликнуть по имени программы. Откроется страница с разделом **Сведения о программе**, в котором в поле **Агенты с уязвимостью** можно просмотреть все хосты с установленными агентами, на которых обнаружена программа.

4.11.3. Изучение сведений об уязвимости

С помощью модуля сканирования уязвимостей аналитик может изучить подробную информацию о найденной уязвимости и определить способы нейтрализации этой уязвимости. Для этого на странице **Сведения об уязвимости** публикуется ее описание на английском языке, а также описание на русском языке, если указанная уязвимость присутствует в БДУ ФСТЭК. Кроме того, на странице публикуется информация о базовых метриках, описанных по стандартам CVSS 3.x и CVSS 2.0.

CVSS – это общая система оценки уязвимостей, которая позволяет сравнивать уязвимости программного обеспечения с точки зрения их опасности. Базовые метрики описывают характеристики

уязвимости, не меняющиеся с течением времени и не зависящие от контекста, то есть среды исполнения (например, вид операционной системы, в которой выполняется программа).

В зависимости от времени публикации информация по той или иной версии CVSS в сведениях об уязвимости может отсутствовать.

Базовые метрики, отображаемые на странице **Сведения об уязвимости** и их возможные значения представлены в таблице 4.

Таблица 4 – Базовые метрики уязвимостей

Стандарт	Метрики	Описание	Значения метрики
CVSS 3.x	Вектор атаки (AV)	Показывает удаленность потенциального атакующего от уязвимого объекта	Сетевой (N)
			Смежная сеть (A)
			Локальный (L) (атакующему требуется локальная сессия)
			Физический (P) (атакующему требуется физический доступ к уязвимой системе)
	Сложность атаки (AC)	В зависимости от количества условий для проведения атаки, ее сложность увеличивается (чем больше условий, тем выше сложность)	Высокая (H)
			Низкая (L)
	Уровень привилегий (PR)	Показывает, требуется ли аутентификация для атаки, и если требуется, то какая	Высокий (H)
			Низкий (L)
			Не требуется (N)
	Взаимодействие с пользователем (UI)	Требуется ли действия со стороны пользователей атакуемой системы	Требуется (R)
			Не требуется (N)
	Влияние на другие компоненты системы (S)	Оказывает ли влияние атакуемая подсистема на другие компоненты	Не оказывает (U)
			Оказывает (C)
	Влияние на конфиденциальность (C)		Не оказывает (N)
			Низкое (L)
			Высокое (H)

	Влияние на целостность (I)	Влияние на надежность и гарантированную правдивость информации	Не оказывает (N)
			Низкое (L)
			Высокое (H)
	Влияние на доступность (A)	Имеется в виду влияние на легкость доступа к информационным ресурсам	Не оказывает (N)
			Низкое (L)
			Высокое (H)
CVSS 2.0	Способ получения доступа (AV)	Удаленность атакующего от уязвимого объекта	Сетевой (N)
			Смежная сеть (A)
			Локальный (L) (любые действия, не затрагивающие сеть)
	Сложность получения доступа (AC)	Метрика показывает сложность атаки, которая позволяет эксплуатировать уязвимость при получении доступа к атакуемой системе	Высокая (H)
			Средняя (M)
			Низкая (L)
	Аутентификация (Au)	Метрика показывает количество раз, которое злоумышленник должен аутентифицироваться, чтобы эксплуатировать уязвимость	Множественная (M)
			Единственная (S)
			Не требуется (N)
	Влияние на конфиденциальность (C)		Не оказывает (N)
			Частичное (P)
			Полное (C)
	Влияние на целостность (I)	Влияние на надежность и гарантированную правдивость информации	Не оказывает (N)
			Частичное (P)
			Полное (C)
	Влияние на доступность (A)	Имеется в виду влияние на легкость доступа к информационным ресурсам	Не оказывает (N)
			Частичное (P)
			Полное (C)

Для уточнения значения метрик дополнительно можно использовать временные и контекстные метрики, которые позволяют учитывать отличные от базовых факторов. Для подобной работы можно

использовать калькулятор БДУ ФСТЭК, ссылка на который содержится на странице с уязвимостью (кнопка  в строке **Вектор атаки**).

4.12 Просмотр исключений

Оператор поиска угроз не обладает правами для операций с исключениями. Для него доступны следующие действия:

- 1) Просмотр наборов исключений для программ;
- 2) Просмотр списка исключений для программ выбранного набора;
- 3) Просмотр наборов исключений для файлов;
- 4) Просмотр списка исключений для файлов выбранного набора;
- 5) Просмотр наборов сетевых исключений;
- 6) Просмотр списка сетевых исключений выбранного набора;
- 7) Просмотр наборов исключений для индикаторов атак;
- 8) Просмотр списка исключений для индикаторов атак у выбранного набора.

Чтобы оператору просмотреть исключение для программы, ему необходимо перейти на страницу **Наборы исключений для программ** (рис. 27). Для перехода к странице следует выбрать на панели управления раздел **Исключения для программ** ( **Исключения для программ**).

Здесь содержатся наборы с правилами, в каждом из них может быть множество исключений.

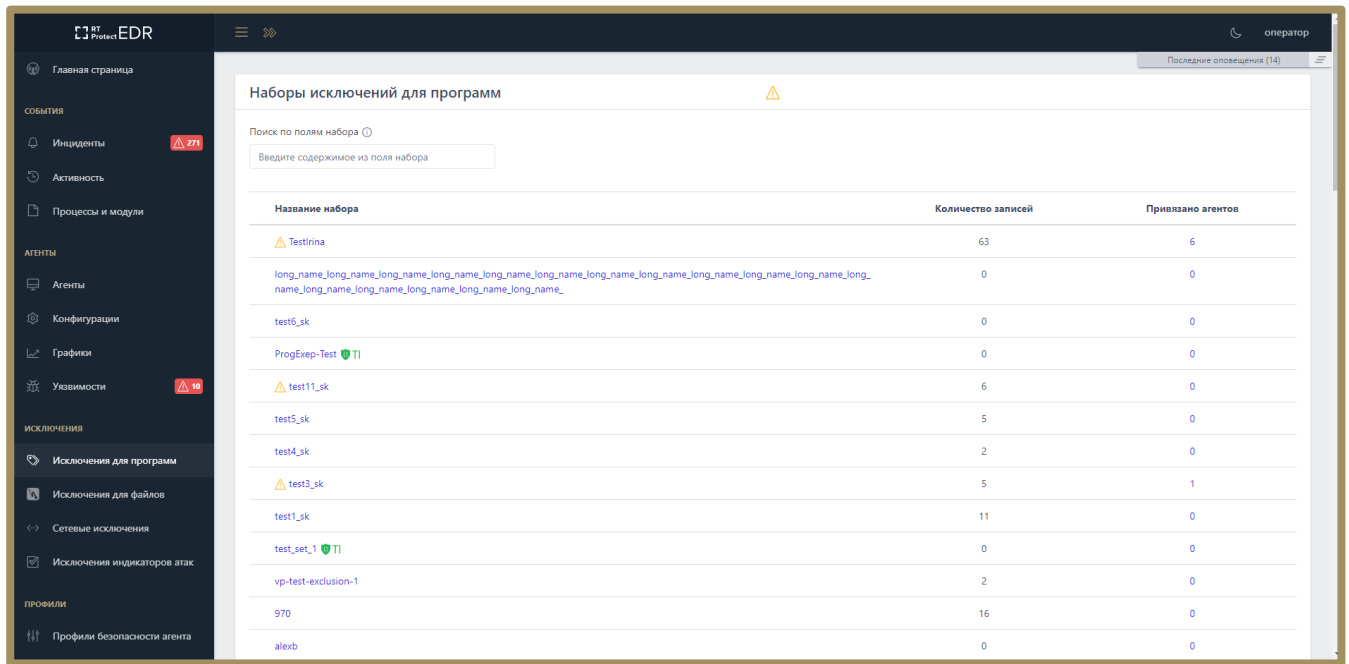


Рисунок 27 – Наборы исключений для программ

Информация на странице **Наборы исключений для программ** представлена в табличном виде.

Таблица с наборами содержит следующие поля:

- 1) Название набора;
- 2) Количество записей;
- 3) Привязано агентов;
- 4) Управление.

Часть наборов содержат значки о том, что они получены с TI-портала, наведение курсора мыши на эти значки позволит прочитать информацию о выбранных наборах. Значок  говорит о том, что набор успешно синхронизируется с TI-порталом, значок  показывает, что набор с портала уже удален. Кроме указанных выше значков название может содержать значок , показывающий, что набор еще не применен.

Переход на страницу **Исключения для программы** происходит при нажатии ЛКМ на имени набора.

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

- 1) Тип (показывает один из трех типов исключения для программ: файл, хеш или командная строка);
- 2) Значение;
- 3) Флаги (могут выводиться различные флаги, управляющие особенностями исполнения программ):
 - разрешить внедрение кода в сторонние программы;

- разрешить запись памяти сторонних программ;
- разрешить доступ к сторонним программам для чтения памяти и управления;
- право взаимодействия с критическими системными программами;
- разрешить прямой доступ к диску для чтения и др.;

4) Издатель ЭП;

5) Правила;

6) Комментарий;

7) Дата создания/Автор;

8) Последнее изменение/Пользователь;

9) Управление.

Просмотр исключений для файлов, сетевых исключений, а также исключений для индикаторов атак происходит таким же образом, как и просмотр исключений для программ.

4.13 Просмотр профилей безопасности агента

На странице **Профили безопасности агента** оператор поиска угроз может просматривать настройки параметров безопасности агента. В соответствии с этими параметрами формируются события и инциденты, присылаемые агентом в модуль администрирования (рис. 28). Профили безопасности позволяют настраивать нагрузку на систему, увеличивая или уменьшая поток событий, регистрируемых на агенте. Оператору не предоставляется возможность управлять профилями безопасности.

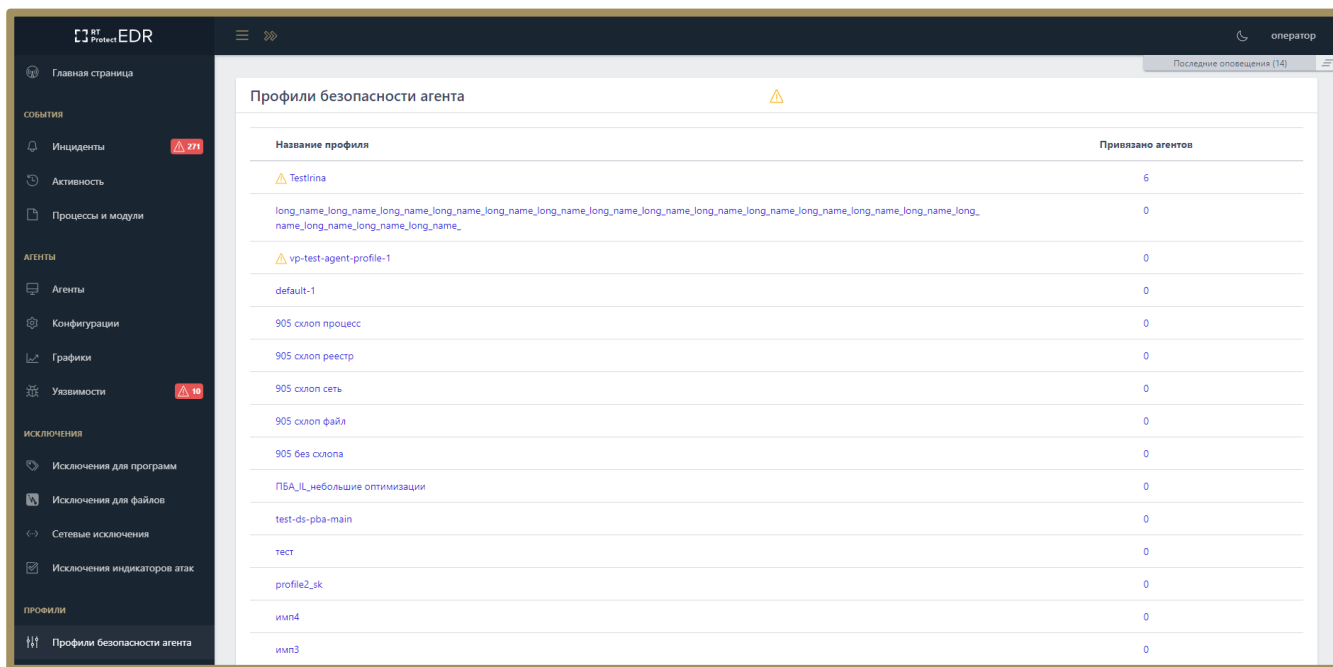


Рисунок 28 – Профили безопасности агента

Информация на странице **Профили безопасности агента** представлена в табличном виде. Таблица содержит следующие поля:

- 1) Название профиля;
- 2) Привязано агентов.

Чтобы перейти на страницу с установленными параметрами профиля необходимо нажать ЛКМ на имя профиля. Информация на странице **Профиль безопасности агента** распределена по следующим областям:

- 1) Оптимизация потока событий;
- 2) Общие настройки безопасности;
- 3) Настройки безопасности монитора процессов;
- 4) Настройки безопасности файлового монитора;
- 5) Настройки безопасности сетевого монитора;
- 6) Настройки безопасности монитора реестра.

В области **Оптимизация потока событий** оператор может просмотреть, какие флаги, позволяющие снизить поток событий с агентов на сервер управления, установлены для выбранного профиля.

В области **Общие настройки безопасности** отображается, включен или нет режим «только детектирование», при котором на агенте отключается противодействие угрозам в режиме реального времени.

В области **Настройки безопасности монитора процессов** оператор может просмотреть, какие реакции запланированы на создание нити в стороннем процессе (кроме авторизованных программ Windows), а также на доступ к стороннему процессу/нити (кроме авторизованных программ Windows). Доступно три реакции:

- блокировать;
- блокировать только для неподписанных программ;
- разрешить.

В области **Настройки безопасности файлового монитора** оператор может увидеть, какая реакция настроена на прямой доступ к жесткому диску (кроме авторизованных программ Windows), а также какой режим глубокого сканирования файлов выбран для профиля безопасности агента. Кроме того, в настройках отображается, подсчитывается или нет хеш SHA-1 и MD5 для выбранного профиля.

В настройках безопасности сетевого монитора и монитора реестра оператор может увидеть, установлены ли для выбранного профиля флаги оптимизации потока сетевых событий и событий реестра соответственно.

На странице **Профиль безопасности агента** оператор может увидеть, кто и когда создал выбранный профиль, а также, кто и когда сделал в нем последние изменения.

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

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

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

5. Модель данных, обнаруживаемых агентом

5.1 Общие сведения

Данные, собранные агентом, отправляются на сервер в формате JSON. Отправка данных с агента осуществляется блоками. Каждый блок содержит заголовок и массив событий разного типа. Каждое событие включает в себя 2 набора полей – общий набор и набор, специфичный для определенного вида события. Полный общий список данных и их JSON-представления, которые могут быть применены для написания DSL-запросов, представлен в таблице 5.

Таблица 5 – Общий список полей событий

Назначение	Тип данных	JSON	Подсистема
Тип события	enum	t	Общая
Время регистрации события	timestamp	time	Общая
Действие, связанное с событием	enum	act	Общая
Причина предпринятого действия	enum	rsn	Общая
Правило, относящееся к событию	string	rul	Общая
Идентификатор техники/тактики MITRE	string	mitre	Общая
Критичность (уровень важности) события	enum	svrt (по умолчанию: 0)	Общая
Уникальный идентификатор процесса	int (индекс в массиве GUID'ов)	uuid	Общая
Уникальный идентификатор группы процессов	int (индекс в массиве GUID'ов)	hid	Общая
Уникальный идентификатор корреляции событий	string (индекс в массиве GUID'ов)	cid	Общая
Идентификатор процесса на агентской системе	unsigned	pid	Общая
Идентификатор родительского процесса на агентской системе	unsigned	ppid	Общая
Полное имя исполняемого файла процесса	string MANGLED	app	Общая
Командная строка процесса	string	cmdl	Общая
Номер сессии, в которой работает процесс на агентской системе	unsigned	sess (по умолчанию: 0)	Общая
SID пользователя, создавшего процесс	string	sid	Общая
Издатель ЭП исполняемого файла процесса	string	app_sgnr	Общая
Имя пользователя, запустившего процесс	string	usr	Общая
Домен (имя компьютера) пользователя, запустившего процесс	string	dom	Общая
Подтип события	enum	st	Общая
Поведенческие признаки процесса (первая группа)	uint64	rf0	Общая

Назначение	Тип данных	JSON	Подсистема
Поведенческие признаки процесса (вторая группа)	uint64	rf1	Общая
Флаги исполняемого файла процесса	int64	exclf	Общая
Синтетическое событие	int (0/1)	syn	Общая
Версия события	unsigned	efmt	Общая
Протокол	enum	proto	Сеть
Признак работы по IPv6	int (0/1)	ipv6	Сеть
Уникальный идентификатор сетевого потока	string (индекс в массиве GUID'ов в текстовой форме)	fluid	Сеть
Идентификатор сетевого потока	int64	flow	Сеть
Отправка или прием	int (0/1)	out	Сеть
Размер полезных данных (payload) сетевого пакета	int64	size	Сеть
Имя хоста, соответствующее удаленному IP-адресу	string	host	Сеть
Тип DNS-запроса	enum	dnsq_t	Сеть
Статус DNS-запроса	unsigned	dnsq_s	Сеть
Результат DNS-запроса	string	dnsq_r	Сеть
Имя хоста из DNS-запроса	string	dnsq_h	Сеть
Имя хоста (server_name) из сообщения SSL Client Hello	string	ssl_h	Сеть
Удаленный IP-адрес	string	r_ip	Сеть
Удаленный порт	unsigned	r_p	Сеть
Локальный IP-адрес	string	l_ip	Сеть
Локальный порт	unsigned	l_p	Сеть
Имя хоста в индикаторе компрометации	string	ioc_h	Сеть
Флаги сетевого события	unsigned	netf	Сеть
Имя хоста в сетевом исключении	string	excl_h	Сеть
Полное имя файла	string MANGLED	name	Файлы, Защита данных
Время создания файла	timestamp	crttime	Файлы, Процессы
Время последнего изменения файла	timestamp	chtime	Файлы, Процессы
Размер файла	int64	fsize	Файлы, Процессы
Тип файла	enum	ftype	Файлы, Процессы
Атрибуты файла	unsigned	attr	Файлы, Процессы
SHA-1 файла	string	sha1	Файлы, Процессы
MD5 файла	string	md5	Файлы, Процессы
SHA-256 файла	string	sha256	Файлы, Процессы
Электронная подпись файла	string	sgnr	Файлы,

Назначение	Тип данных	JSON	Подсистема
			Процессы
Статус электронной подписи файла	enum	sgnr_s	Файлы, Процессы
Оригинальное имя файла	string	ofn	Файлы, Процессы
Компания-издатель файла	string	fcomp	Файлы, Процессы
Версия файла	string	fver	Файлы, Процессы
Описание файла	string	fdesc	Файлы, Процессы
Продукт, к которому относится файл	string	fprod	Файлы, Процессы
Тип упаковщика файла	string	pack	Файлы, Процессы
Файл расположен в директории автозапуска	int (0/1)	arun	Файлы
Новое имя файла	string MANGLED	fnew	Файлы
Файл был заменен	int (0/1)	owrt	Файлы
Предыдущее время создания файла	timestamp	old_t	Файлы
Новое время создания файла	timestamp	new_t	Файлы
Файл содержит атрибут "скрытый"	int (0/1)	hdn	Файлы
Файл содержит атрибут "системный"	int (0/1)	sys	Файлы
Операция совершается над альтернативным потоком данных файла	int (-/1)	ads	Файлы
Для файла была создана резервная копия	int (-/1)	save	Файлы
Доступ на удаление	int (-/1)	delete	Файлы
Доступ на чтение	int (-/1)	read	Файлы
Доступ на модификацию	int (-/1)	modify	Файлы
Код оповещения	enum	detect	Сеть, Файлы, Процессы, Реестр
Полное имя исполняемого модуля–инициатора операции	string MANGLED	who	Файлы, Процессы, Реестр
Идентификатор нити–инициатора операции	unsigned	whotid	Файлы, Процессы, Реестр
Стартовый адрес нити–инициатора операции	uint64	whoaddr	Файлы, Процессы, Реестр
Флаги исполняемого модуля-инициатора операции	uint64	whof	Файлы, Процессы, Реестр
Стек вызовов операции	string	trace	Процессы
Командная строка родительского процесса	string	cmdlp	Процессы

Назначение	Тип данных	JSON	Подсистема
Командная строка прародителя (grand parent)	string	cmdlg	Процессы
Рабочий каталог процесса	string MANGLED	wdir	Процессы
Уровень защиты процесса	unsigned	prot	Процессы
Уровень доверия (integrity level) процесса	unsigned	integ	Процессы
Время создания процесса	timestamp	when	Процессы
Уникальный идентификатор родительского процесса	int (индекс в массиве GUID'ов)	parent	Процессы
Уникальный идентификатор процесса-создателя	int (индекс в массиве GUID'ов)	caller	Процессы
Идентификатор процесса-инициатора операции	unsigned	cpid	Процессы
Полное имя процесса-инициатора операции	string MANGLED	cpath	Процессы
Код завершения процесса	unsigned	code	Процессы
Уникальный идентификатор целевого процесса	int (индекс в массиве GUID'ов)	targ	Процессы
Полное имя целевого процесса	string MANGLED	tpath	Процессы
Идентификатор целевого процесса	unsigned	tpid	Процессы
Флаги образа целевого процесса	uint64	targf	Процессы
Поведенческие признаки целевого процесса (первая группа)	uint64	trf0	Процессы
Поведенческие признаки целевого процесса (вторая группа)	uint64	trf1	Процессы
Имя модуля целевой нити	string	tmod	Процессы
Имя функции целевой нити	string	tfunc	Процессы
Полное имя файла образа	string MANGLED	path	Процессы
Флаги нити	unsigned	tf	Процессы
Флаги операции загрузки образа	unsigned	ldf	Процессы
Флаги образа	int64	imgf	Процессы
Базовый адрес образа	int64	base	Процессы
Размер образа	unsigned	isize	Процессы
Идентификатор целевой нити	unsigned	tid	Процессы
Стартовый адрес целевой нити	int64	taddr	Процессы
Запрашиваемые права	unsigned	dsrd	Процессы
Предоставленные права	unsigned	grnt	Процессы
Новый уровень защиты процесса	int	prot1	Процессы
Новая командная строка	string	cmdl1	Процессы
Локальная сессия	int (0/1)	local	Сессии
Номер сессии	unsigned	sess_id	Сессии
Тип дистанционного управления	unsigned (опционально)	sess_opt	Сессии
Тип сессии	unsigned (опционально)	sess_proto	Сессии
Имя оконной станции	string	win_stn	Сессии
Имя клиента	string (опционально)	sess_cl	Сессии
IP-адрес клиента	string (опционально)	sess_claddr	Сессии
Имя пользователя	string (опционально)	sess_usr	Сессии
Имя домена\компьютера	string (опционально)	sess_dom	Сессии
Путь ключа	string	key	Реестр

Назначение	Тип данных	JSON	Подсистема
Имя значения	string	val_n	Регистр
Тип данных значения	enum	val_t	Регистр
Размер данных значения	unsigned	val_s	Регистр
Данные значения	string	val_d	Регистр
Новое имя ключа	string	new	Регистр
Имя файла-источника загружаемой в регистр информации	string MANGLED	src	Регистр
Имя файла, в который записываются данные из регистра	string MANGLED	dst	Регистр
Ключ/значение относится к категории автозапуска	int (-/1)	asep	Регистр
WMI: Тип события	enum	wmi	Система: WMI
WMI: Путь	string	wmi_pth	Система: WMI
WMI: SID пользователя	string	wmi_sid	Система: WMI
WMI: Пространство имен	string	ns	Система: WMI
WMI: Путь до исполняемого файла	string MANGLED	exe_path	Система: WMI
WMI: Имя файла	string MANGLED	fname	Система: WMI
WMI: Имя фильтра событий	string	wmi_nm	Система: WMI
WMI: Строка запроса	string	qstr	Система: WMI
WMI: Имя файла скрипта	string MANGLED	scrfname	Система: WMI
WMI: Текст скрипта	string	scrtxt	Система: WMI
WMI: Имя источника	string MANGLED	sname	Система: WMI
WMI: SMTP	string	smtp	Система: WMI
WMI: Фильтр	string	flt	Система: WMI
WMI: Потребитель	string	cnsn	Система: WMI
WMI: Идентификатор процесса клиента	unsigned (по умолчанию 0)	wmi_clpid	Система: WMI
WMI: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	wmi_cluuid	Система: WMI
WMI: Время создания процесса клиента	timestamp	wmi_cltime	Система: WMI
WMI: Командная строка процесса клиента	string	wmi_clcmdl	Система: WMI
WMI: Локальный запрос	int (-/1)	wmi_local	Система: WMI
WMI: Идентификатор созданного процесса	unsigned	wmi_crpuid	Система: WMI
WMI: Уникальный идентификатор созданного процесса	int (индекс в массиве GUID'ов)	wmi_cruuid	Система: WMI
WMI: Время создания созданного процесса	timestamp	wmi_crtime	Система: WMI
WMI: Командная строка созданного процесса	string	wmi_crcmdl	Система: WMI
WMI: Имя машины, выполнившей запрос	string	wmi_cl	Система: WMI
WMI: FQDN машины, выполнившей запрос	string	wmi_clfqdn	Система: WMI
WMI: Имя пользователя клиента, выполнившего запрос	string	wmi_usr	Система: WMI
WMI: Имя домена клиента, выполнившего запрос	string	wmi_dom	Система: WMI
WMI: Имя вызываемого метода	string	wmi_mthd	Система: WMI
Атаки на Kerberos: Подтип атаки	enum	atck	Система: Атаки на Kerberos

Назначение	Тип данных	JSON	Подсистема
Golden ticket: Причина	enum	goldent_r	Система: Атаки на Kerberos
Golden ticket: Имя пользователя	string	goldent_u	Система: Атаки на Kerberos
Golden ticket: Имя домена	string	goldent_d	Система: Атаки на Kerberos
Golden ticket: IP-адрес	string	goldent_ip	Система: Атаки на Kerberos
Silver ticket: Причина	enum	silvert_r	Система: Атаки на Kerberos
Silver ticket: Имя пользователя	string	silvert_u	Система: Атаки на Kerberos
Silver ticket: Имя домена	string	silvert_d	Система: Атаки на Kerberos
Silver ticket: IP-адрес	string	silvert_ip	Система: Атаки на Kerberos
Kerberoasting: Причина	enum	kerberoasting_r	Система: Атаки на Kerberos
Kerberoasting: Имя пользователя	string	kerberoasting_u	Система: Атаки на Kerberos
Kerberoasting: Имя домена	string	kerberoasting_d	Система: Атаки на Kerberos
Kerberoasting: IP-адрес	string	kerberoasting_ip	Система: Атаки на Kerberos
AS-REP roasting: Причина	enum	asreproasting_r	Система: Атаки на Kerberos
AS-REP roasting: Имя пользователя	string	asreproasting_u	Система: Атаки на Kerberos
AS-REP roasting: Имя домена	string	asreproasting_d	Система: Атаки на Kerberos
AS-REP roasting: IP-адрес	string	asreproasting_ip	Система: Атаки на Kerberos
Новое время	timestamp	new_time	Система: Изменение системного времени
Предыдущее время	timestamp	prev_time	Система: Изменение системного времени
Причина завершения	unsigned	sht	Система: Завершение работы
Уровень	unsigned	e_lvl	Журналы
Дополнительные данные	JSON object	e_ex	Журналы
Описание событий	string (опционально)	e_msg	Журналы
Блок информации winlogbeat	JSON object	winlog	Журналы

Назначение	Тип данных	JSON	Подсистема
RPC: UUID интерфейса	int (индекс в массиве GUID'ов)	rpc_id	Вызовы: RPC
RPC: Конечная точка	string	endp	Вызовы: RPC
RPC: Сетевой адрес	string (опционально)	n_addr	Вызовы: RPC
RPC: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	c_uuid	Вызовы: RPC
RPC: PID процесса клиента	unsigned	c_pid	Вызовы: RPC
RPC: Исполняемый файл процесса клиента	string MANGLED	c_path	Вызовы: RPC
RPC: Уникальный идентификатор процесса сервера	int (индекс в массиве GUID'ов)	s_uuid	Вызовы: RPC
RPC: PID процесса сервера	unsigned	s_pid	Вызовы: RPC
RPC: Исполняемый файл процесса сервера	string MANGLED	s_path	Вызовы: RPC
Количество открытий/созданий файлов с последующими обращениями к ним	unsigned	cf_ac	Защита файлов
Количество открытых файлов из защищаемых каталогов	unsigned	cf_oc	Защита файлов
Количество созданных процессом файлов после активации мониторинга	unsigned	cf_cc	Защита файлов
Количество удалённых файлов в защищаемых каталогах	unsigned	si_dc	Защита файлов
Количество переименованных файлов в защищаемых каталогах	unsigned	si_rc	Защита файлов
Количество перемещённых файлов в защищаемые каталоги	unsigned	si_mi	Защита файлов
Количество перемещённых файлов из защищаемых каталогов	unsigned	si_mo	Защита файлов
Количество файлов из защищаемых каталогов, которые только читали	unsigned	ro_fc	Защита файлов
Количество файлов из защищаемых каталогов, в которые только писали	unsigned	wo_fc	Защита файлов
Количество файлов из защищаемых каталогов, которые читали и писали	unsigned	rw_fc	Защита файлов
Среднее значений файловой энтропии по чтению	unsigned	pr_re	Защита файлов
Среднее значений файловой энтропии по записи	unsigned	pr_we	Защита файлов
Правило блокировки процесса	unsigned	pr_lr	Защита файлов
Реакция модуля на идентификацию шифровальщика	unsigned	pr_ra	Защита файлов
Количество файлов с нарушенной целостностью	unsigned	a_fcc	Защита файлов
Количество файлов с превышенной энтропией	unsigned	a_eoc	Защита файлов
Количество расширений файлов из которых читали	unsigned	extrac_	Защита файлов
Количество расширений файлов в которые писали	unsigned	exwac_	Защита файлов

Назначение	Тип данных	JSON	Подсистема
Количество уникальных расширений файлов из которых только читали	unsigned	exurac	Защита файлов
Количество уникальных расширений файлов в которые только писали	unsigned	exuwac	Защита файлов
Категории файлов, к которым осуществлялся доступ	unsigned	gf_am	Защита файлов
Категории файлов, из которых производилось чтение	unsigned	gf_rm	Защита файлов
Категории файлов, в которые производилось запись	unsigned	gf_wm	Защита файлов
Категории файлов, которые удалялись	unsigned	gf_dm	Защита файлов
Группа, к которой относится файл	unsigned	gf_ai	Защита файлов

Типы событий представлены в таблице 6.

Таблица 6 – Типы событий (t)

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

Поля общей части событий представлены в таблице 7.

Таблица 7 – Поля общей части событий

Назначение	JSON
Тип события	t
Время регистрации события (в формате UTC)	time
Действие, связанное с событием (0 – заблокировать, 1 – разрешить, 2 – продолжить наблюдение)	act (по умолчанию – 2)
Причина предпринятого действия	rsn (опционально)
Правило, относящееся к событию	rul (опционально)
Идентификатор техники/тактики MITRE	mitre (опционально)

Критичность (уровень важности) события	svrt (по умолчанию – 0)
Уникальный идентификатор процесса	uuid
Идентификатор процесса на агентской системе	pid
Идентификатор родительского процесса на агентской системе	ppid (опционально)
Полное имя (вместе с путем) исполняемого модуля процесса	app
Номер сессии, в которой работает процесс на агентской системе	sess (по умолчанию – 0)
Имя пользователя, запустившего процесс	usr
Домен (имя компьютера) пользователя, запустившего процесс	dom
Подтип события (интерпретируется в зависимости от типа)	st
Поведенческие признаки процесса (первая группа)	rf0 (опционально)
Поведенческие признаки процесса (вторая группа)	rf1 (опционально)
Совокупная маска доступа процесса к нитям сторонних процессов в системе	ta (опционально)
Совокупная маска доступа процесса к сторонним процессам в системе	pa (опционально)
Флаги исполняемого файла процесса	exclf (опционально)

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

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

Критичность события может принимать следующие значения:

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



Примечание

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

В поле **act** (action) передается действие, предпринятое в связи с событием. Это может быть одно из 3 значений:

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

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

MORE_PROCESSING (код 2, значение по умолчанию, т.е. непосредственно в теле события этот код не передается) – трактуется по-разному в зависимости от контекста. В контексте события телеметрии означает, что никакого действия, связанного с событием, не предпринято. В контексте обнаружения (alert) код 2 означает, что логика обнаружения не предписывает никакого действия, кроме фиксации самого факта обнаружения – обнаруженная активность не блокируется, что не отменяет самого факта ее обнаружения.



Примечание

Для события телеметрии поля **rsn** и **rul**, как правило (но необязательно), не заполняются, а для события-обнаружения поле **rul** содержит правило, идентифицирующее обнаружение. И тогда поле **rsn**, как и в других случаях, содержит причину, по которой установлена такая реакция на обнаружение.

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

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

Поля **rf0**, **rf1**, **ta** и **pa** определяют поведенческий профиль процесса. Поле **rf0** – это runtime-флаги процесса (первая группа); **rf1** – runtime-флаги процесса (вторая группа); **ta** – совокупная маска доступа, с которой процесс пытался получить доступ к нитям других процессов; **pa** – совокупная маска доступа, с которой процесс пытался получить доступ к другим сторонним процессам.

Runtime-флаги (**rf0**, **rf1**, **pa**, **ta**) процесса составляют его поведенческий профиль и могут меняться от события к событию сообразно с поведением процесса в системе. Флаги в явном виде не отображаются, а используются при формировании удобочитаемого представления профиля поведения процесса.

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

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

5.2 События монитора сети

Подтипы событий (**st**) и их текстовые описания представлены в таблице 8.

Таблица 8 – События монитора сети

Код события	Имя события	Описание
0	Сеть: Исходящее подключение	Исходящее подключение к remote_endpoint (удаленному хосту) по proto

1	Сеть: Входящее подключение	Входящее подключение от remote_endpoint (удаленного хоста) по proto
2	Сеть: Отправка	Отправка size байт на remote_endpoint (удаленный хост) по proto
3	Сеть: Прием	Прием size байт от remote_endpoint (удаленного хоста) по proto
5	Сеть: DNS запрос	DNS-запрос dnsq_t к remote_endpoint (удаленному хосту) на имя dnsq_h размером size байт
6	Сеть: SSL HELLO	Запрос SSL HELLO (ssl_h) с remote_endpoint (удаленного хоста) размером size байт
7	Сеть: Оповещение	Расшифровка кода detect
8	Сеть: Обнаружение: срабатывание индикатора компрометации	Срабатывание индикатора компрометации при сетевом взаимодействии с remote_endpoint (удаленным хостом)
10	Сеть: Открытие локального порта на прием	Открытие локального порта l_p на прием

Поля сетевых событий представлены в таблице 9.

Таблица 9 – Поля сетевых событий

Назначение	JSON
Номер протокола 6 – TCP, 17 – UDP, 1 – ICMP, 58 – ICMPv6	proto
Признак работы по IPv6 (принимает значения true или false)	ipv6
Идентификатор сетевого потока (служебное значение, позволяет группировать события, относящиеся к одному сетевому потоку)	flow
Отправка (1) или прием (0)	out
Размер полезных данных (payload) сетевого пакета	size
Имя хоста, соответствующее удаленному ip	host
Тип DNS запроса: 0x1 – A, 0x5 – CNAME, 0x1C – AAAA, 0x0F – MX, 0x21 – SRV. Остальные типы запросов выводятся кодом (2 байта), пример: 0x0002	dnsq_t
Имя хоста из DNS-запроса	dnsq_h
Имя хоста (server_name) из SSL Client Hello сообщения	ssl_h
Удаленный IP-адрес	r_ip
Удаленный порт	r_p
Локальный IP-адрес	l_ip
Локальный порт	l_p
Код обнаружения	detect

5.3 События монитора файловых операций

Подтипы событий (**st**) монитора файловых операций и их текстовые описания представлены в таблице 10.

Таблица 10 – События монитора файловых операций

Код события	Имя события	Описание
0	Файлы: Создан новый файл	Создан новый файл name
1	Файлы: Файл переименован	Файл name переименован в fnew
2	Файлы: Удален файл	Удален файл name
3	Файлы: У файла изменен атрибут или время создания	У файла name [установлен/снят атрибут "системный" (если присутствует sys , sys = 0 – снят, sys = 1 – установлен)], [установлен атрибут "скрытый" (если присутствует hdn)], [изменено время создания с old_t на new_t (если присутствуют old_t и new_t)]
4	Файлы: Другие обнаружения	<расшифровка кода detect > (см. ниже)
7	Файлы: Файл был модифицирован	Файл name был модифицирован
8	Файлы: Файл был прочитан	Файл name был прочитан
12	Файлы: прямой доступ к тому на чтение	Прямой доступ к диску (тому) name на чтение
13	Файлы: Прямой доступ к тому на запись	Прямой доступ к диску (тому) name на запись
14	Файлы: Создан именованный канал	Создан именованный канал name
15	Файлы: Подключение к именованному каналу	Подключение к именованному каналу name
16	Файлы: Доступ к файлу	Доступ к файлу name
17	Файлы: срабатывание индикатора компрометации для файла	Срабатывание индикатора компрометации для файла name
18	Файлы: Срабатывание исключения для файла	Срабатывание исключения для файла name
19	Файлы: Файл классифицирован как вредоносный (ML на агенте)	Файл name классифицирован как вредоносный (ML на агенте)
20	Файлы: Файл классифицирован как вредоносный (Yara-правила)	Файл name классифицирован как вредоносный (Yara-правила)
21	Файлы: Подмена образа процесса в памяти	Подмена образа процесса в памяти: HERPADERPING (имя образа: name)

Поля событий монитора файловой системы представлены в таблице 11.

Таблица 11 – Поля событий монитора файловой системы

Назначение	JSON	Тип
Полное имя исполняемого модуля-инициатора операции	who	string MANGLED
Идентификатор нити-инициатора операции	whotid	unsigned
Стартовый адрес нити-инициатора операции	whoaddr	uint64
Флаги исполняемого модуля-инициатора операции	whof	uint64
Стек вызовов операции	trace	string
Полное имя файла	name	string MANGLED
Время создания файла	crttime	timestamp
Время последнего изменения файла	chtime	timestamp

Размер файла	fsize	int64
Тип файла	ftype	enum
Атрибуты файла	attr	unsigned
SHA-1 файла	sha1	string
MD5 файла	md5	string
SHA-256 файла	sha256	string
Электронная подпись файла	sgnr	string
Статус электронной подписи файла	sgnr_s	enum
Оригинальное имя файла	ofn	string
Компания-издатель файла	fcomp	string
Версия файла	fver	string
Описание файла	fdesc	string
Продукт, к которому относится файл	fprod	string
Файл находится в белом списке	fwhite	int (-/1)
Тип упаковщика файла	pack	string
Файл расположен в директории автозапуска	arun	int (-/1)
Новое имя файла	fnew	string MANGLED
Файл был заменен	owrt	int (-/1)
Время создания файла до изменения атрибутов	old_t	timestamp
Время создания файла после изменения атрибутов	new_t	timestamp
Файл содержит атрибут "скрытый"	hdn	int (0/1)
Файл содержит атрибут "системный"	sys	int (0/1)
Операция совершается над альтернативным потоком данных файла	ads	int (-/1)
Для удаляемого файла была создана резервная копия	save	int (-/1)
Код обнаружения	detect	unsigned
Доступ на удаление	delete	int (-/1)
Доступ на чтение	read	int (-/1)
Доступ на модификацию	modify	int (-/1)
Обмен именами (доступен только в Linux)	nxchg	int (-/1)

Поля **hdn**, **arun**, **owrt**, **sys**, **ads**, и **save** могут принимать только значения **true** или **false**.

Поле **ftype** принимает следующие значения, представленные в таблице 12.

Таблица 12 – Значение поля ftype

Значение	Описание
2	PE
3	Active content
4	PowerShell script

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

Список всех возможных атрибутов файлов для ОС Windows содержится в [документации](#) Microsoft.

5.4 События монитора реестра

Подтипы событий (**st**) монитора реестра и их текстовые описания представлены в таблице 13.

Таблица 13 – Подтипы событий монитора реестра

Код события	Имя события	Описание
0	Реестр: Создан новый ключ	Создан новый ключ key
1	Реестр: Удален ключ	Удален ключ key
2	Реестр: в значение ключа записаны данные	В значение val_n ключа key записаны данные val_d (тип: val_t , размер: val_s)
3	Реестр: Удалено значение ключа	Удалено значение val_n ключа key
4	Реестр: Ключ переименован	Ключ key переименован в new
5	Реестр: Ключ восстановлен из файла	Ключ key восстановлен из файла src
6	Реестр: Данные ключа заменены файлом	Данные ключа key заменены файлом src , предыдущее состояние сохранено в dst
7	Реестр: Другие обнаружения	Расшифровка поля detect

Поля событий монитора реестра представлены в таблице 14.

Таблица 14 – Поля событий монитора реестра

Назначение	JSON
Путь до исполняемого модуля-инициатора операции	who
Идентификатор нити-инициатора операции	whotid
Стартовый адрес нити-инициатора операции	whoaddr
Флаги исполняемого модуля-инициатора операции	whof
Стек вызовов операции	trace
Путь ключа реестра	key
Имя значения	val_n
Тип данных значения: 1 – REG_SZ; 2 – REG_EXPAND_SZ; 3 – REG_BINARY; 4 – REG_DWORD; 5 – REG_DWORD_BE; 6 – REG_LINK; 7 – REG_MULTI_SZ; 8 – REG_RES_LIST; 9 – REG_FULL_RES_DESC; 10 – REG_RES_REQ_LIST; 11 – REG_QWORD	val_t
Размер данных значения	val_s
Данные значения	val_d
Новое имя ключа	new

Имя файла-источника загружаемой в реестр информации	src
Ключ/значение относится к категории автозапуска	asep
Код обнаружения	detect

Поле **asep** принимает значение только **true** или **false**.

5.5 События системного журнала Windows (ETW)

Подтипы событий и их текстовые описания представлены в таблице 15.

Таблица 15 – Подтипы событий системного журнала Windows

Назначение	JSON
Подтип события (всегда = 0)	st
Уровень (возможно значение: Критическая ошибка = 1, Ошибка = 2, Предупреждение = 3, Информация = 4, Подробно = 0 или 5)	e_lvl
Дополнительные данные (выводятся в поле карточки событий в JSON-формате)	e_ex
Описание события	e_msg
Событие в формате winlogbeat (см. winlogbeat)	winlog

События формата winlogbeat могут принимать значения, представленные в таблице 16.

Таблица 16 – События winlogbeat

Поле	Тип	Расшифровка
winlog.api	keyword	Тип API
winlog.event_id	keyword	Идентификатор события
winlog.activity_id	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор действия
winlog.related_activity_id	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор действия, которому было передано управление
winlog.computer_name	keyword (опционально)	Имя компьютера
winlog.keywords	keyword (опционально)	Ключевые слова
winlog.channel	keyword (опционально)	Имя канала
winlog.record_id	keyword	Номера записи
winlog.opcode	keyword (опционально)	Код операции
winlog.provider_guid	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор провайдера
winlog.provider_name	keyword (опционально)	Имя провайдера
winlog.process.pid	long (опционально)	Идентификатор процесса
winlog.task	keyword (опционально)	Имя задачи

Поле	Тип	Расшифровка
winlog.time_created	date (опционально) (ISO 8601)	Дата и время создания события
winlog.process.thread.id	long (опционально)	Идентификатор нити
winlog.user.identifier	keyword (опционально)	SID пользователя
winlog.user.name	keyword (опционально)	Имя пользователя
winlog.event_data	json_object (опционально) (набор полей отличаются от провайдера к провайдеру, все поля должны иметь тип: keyword)	Поля события
winlog.user_data	json_object (опционально) (набор полей отличаются от провайдера к провайдеру, все поля должны иметь тип: keyword)	Пользовательские поля события

5.6 События монитора процессов

Подтипы событий и их текстовые описания представлены в таблице 17.

Таблица 17 – Подтипы событий монитора процессов и их тестовые описания

Код события	Имя события	Описание
0	Процессы: Загрузка драйвера	Загрузка драйвера path
1	Процессы: Старт процесса	Старт процесса командой cmdl из cpath (cpid) , нить = whotid (из модуля who)
2	Процессы: Завершение процесса	Завершение процесса с кодом code
3	Процессы: Загрузка образа	Загрузка образа path
6	Процессы: Доступ к процессу	Доступ к процессу tpath (tpid) с правами dsrd , { разрешено ИЛИ запрещено dsrd-grnt }
7	Процессы: Создание нити в процессе	Создание нити tid в процессе tpath (tpid) , нить = whotid (из модуля who)
13	Процессы: Обнаружение: подмена командной строки	Подмена командной строки с cmdl1 на cmdl
15	Процессы: Доступ к рабочему столу	Доступ к рабочему столу desk с правами dsrd , { разрешено ИЛИ запрещено dsrd-grnt }, нить = whotid (из модуля who)
16	Процессы: Обнаружение: изменение системной защиты процесса	Изменение системной защиты процесса с prot на prot1
18	Процессы: Доступ к нити процесса	Доступ к нити tid процесса tpath (tpid) с правами dsrd , { разрешено ИЛИ запрещено dsrd-grnt }, нить = whotid (из модуля who)
20	Процессы: Загрузка образа в процесс	Загрузка образа path в процесс tpath (tpid) , нить = whotid (из модуля who)
23	Процессы: Другие обнаружения	Расшифровка кода detect

Поля событий монитора процессов представлены в таблице 18.

Таблица 18 – Поля событий монитора процессов

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

Назначение	JSON	Тип
Размер файла	fsize	int64
Тип файла	ftype	enum
SHA-1 файла	sha1	string
MD5 файла	md5	string
SHA-256 файла	sha256	string
Электронная подпись файла	sgnr	string
Статус электронной подписи	sgnr_s	enum
Тип упаковщика файла	pack	string
Атрибуты файла	attr	unsigned
Время создания файла	crttime	timestamp
Время последней записи файла	chtime	timestamp
Оригинальное имя файла	ofn	string
Компания-издатель файла	fcomp	string
Версия файла	fver	string
Описание файла	fdesc	string
Продукт, к которому относится файл	fprod	string
Файл находится в "белом" списке	fwhite	int (-/1)
Код обнаружения	detect	unsigned

5.7 События монитора системы

Подтипы событий (**st**) монитора системы представлены в таблице 19.

Таблица 19 – Подтипы событий монитора системы

Код события	Имя события	Описание
0	Система: WMI	WMI
1	Система: Атаки на Kerberos	Атаки на Kerberos

События монитора систем с кодом события 0 (WMI) представлены в таблице 20.

Таблица 20 – События монитора системы (код события 0)

Назначение	JSON
WMI: Тип события (создание = 0, удаление = 1, изменение = 2)	wmi
WMI: Путь	wmi_pth
WMI: SID пользователя	wmi_sid
WMI: Пространство имен	ns

Назначение	JSON
WMI: Путь до исполняемого файла	exe_path
WMI: Имя файла	fname
WMI: Имя фильтра событий	wmi_nm
WMI: Строка запроса	qstr
WMI: Имя файла скрипта	scrfname
WMI: Текст скрипта	scrtxt
WMI: Имя источника	sname
WMI: SMTP	smtp
WMI: Фильтр	flt
WMI: Потребитель	cnsn

Пример строки события представлен в таблице 21.

Таблица 21 – События WMI

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

Подтипы атак (**atck**) на Kerberos представлены в таблице 22:

Таблица 22 – События монитора системы (Атаки на Kerberos)

Код события	Имя события	Описание
0	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_GOLDEN_TICKET	Golden ticket
1	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_SILVER_TICKET	Silver ticket
2	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_KERBEROASTING	Kerberoasting
3	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_AS_REP_ROASTING	AS-REP roasting

События монитора системы атаки Golden ticket представлены в таблице 23.

Таблица 23 – События монитора системы (атаки golden ticket)

Назначение	JSON
Golden ticket: Причина	goldent_r
Golden ticket: Имя пользователя	goldent_u
Golden ticket: Имя домена	goldent_d
Golden ticket: IP-адрес	goldent_ip

События монитора системы атаки Silver ticket представлены в таблице 24.

Таблица 24 – События монитора системы (атаки silver ticket)

Назначение	JSON
Silver ticket: Причина	silvert_r
Silver ticket: Имя пользователя	silvert_u
Silver ticket: Имя домена	silvert_d
Silver ticket: IP-адрес	silvert_ip

События монитора системы атаки Kerberoasting представлены в таблице 25.

Таблица 25 – События монитора системы (атака Kerberoasting)

Назначение	JSON
Kerberoasting: Причина	kerberoasting_r
Kerberoasting: Имя пользователя	kerberoasting_u
Kerberoasting: Имя домена	kerberoasting_d
Kerberoasting: IP-адрес	kerberoasting_ip

События монитора системы атаки AS-REP roasting представлены в таблице 26.

Таблица 26 – События монитора системы (атака AS-REP roasting)

Назначение	JSON
AS-REP roasting: Причина	asreproasting_r
AS-REP roasting: Имя пользователя	asreproasting_u
AS-REP roasting: Имя домена	asreproasting_d
AS-REP roasting: IP-адрес	asreproasting_ip

Таблица 27 – Подтипы атак на Kerberos в зависимости от причины

Код события	Имя события	Описание
0	KERBEROS_ATTACK_REASON_NO_TGT	Отсутствует запрос TGT
1	KERBEROS_ATTACK_REASON_LIFETIME_TICKET	Превышено время жизни билета, установленное групповой политикой
2	KERBEROS_ATTACK_REASON_WEAK_ENCRYPTION	Возможна атака, т.к. используется слабый алгоритм шифрования
3	KERBEROS_ATTACK_REASON_INTEGRITY_FAILED	Билет зашифрован с помощью не сессионного ключа
4	KERBEROS_ATTACK_REASON_DOMAINNAME_IS_EMPTY	Имя домена не задано
5	KERBEROS_ATTACK_REASON_DOMAINNAME_IS_INVALID	Неправильное имя домена

6	KERBEROS_ATTACK_REASON_LARGE_COUNT_REQUEST_TGS	Большое количество запросов билетов TGS со слабым шифрованием
---	--	---

Пример описания события, связанного с атакой на Kerberos, как оно при обнаружении отобразится в Программе в поле **Описание** таблицы на странице **Активность**, приведен в таблице 28.

Таблица 28 – Примеры описания атак

Причина	Описание
0	[Система] Атака Golden ticket. Отсутствует запрос TGT. Пользователь: goldent_u@goldent_d , ip-адрес: goldent_ip
1	[Система] Атака Silver ticket. Имя домена не задано. Пользователь: silvert_u@silvert_d , ip-адрес: silvert_ip
2	[Система] Атака Kerberoasting. Возможна атака, т.к. используется слабый алгоритм шифрования. Пользователь: kerberoasting_u@kerberoasting_d , ip-адрес: kerberoasting_ip
3	[Система] Атака AS-REP roasting. Используется слабый алгоритм шифрования. Пользователь: asreproasting_u@asreproasting_d , ip-адрес: asreproasting_ip

5.8 События пользовательских сессий

Подтипы событий и их текстовые описания представлены в таблице 29.

Таблица 29 – Подтипы событий пользовательских сессий

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

Обозначение **%type%** заменяется на «локальной», если **local**, иначе «дистанционной».

Обозначение **%type2%** заменяется на «локальной», если **local**, иначе «дистанционной».

5.9 События монитора вызовов

Подтипы событий монитора вызовов представлены в таблице 30.

Таблица 30 – Подтипы событий монитора вызовов

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

События монитора вызовов (RPC-вызовы) представлены в таблице 31.

Таблица 31 – События монитора вызовов (RPC вызовы)

Назначение	JSON
RPC: UUID интерфейса	rpc_id
RPC: Конечная точка	endp
RPC: Сетевой адрес	n_addr
RPC: Уникальный идентификатор процесса клиента	c_uuid
RPC: PID процесса клиента	c_pid
RPC: Исполняемый файл процесса клиента	c_path
RPC: Уникальный идентификатор процесса сервера	s_uuid
RPC: PID процесса сервера	s_pid
RPC: Исполняемый файл процесса сервера	s_path

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

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

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

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

5.10 События модуля контроля USB

Тип события – **Контроль USB** (t:9 в DSL). Подтипы событий (**st**) и их текстовые описания представлены в таблице 32.

Таблица 32 – Подтипы событий модуля контроля USB

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

Поля событий модуля контроля USB указаны в таблице 33.

Таблица 33 – События модуля контроля USB

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

Общее количество прочитанных байтов	uint64	usb_tr
Общее количество записанных байтов	uint64	usb_tw

5.11 События статистики

Поля событий статистики работы системы представлены в таблице 34.

Таблица 34 – Поля событий статистики

Назначение	JSON
Загрузка процессора	cpu_load
Загрузка памяти	mem_load
Кол-во процессов	processes
Кол-во нитей	threads
Кол-во открытых дескрипторов	handles
Объем прочитанных на диск данных в секунду	disk_read
Объем записанных на диск данных в секунду	disk_write
Объем переданных данных по сети в секунду	net_send
Объем принятых данных по сети в секунду	net_recv
Время регистрации события (UTC)	time
Временная зона	timezone
Признак нахождения в режиме network containment	net_locked
Общее количество сетевых соединений	connections
Состояние функций защиты (0 - вкл, 1 - выкл)	disabled
Время последнего обновления аналитики по наборам	config_time

5.12 События anti-ransomware-модуля

Подтипы событий и их текстовые описания представлены в таблице 35.

Таблица 35 – Подтипы событий antiransomware-модуля

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

Поля событий anti-ransomware модуля представлены в таблице 36.

Таблица 36 – Поля событий anti-ransomware модуля

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

6. Перечень сокращений

Аббревиатура	Расшифровка
ГОСТ	Государственный стандарт
ИБ	Информационная безопасность
ОС	Операционная система
ПО	Программное обеспечение
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
CSRSS	Client/Server Runtime Subsystem
DLL	Dynamic Link Library
DNS	Domain Name System
DSL	Domain-specific language
EDR	Endpoint Threat Detection & Response
ETW	Event Tracing for Windows
HEX	Hexadecimal
HTTPS	Hyper Text Transfer Protocol Secure
IOC	Indicator of Compromise
JSON	Java Script Object Notation
ML	Machine Learning
PE	Portable Executable
RPC	Remote Procedure Call
SHA-256	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TTP	Tactics, Techniques, and Procedures
UUID	Universally Unique Identifier
WMI	Windows Management Instrumentation

7. Перечень терминов и определений

Термин	Расшифровка термина
ИБ	Комплекс организационных и технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
ИСО	Международная организация по стандартизации.
МЭК	Международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий. Некоторые из стандартов МЭК разрабатываются совместно с Международной организацией по стандартизации.
Провайдер ETW	Любой компонент, который использует Event Tracing API. Это могут быть как классические провайдеры, созданные до Windows Vista и применяющие MOF-классы, так и провайдеры на основе манифестов, использующие новые интерфейсы, появившиеся в Windows Vista.
Ретроспективный анализ	Детальное исследование образов систем, журналов событий, дампов памяти и сетевого трафика за определенный промежуток времени в прошлом с целью выявить следы компрометации.
Телеметрия	Совокупность методов сбора информации и измерения параметров, позволяющих получить необходимые сведения об удаленных объектах.
Хеш-сумма	Уникальный идентификатор, который задается (автором программы или первым владельцем файла) с помощью «перемешивания» и шифрования содержимого файла по специальному алгоритму с последующей конвертацией результата в обычную строку символов.
Хост	Любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определенное на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключенный к локальной или глобальной сети.
Хост-процесс	Контейнер для нескольких служб, расположенных внутри и отображающихся как один процесс.
Anti-Ransomware	Программное обеспечение, защищающее конечные точки от вирус-шифровальщиков.
APT-атака	Целевая кибератака (таргетированная кибератака) – вид кибератаки, процесс которой контролируется вручную в реальном времени человеком, являющимся центром атаки. Целью данной атаки является хищение защищенной информации из информационной системы конкретной компании, организации или государственной службы.
ATT&CK	База знаний компании MITRE Corporation, содержащая описание тактик, приемов и методов, используемых киберпреступниками.
Cmd	Команда для запуска интерпретатора команд.

Термин	Расшифровка термина
CSRSS	Клиент-серверная подсистема времени выполнения. Безопасный процесс Microsoft, помогающий управлять большинством наборов графических инструкций в операционной системе Windows. До Windows NT 4.0 csrss.exe отвечал за всю графическую подсистему, включая управление окнами, параметры рисования и многие другие функции. В Windows NT 4.0 большое количество мощностей рабочей системы было перемещено из процесса выполнения клиент-сервера в ядро Windows, которое продолжает работать как обычная процедура.
DLL	Динамически подключаемая библиотека.
DNS	Служба имён доменов (механизм, используемый в сети Internet и устанавливающий соответствие между числовыми IP-адресами).
DSL	Предметный язык программирования, специализированный для конкретной области применения.
EDR	Класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, и других устройствах
ETW	Высокоэффективная масштабируемая система трассировки с минимальными затратами ресурсов, реализуемая в операционных системах Windows.
HEX	Позиционная система счисления по целочисленному основанию 16.
HTTPS	Расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IOC	Индикаторы компрометации.
JSON	Текстовый формат обмена данными, основанный на JavaScript.
Kerberos	Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы.
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux, включающих тот или иной набор утилит и программ проекта GNU.
MD5	128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности.
MITRE (The MITRE Corporation)	Американская некоммерческая организация с двумя штаб-квартирами в Бедфорде, штат Массачусетс, и Маклине, штат Вирджиния. Сотрудники компании занимаются исследованиями и разработками в области обороны, здравоохранения, авиации, внутренней безопасности и кибербезопасности.
ML	Класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение за счёт применения решений множества сходных задач.
Network containment	Технология, позволяющая осуществлять сетевое сдерживание.
NSRL	Национальная справочная библиотека программного обеспечения, созданная в США.

Термин	Расшифровка термина
PE	Формат исполняемых файлов, объектного кода и динамических библиотек, используемый в 32-х и 64-разрядных версиях операционной системы Microsoft Windows.
Powershell	Расширяемое средство автоматизации от Microsoft с открытым исходным кодом, состоящее из оболочки с интерфейсом командной строки и сопутствующего языка сценариев.
RPC	Класс технологий, позволяющих программам вызывать функции или процедуры в другом адресном пространстве. Обычно реализация RPC-технологии включает два компонента: сетевой протокол для обмена в режиме клиент-сервер и язык сериализации объектов.
SHA-1	Алгоритм криптографического хеширования. Описан в RFC 3174. Для входного сообщения произвольной длины алгоритм генерирует 160-битное хеш-значение, называемое также дайджестом сообщения, которое обычно отображается как шестнадцатеричное число длиной в 40 цифр.
SHA-256	Алгоритм хеширования. Криптографическая хэш-функция, разработанная Агентством национальной безопасности США.
Sophos	Британский производитель средств информационной безопасности для настольных компьютеров, серверов, мобильных устройств, почтовых систем и сетевых шлюзов.
SSL	Криптографический протокол, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.
Threat Hunting	Охота на киберугрозы – это активная деятельность по киберзащите. Процесс упреждающего и итеративного поиска в сетях для обнаружения и изоляции сложных угроз, которые обходят существующие решения безопасности.
TPP	Тактики, техники и процедуры, используемые злоумышленниками для осуществления атак
UTC	Стандарт, по которому общество регулирует часы и время. Отличается на целое количество секунд от атомного времени и на дробное количество секунд от всемирного времени UT1.
UUID	Стандарт идентификации, используемый в создании программного обеспечения, основное назначение которого – позволить распределённым системам уникально идентифицировать информацию без центра координации.
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ. Кроме бесплатной существует корпоративная платная версия.
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса.
WMI	Инструментарий управления Windows. Одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.

Термин	Расшифровка термина
YARA	Инструмент для матчинга текстовой информации, направлен на помощь исследователям вредоносных программ в выявлении и классификации образцов вредоносных программ.

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