

RT Protect EDR

Руководство оператора поиска угроз

Версия 1.0.10 от 12 марта 2024

Разработано компанией АО «РТ-Информационная безопасность»



1. Общие положения	4
1.1 Аннотация документа	4
1.2 Термины и определения	4
1.3 Условные обозначения	5
2. Общие сведения	6
2.1 Общие сведения о программе	6
3. Описание принципов безопасной работы программы	8
3.1 Общая информация	8
3.2 Компрометация паролей	9
4. Основные операции в программе «RT Protect EDR»	10
4.1 Просмотр состояния защищаемой инфраструктуры	11
4.2 Работа с панелью управления	13
4.3 Работа с инцидентами	15
4.3.1. Страница «Инцидент»	19
4.4 Работа с деревом процессов	20
4.4.1. Вкладка «Информация»	23
4.4.2. Вкладка «Файлы»	25
4.4.3. Вкладка «Сеть»	26
4.4.4. Вкладка «Реестр»	28
4.4.5. Вкладка «Процессы»	29
4.4.6. Вкладка «Загруженные DLL/SO»	30
4.4.7. Вкладка «Точки автозапуска»	31
4.4.8. Вкладка «Распространенность»	32
4.4.9. Вкладка «Событие старта»	33

4.4.10. Вкладка «Правила/MITRE»	33
4.5 Проактивный поиск угроз.....	34
4.5.1. Просмотр графиков активности.....	46
4.5.2. Создание инцидента на странице «Активность»	47
4.6 Проверка артефактов с помощью TI-платформы.....	48
4.7 Проверка распространенности программы в агентской сети	48
4.8 Действия с агентами	50
4.8.1. Сканирование уязвимостей на странице «Агент»	53
4.9 Просмотр графиков	55
4.10 Просмотр информации об уязвимостях	56
4.10.1. Формирование отчетности на странице с уязвимостями.....	61
4.10.2. Распространенность уязвимости в защищаемой инфраструктуре	61
4.10.3. Изучение сведений об уязвимости.....	62
4.11 Просмотр программ в списке исключений	65
4.12 Просмотр профилей безопасности агента	67
4.13 Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения	70
5. Модель данных, обнаруживаемых агентом.....	71
5.1 Общие сведения	71
5.2 События монитора сети	88
5.3 События монитора файловых операций	89
5.4 События монитора реестра	91
5.5 События системного журнала Windows (ETW).....	92
5.6 События монитора процессов	94
5.7 События монитора системы	96
5.8 События пользовательских сессий	99
5.9 События монитора вызовов.....	100
5.10 События статистики	101

5.11 События anti-ransomware-модуля	102
6. Перечень сокращений.....	104
7. Перечень терминов и определений	105
8. Заключение.....	109

1. Общие положения

1.1 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.

1.2 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 1.

Таблица 1 – 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).

Термин	Расшифровка
Инцидент информационной безопасности	Единичное 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.

1.3 Условные обозначения

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

Таблица 2 – Условные обозначения

Обозначение	Описание
ПРОПИСНЫЕ БУКВЫ	Акронимы, аббревиатуры.
«Times New Roman»	Названия документов, команд, каталогов, файлов и т.д.
Жирный шрифт	Подписи таблиц, рисунков, названия разделов, подразделов, пунктов и подпунктов, 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

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, защищенному с помощью SSL с применением шифрования ГОСТ.

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 «RT Protect EDR»

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.

При входе в программу под учетной записью оператора поиска угроз по умолчанию открывается страница **Активность**.

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.

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.

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 ТТР);

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 **Заккрыть 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) Заккрыть 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 (рис. 3).

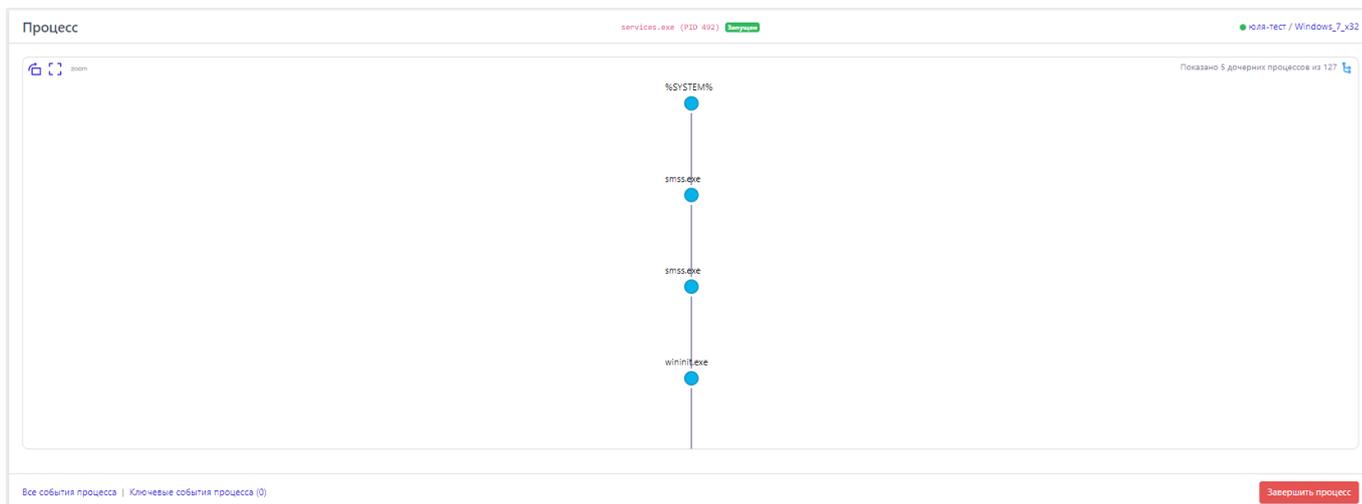


Рисунок 3 – Дерево процессов без вкладки «Информация»

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. 4).

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: `uid:8db667ba-d8f8-01d7-0700-000000000000 AND (svrt:[1 TO *] OR (svrt0 AND (rul* OR act:0)))`. Below the filters, a table displays one event with the following details:

Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Критичность	Действие	Инцидент
17.11.2023, 11:46:09	17.11.2023, 11:46:03	Gr_Илм / Ag_for_ila_W8.1_64	Ключ Создан новый ключ \\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\WppSvc	services.exe (688)	Низкая		

Рисунок 4 – 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. 5):

- 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" -noudate
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, 18:28:29

Рисунок 5 – 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 (рис. 6).

* Внимание! Информация о файловой активности процесса может быть неполной из-за настроек в профиле безопасности агента и исключений, установленных для процесса

Файл (596 из 596)	Действие
\device\harddiskvolume3\windows\debug\mrt.log ↓	Модифицирован
\device\harddiskvolume3\windows\system32\catroot\{ff750e6c3-38ee-11d1-85e5-00c04fc295ee}\microsoft-windows-client-features-package03~31bf3856ad364e35~amd64~10.0.19041.1766.cat ↓	Прочитан
\device\harddiskvolume3\windows\system32\mrt\6a18629d-500e-437f-b64b-394f5ee7416e\01d8c1bbfc696428 ↓ !	Создан Удален
\device\harddiskvolume3\windows\system32\mrt\6a18629d-500e-437f-b64b-394f5ee7416e\history\results\quick\{9d62186a-0e50-7f43-b64b-394f5ee7416e} ↓ !	Создан Удален
\device\harddiskvolume3\windows\system32\mrt\6a18629d-500e-437f-b64b-394f5ee7416e\mpgearsupport_20220906_094158bd135034-b13d-06f3-4ab1-adc8dbd21975.log ↓ !	Создан Удален

Рисунок 6 – Информация о файлах процесса

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. 7).

В списке действий с файлом
присутствует удаление

Рисунок 7 – Сообщение о присутствии в списке удаления файла

4.4.3. Вкладка «Сеть»

Во вкладке **Сеть** отображается информация о сетевых подключениях процесса (рис. 8):

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

* Внимание! Информация о сетевой активности процесса может быть неполной из-за исключений, установленных для процесса

Входящие подключения (0)

Нет подключений

Исходящие подключения (1)

IP-адрес	Имя хоста	Удаленный порт	Протокол
20.93.58.141	wdcp.microsoft.com	443	TCP

DNS-запросы (0)

Нет запросов

Рисунок 8 – 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.

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 9 – 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. 10).

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 10 – 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. 11).

Нативные (показано 27 из 27)	Размер файла	Подпись	Размещение	Хеш (SHA-256)
> \Device\HarddiskVolume4\Windows\System32\winnr.dll	31232		0x00007FFC970600 - 0x00007FFC9706E0 00	0ce5de9525699efa35d7378472391be 583e3cb160557eb5908fdd5f6a38324 f9  
> \Device\HarddiskVolume4\Windows\System32\wshbth.dll	64000		0x00007FFC967600 - 0x00007FFC967750 00	5e6d0f371594b4388c51d5153d7209 ef9a8e691e669c6a6499c97ec33b290f d4  
> \Device\HarddiskVolume4\Windows\System32\wpnapps.dll	1348608		0x00007FFC82F700 - 0x00007FFC830BE0 00	58fd01809188e2e13c977b2bfc4680 a4c55677ff75dd1f2f352165f103d704 3  
> \Device\HarddiskVolume4\Windows\System32\netprofm.dll	229376		0x00007FFC9E3F000 - 0x00007FFC9E42D0 00	f03f71d6a6507a364a5789ecd78220b 8e586ab6a619bc83d5c75cca1c3ca15 e8  
> \Device\HarddiskVolume4\Windows\System32\npmproxy.dll	45056		0x00007FFC9C2C00 - 0x00007FFC9C2D00 00	8d10f12787c97ce4c91a4bb6584bacc 21d0d1d19f30c40127847491266ff2a 65  

.NET (показано 0 из 0)	Размер файла	Подпись	Размещение	Хеш (SHA-256)
Нет загруженных DLL				

Рисунок 11 – 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 содержатся 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 рассматриваемыми 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. 12).

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 12 – 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. 13).

Процесс: vcpkgssrv.exe (PID 21972) Запущен Агент: DESKTOP-YGKODS

Процессное дерево:

- %SYSTEM% (4)
- smss.exe (632)
- smss.exe (848)
- winlogon.exe (964)
- userinit.exe (7416)
- explorer.exe (7556)
- devenv.exe (2136)
- vshost.exe (11748)
- vcpkgssrv.exe (21972)

Вкладка: Распространенность (1/318)

Время первой регистрации	Группа/агент	Путь до исполняемого файла
28.09.2022, 11:03:22	Агент: DESKTOP-YGKODS	\\Device\\HarddiskVolume2\\Program Files\\Microsoft Visual Studio\\2022\\Community\\Common7\\DEVC\\vcpackages\\x80\\vcpkgssrv.exe

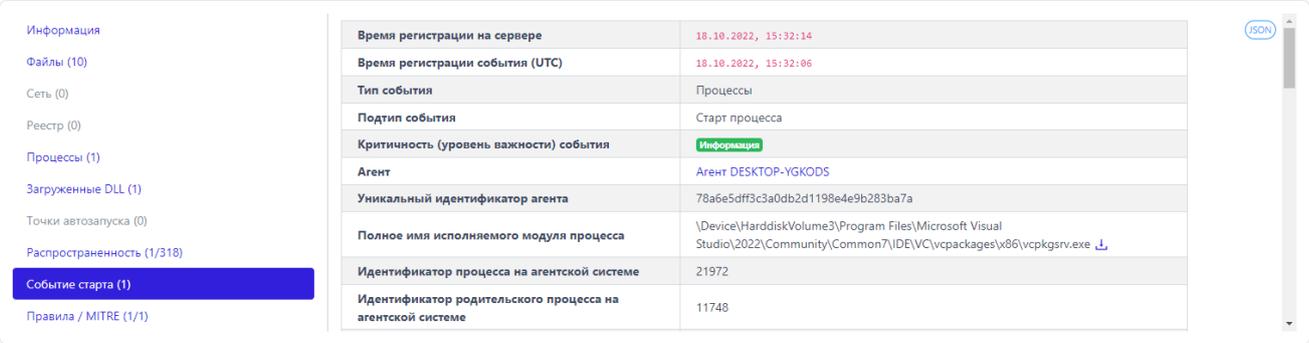
Восстановить файлы | Завершить процесс

Рисунок 13 – 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. 14).



Информация	Время регистрации на сервере	18.10.2022, 15:32:14
Файлы (10)	Время регистрации события (UTC)	18.10.2022, 15:32:06
Сеть (0)	Тип события	Процессы
Реестр (0)	Подтип события	Старт процесса
Процессы (1)	Критичность (уровень важности) события	Информация
Загруженные DLL (1)	Агент	Агент DESKTOP-YGKODS
Точки автозапуска (0)	Уникальный идентификатор агента	78a6e5dff3c3a0db2d1198e4e9b283ba7a
Распространенность (1/318)	Полное имя исполняемого модуля процесса	\\Device\\HarddiskVolume3\\Program Files\\Microsoft Visual Studio\\2022\\Community\\Common7\\IDE\\VC\\vcpackages\\x86\\vcprkgshr.exe ↓
Событие старта (1)	Идентификатор процесса на агентской системе	21972
Правила / MITRE (1/1)	Идентификатор родительского процесса на агентской системе	11748

Рисунок 14 – 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 (рис. 15).

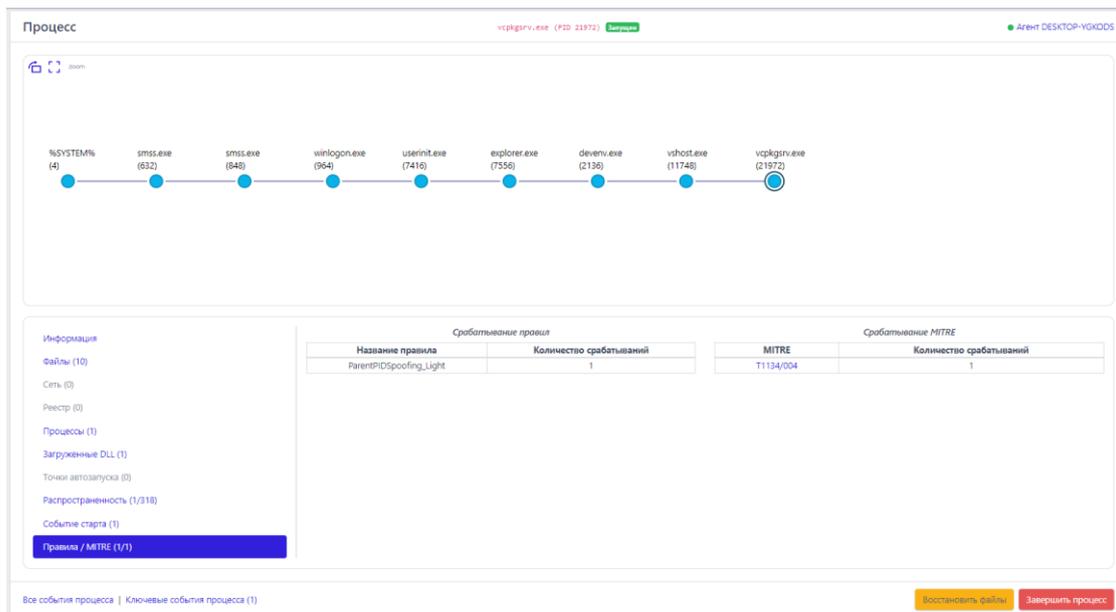


Рисунок 15 – Правила/MITRE

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 АРТ-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 зловред мог проникнуть в инфраструктуру компании.

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

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

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 АРТ-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 (рис. 16).

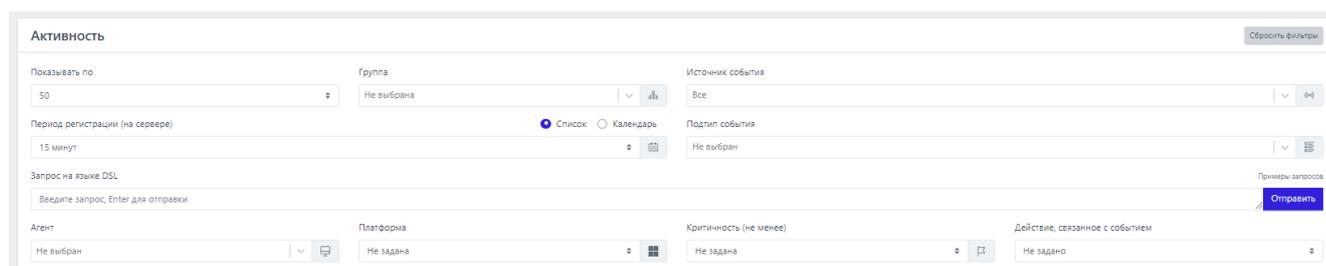


Рисунок 16 – Фильтры на странице «Активность»

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 17.

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
>	25.05.2023, 13:55:44	25.05.2023, 13:55:42	юля-тест / Win_Server_2016	WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root(cimv2 : Win32_PageFileSetting)"	svchost.exe (76)	
>	25.05.2023, 13:55:44	25.05.2023, 13:55:42	юля-тест / Win_Server_2016	WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root(cimv2 : Win32_PageFileUsage)"	svchost.exe (76)	
>	25.05.2023, 13:55:44	25.05.2023, 13:55:42	юля-тест / Win_Server_2016	WMI-запрос: "Start IWbemServices::CreateInstanceEnum - root(cimv2 : Win32_PageFileUsage)"	svchost.exe (76)	

Рисунок 17 – 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 18.

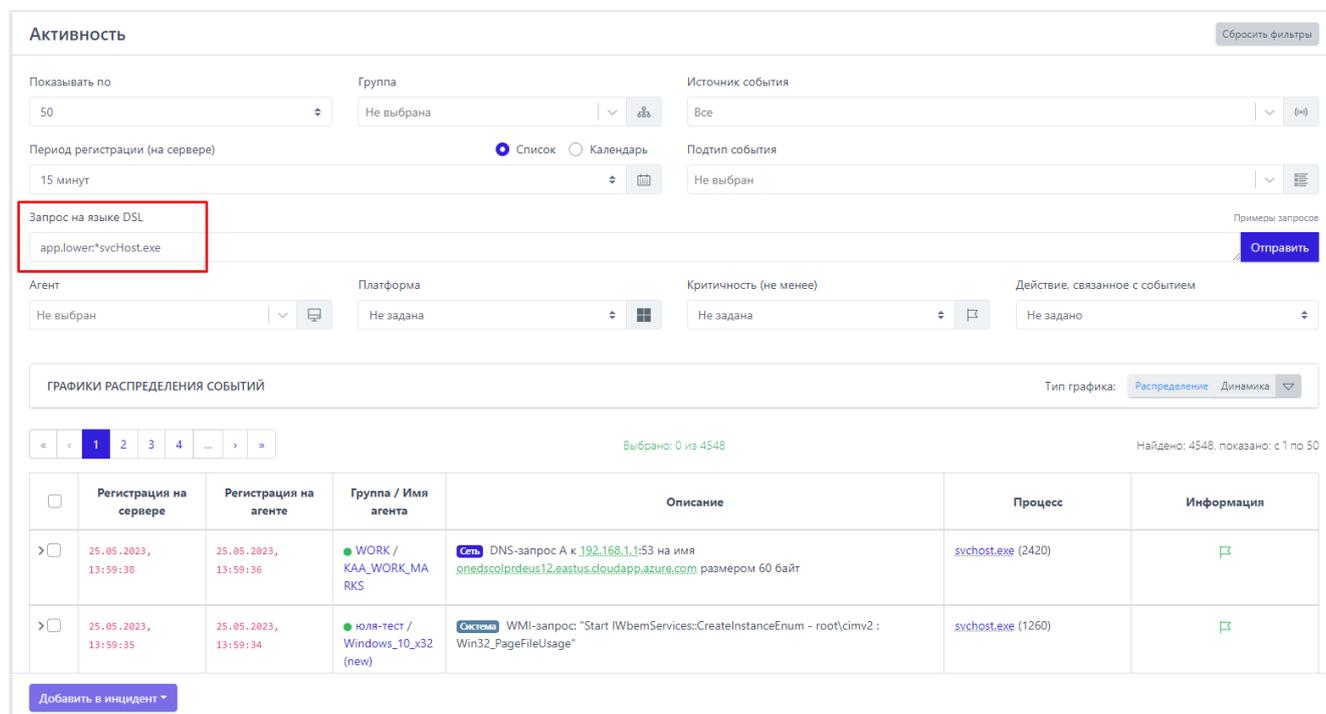
The screenshot shows the 'Активность' (Activity) section of the RT Protect EDR interface. The search filter 'app:svchost.exe' is entered in the 'Запрос на языке DSL' field and is highlighted with a red box. Below the search bar, there are several filter options: 'Агент' (Agent), 'Платформа' (Platform), 'Критичность (не менее)' (Criticality), and 'Действие, связанное с событием' (Action). The interface also displays a table of search results with columns for 'Регистрация на сервере', 'Регистрация на агенте', 'Группа / Имя агента', 'Описание', 'Процесс', and 'Информация'. The table shows three results for the search query, all related to 'svchost.exe' processes.

Рисунок 18 – 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 19.



The screenshot shows the 'Активность' (Activity) search interface. The search query 'app.lower:svchost.exe' is entered in the 'Запрос на языке DSL' field, which is highlighted with a red box. The interface includes various filters for 'Показывать по', 'Группа', 'Источник события', 'Период регистрации', 'Подтип события', 'Агент', 'Платформа', 'Критичность', and 'Действие'. Below the filters, there is a table of search results with columns for 'Регистрация на сервере', 'Регистрация на агенте', 'Группа / Имя агента', 'Описание', 'Процесс', and 'Информация'.

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 onedscopprdus12.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)	

Рисунок 19 – 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 20.

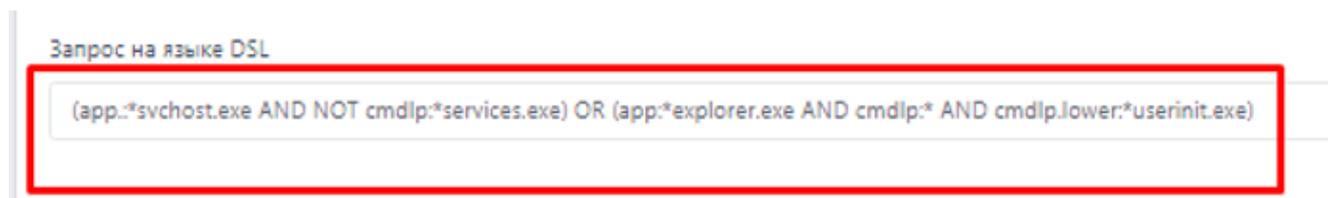


Рисунок 20 – Сложный DSL-запрос

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 21.

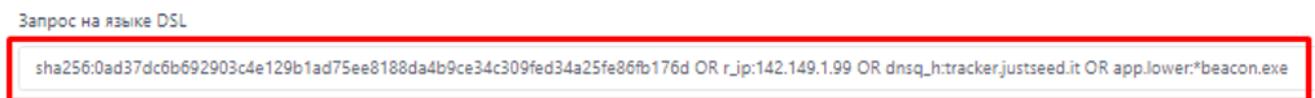


Рисунок 21 – Пример запроса для ретроспективного анализа угроз

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 22.

	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	Описание	Процесс	Информация
>	25.05.2023, 14:55:53	25.05.2023, 14:55:51	lla_group / Ag_for_lla_WS2012	Сеть DNS-ответ со статусом 9501 на запрос А к 194.85.252.62:53 на имя ns2.spektr-opel.ru размером 994 байт	dns.exe (1400)	
>	25.05.2023, 14:55:53	25.05.2023, 14:55:50	lla_group / Ag_for_lla_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)	

Рисунок 22 – 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 23.

The screenshot shows the 'Активность' (Activity) section of the RT Protect EDR interface. A search filter is applied: 'Запрос на языке DSL: r_ip:[1080 TO 1800]'. The interface includes various filters for 'Показывать по', 'Период регистрации', 'Агент', 'Платформа', 'Критичность', and 'Действие'. Below the filters, there is a table of events with columns for 'Регистрация на сервере', 'Регистрация на агенте', 'Группа / Имя агента', 'Описание', 'Процесс', and 'Информация'.

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, 14:57:04	25.05.2023, 14:56:59	WORK / ANPG_WORK_10	Сеть Исходящее подключение к mail.vr-protect.ru (178.208.150.156:443) по TCP	chrome.exe (13756)	

Рисунок 23 – 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 24 - 25.

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: `r_ip:[1080 TO 1800]` Примеры запросов

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 24 – Пример неправильного DSL-запроса

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.exe"` Примеры запросов

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_WS20 12	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_WS20 12	Сеть Исходящее подключение к jtvnw.twitchcdn.net (18.165.128.214:443) по TCP	chrome.exe (4792)	🔗

[Добавить в инцидент](#)

Рисунок 25 – 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 26.

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

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	Исходящее подключение к clientservices.googleapis.com (142.251.1.94:443) по UDP	chrome.exe (8996)	[i]
>	25.05.2023, 15:05:38	25.05.2023, 15:05:34	юля-тест / WIN_8_x32	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)	[i]
>	25.05.2023,	25.05.2023,	lla_group /	SSL HELLO (pubsub-edges.twitch.tv) с pubsub-edge.twitch.tv (44.240.168.143:443)	chrome.exe (4792)	[i]

Добавить в инцидент

Рисунок 26 – 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. 27).

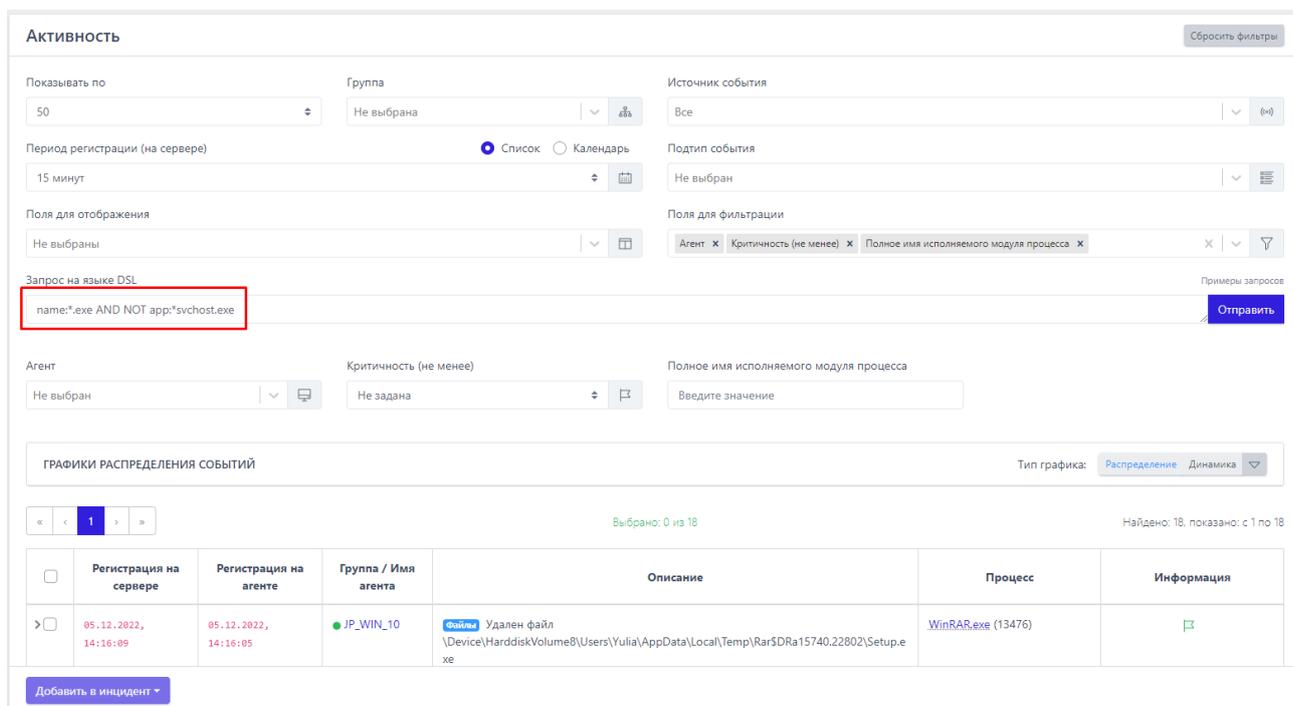


Рисунок 27 – Пример использования оператора NOT

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. 28 и 29):

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).

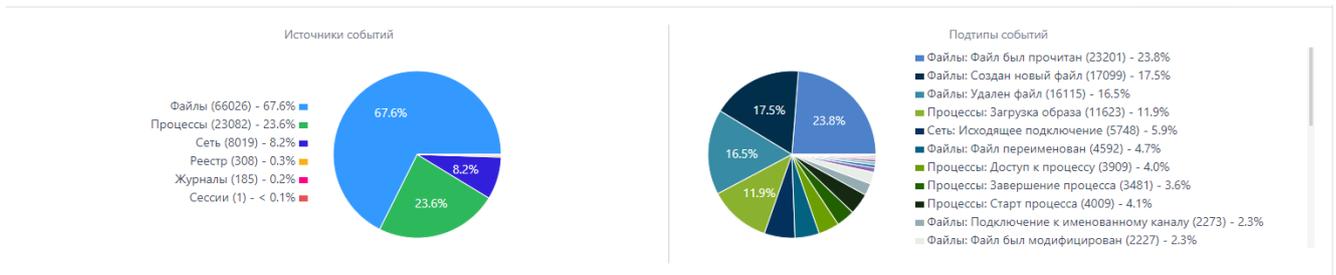


Рисунок 28 – График с распределением событий

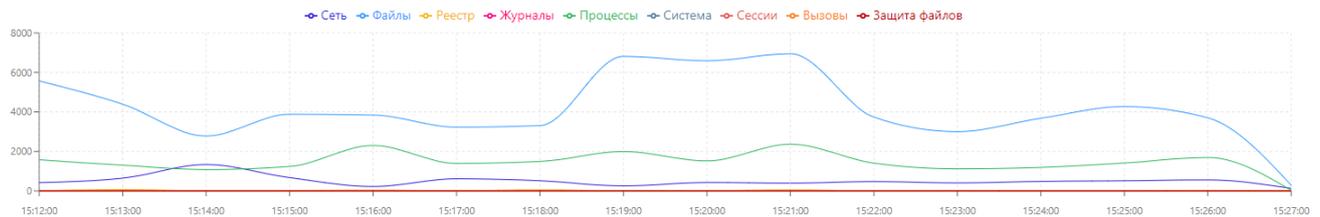


Рисунок 29 – График с динамикой событий

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, открывающейся 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 сервера аналитики по этой программе (рис. 30). Распространённость программы показывает, на каких агентах появлялся файл с определенной хеш-суммой.

Процессы и модули Сбросить фильтры

Показывать по: 50

Платформа: Не задана

Имя модуля: Введите имя модуля

Подпись: Введите значение

Тип подписи: Все

Хеш модуля (SHA-256): Введите хеш

Период регистрации (на сервере): Список Календарь

1 день

Найдено: 114, показано: с 101 по 114

	Регистрация на сервере	Регистрация на агенте	Первичное обнаружение	Хеш модуля (SHA-256)	Имя модуля	Подпись	Число агентов	Распространение
>	24.04.2023, 00:24:37	24.04.2023, 00:24:34	● WORK / FILE	5160ccdc3a3a34a1cde56df497cc589980294876e3ba658bbaec1731b9381deb2	AM_Delta_Patch_1.387.196.5.0.exe	Microsoft Corporation	1	0.26 %
>	24.04.2023, 00:03:31	24.04.2023, 00:03:26	● WORK / alexb	837f2d6c7a92d52058cbb07ea5ac2efdac54bc65ad0bf58659afaf03d09ff83a2	AM_Delta_Patch_1.387.195.3.0.exe	Microsoft Corporation	1	0.26 %
>	23.04.2023, 23:20:44	23.04.2023, 23:20:42	● Агент DESKTOP-JVITBFG	05449a6e41b553e4617f12cc4cbfc6c5343d423217902d41ebd7e60b07ac36d	mshtml.dll	(нет данных)	1	0.26 %
>	23.04.2023, 23:18:15	23.04.2023, 23:18:13	● Агент DESKTOP-JVITBFG	41f55aa4c3bad4da020358bbc649c2e12db0791550e094a34eb6d45faeb835d	Microsoft.PowerShell.Commands.Utility.dll	(нет данных)	1	0.26 %
>	23.04.2023, 23:18:10	23.04.2023, 23:18:10	● Агент DESKTOP-JVITBFG	24fd5e0f350ed0d63e07f6bd2720082add2a2ad2c67650fdf1a9dd9c7d819fb	MIGUIControls.dll	(нет данных)	1	0.26 %
>	23.04.2023, 23:16:40	23.04.2023, 23:16:37	● Агент DESKTOP-JVITBFG	1b37eda0d65e3217d56910f4a4a5190d541d48582d131bc189ce08b8155885b	Markdig.dll	Microsoft 3rd Party Application Component	1	0.26 %
>	23.04.2023, 23:16:40	23.04.2023, 23:16:37	● Агент DESKTOP-JVITBFG	2920a6a51fdc4e7550a05ea5119263d1bc682c5faa745bee67a938c694d15d9e	Markdig.Wpf.dll	Microsoft 3rd Party Application	1	0.26 %

Рисунок 30 – 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 () , 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). Все измененные элементы отображаются в вышеуказанных разделах в красной или зеленой заливке. Красная заливка и зачеркнутое наименование элемента (**Имя: Microsoft OneDrive**) означает, что он был удален с компьютера с установленным агентом, но при этом присутствует в золотом образе. Зеленая заливка (**Имя: Google Chrome**) означает, что элемент был установлен на компьютер с агентом, но при этом в золотом образе этот элемент отсутствует.

4.8.1. Сканирование уязвимостей на странице «Агент»

Сканирование уязвимостей для установленного ПО позволяет выявить программы, которые могут быть использованы злоумышленниками для вредоносной деятельности. Для запуска сканирования необходимо нажать значок  (так он выглядит, если сканирование не запускалось ни разу) в области **Информация о системе** на странице **Агент**. Открывается окно с данными сканера уязвимостей (рис. 31).

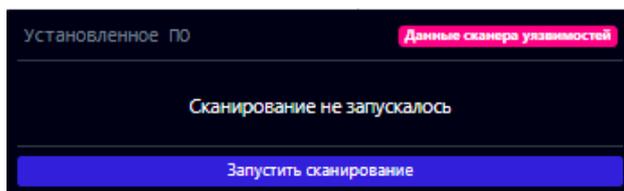


Рисунок 31 – Данные сканера уязвимостей

Чтобы выявить уязвимости, необходимо нажать кнопку **Запустить сканирование**. Сканирование может занять несколько минут, на этот период

значок меняет цвет () , а в окне с данными сканера уязвимостей появляется значок загрузки (). Не обязательно дожидаться завершения проверки, чтобы продолжить работу в модуле администрирования. Проверка будет выполнена в фоновом режиме.

После завершения сканирования значок поменяет цвет, если выявлены уязвимости () , а также будет содержать количество найденных программ с уязвимостями (). Если уязвимости не обнаружены, то значок поменяет цвет на зеленый (). В некоторых случаях для части уязвимостей появляется значок о наличии эксплуатируемых уязвимостей, так называемых эксплойтов (). Это означает, что для выявленной уязвимости существует в открытом доступе программа или скрипт, позволяющие её эксплуатировать. После завершения сканирования в окне с данными по сканированию можно перейти к отчету, нажав значок . Отчет по сканированию содержит подробную информацию об уязвимостях (подробнее см. в разделе 4.10).

Чтобы просмотреть уязвимые программы и сами уязвимости, необходимо раскрыть данные в области **Установленное ПО**, нажав кнопку **Показать все**. При этом, чтобы не листать весь список с установленным ПО можно установить флаг **Только уязвимые**. Тогда в списке установленного ПО останутся только программы с выявленными уязвимостями. Возле программ с выявленными уязвимостями будет отображаться значок с их количеством () , нажав на который, можно открыть карточку с данными об обнаруженных уязвимостях (рис. 32).

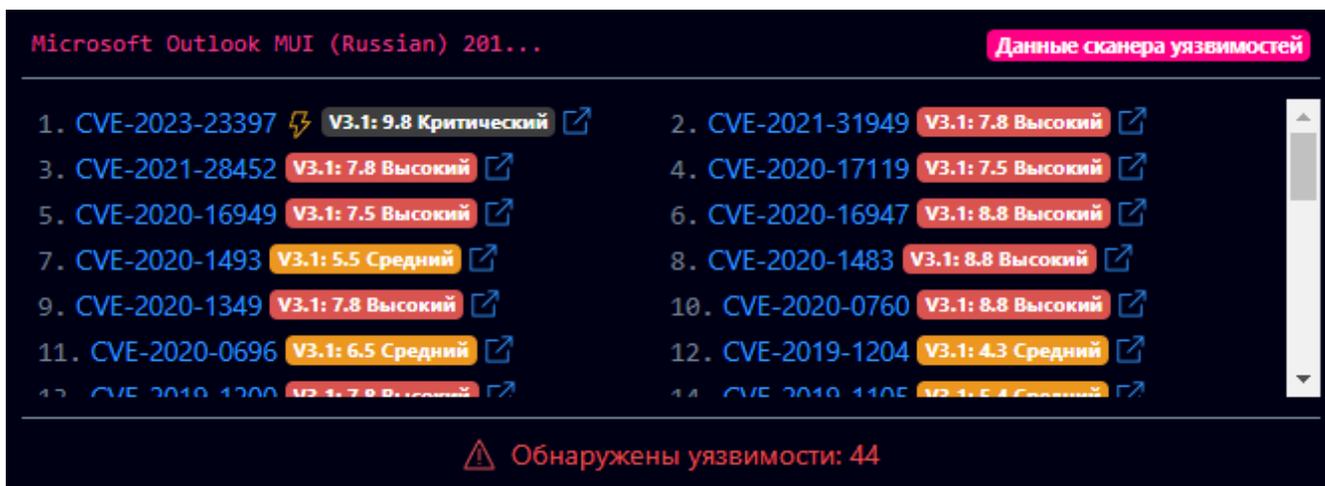


Рисунок 32 – Информация об уязвимостях программы

Каждая запись об уязвимости является ссылкой для перехода на страницу с описанием этой уязвимости на сайте NIST (National Institute of Standards and Technology). В строке с кодовым обозначением уязвимости указывается показатель её опасности (от 0 до 10, где 10 является максимально возможной степенью опасности уязвимости), а также версия стандарта, по которому проводится оценка. Чтобы подробно изучить калькуляцию оценки для выбранной уязвимости, необходимо кликнуть значок , после чего откроется форма на сайте с банком данных угроз безопасности информации (bdu.fstec.ru). Кроме CVE-представления (Common Vulnerability and Exposures) уязвимости для некоторых из уязвимостей в строке отображается CWE-представление (Common Weakness Enumeration), на которое также можно перейти, нажав ссылку с CWE-номером.

4.9 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.

4.10 Просмотр информации об уязвимостях

Информация о сканированиях и найденных в результате уязвимостях осуществляется в разделе **Уязвимости**. Сканер уязвимостей 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). В программе такие уязвимости дополняются информацией из базы данных угроз ФСТЭК (БДУ

ФСТЭК). При этом необходимо понимать, что угрозы, описанные только в БДУ ФСТЭК, в список сканера уязвимостей EDR не попадают.



Примечание

Проверка на наличие уязвимостей (сканирование) запускается в двух сценариях: автоматически либо вручную. Ручной запуск выполняется со страницы **Агент**. Автоматический запуск происходит при следующих условиях:

- 1) При получении сервером блока inventory от агента (по умолчанию 1 раз в сутки);
- 2) После очередной верификации;
- 3) При обработке агентом команды "inventory" в терминале.

Чтобы исключить повторное сканирование ПО на уязвимости, для сканера уязвимостей предусмотрен следующий алгоритм работы:

- 1) Если ПО не проверялось, выполняется проверка по всей базе;
- 2) Если с последнего сканирования БД не обновлялась, проверка завершается;
- 3) Если с последнего сканирования БД обновлялась, то ПО проверяется на наличие уязвимостей только среди последнего обновления БД.

Страница **Управление уязвимостями** содержит список сканирований агентов за последние 3 месяца, список ПО, просканированного программой, а также список уязвимостей, найденных на агентах. Для изучения статистики по сканируемой инфраструктуре в верхней части страницы находятся диаграммы с информацией по общему количеству выполненных сканирований (диаграмма **Сканирования**), количеству уникальных и уязвимых программ, обнаруженных на просканированных агентах диаграмма (**Программы**), количеству обнаруженных уязвимостей, разделенных по степени критичности (диаграмма **Уязвимости**), и

количеству проверенных и непроверенных агентов в общей защищаемой инфраструктуре (диаграмма **Покрытие**). При нажатии строк с количественными значениями на диаграммах **Сканирования, Программы и Уязвимости** происходит переход на соответствующие вкладки с соответствующей значению выборкой данных.

Подробную информацию о сканировании агента можно просмотреть, нажав номер ID сканирования.

Страница **Сканирование** содержит следующие вкладки:

1) Установленные программы (таблица со списком обнаруженных во время сканирования агента программ содержит название программы, издателя, версию и количество найденных уязвимостей), с помощью флага **Только уязвимые программы** можно отсортировать;

2) Критические уязвимости (информация содержит номер CVE и CWE, уровень критичности и ссылку на расчеты калькулятора БДУ на сайте ФСТЭК).



Примечание

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

3) Рекомендации по устранению (содержит общедоступные известные способы устранить уязвимости).

На странице **Сканирование** также отображается общая информация о сканировании и уязвимостях: название агента, идентификатор и статус сканирования, дата начала и завершения операции, диаграмма с числом и уровнем критичности уязвимостей, которые были найдены для выбранного сканирования.

В разделе **Список программ** аналитик может просмотреть список всех программ, установленных в защищаемой инфраструктуре, которые были просканированы на наличие уязвимостей. Можно сортировать программы на те, у которых уязвимости были найдены, и программы без найденных уязвимостей. Информация о программах представлена в таблице, которая содержит следующие поля:

- 1) Название;
- 2) Издатель;
- 3) Версия;
- 4) Число агентов с установленной программой;
- 5) Количество уязвимостей.

Анализ этих данных позволит аналитику выяснить, какие программы и с каким количеством уязвимостей наиболее распространены в защищаемой инфраструктуре.

Нажав ЛКМ на название программы в списке, аналитик может перейти на страницу **Сведения о программе**, на которой представлена информация о найденных в программе уязвимостях, их критичности, количестве, количестве агентов с этой программой, поименный список этих агентов и т. д. Эта информация позволит аналитику определить, какие программы влияют на безопасность в наибольшей степени, то есть расставить приоритеты в решении проблем с уязвимостями на отдельных агентах и в защищаемой инфраструктуре в целом.

В разделе **Список уязвимостей** аналитик может изучить найденные на всех просканированных агентах уязвимости. Информация о них представлена в таблице, которая содержит следующие поля:

- 1) CVE (содержит CVE-идентификатор);
- 2) Опубликована (содержит дату публикации уязвимости в NVD (National Vulnerability Database));

3) Изменена (содержит последнюю дату изменения информации об уязвимости в NVD);

4) Статус (содержит сведения о состоянии уязвимости, данные обновляются NIST);

5) Балл по CVSS 2.0 (количественная оценка уязвимости безопасности по указанному стандарту);

6) Балл по CVSS 3.x;

7) Критичность;

8) Количество уязвимых программ.

Уязвимости можно сортировать с помощью следующих фильтров:

1) Количество уязвимостей на странице;

2) Критичность (используется стандарт CVSSv3, где 0,1-3,9 – это низкая критичность, 4,0-6,9 – средняя, 7,0-8,9 – высокая, 9,0-10 – критичная);

3) Статус;

4) Наличие уязвимых программ;

5) CVE;

6) Период публикации;

7) Период изменения.

Идентификатор уязвимости в таблице служит гиперссылкой для перехода на страницу, содержащую сводные сведения о найденной уязвимости. На этой странице будет содержаться источник, на основе которого предоставлены сведения об уязвимости, ее описание и критичность, список агентов, на которых уязвимость была найдена, рекомендации по устранению и другие сведения, относящиеся к найденной уязвимости. Кнопка  в верхней части страницы **Сведения об уязвимости** позволяет перейти к источнику данных об оценке уязвимости, то есть к базе данных NIST. Источник сведений, указанный на странице **Сведения об уязвимости** в поле **Источник** показывает, откуда информация об уязвимости появилась впервые, это может быть как NIST, так и

другие ресурсы. Сводная информация по уязвимости может быть показана по двум различным стандартам 2.0 и 3.0.

4.10.1. 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** в разделе **Сканирования**. Чтобы сохранить отчет в формате csv, необходимо нажать кнопку , после чего отчет будет доступен в папке **Загрузки**. Для формирования отчета необходимо использовать кнопку . В отчете отображается полный список ПО на просканированных агентах, в котором присутствуют программы с найденными уязвимостями.

4.10.2. Распространенность уязвимости в защищаемой инфраструктуре

Чтобы получить информацию о том, как сильно распространена та или иная уязвимость в защищаемой EDR инфраструктуре, аналитику необходимо выполнить следующие действия:

- 1) Перейти в раздел **Уязвимости**;
- 2) Перейти в раздел **Список уязвимостей**;
- 3) С помощью представленных на странице фильтров найти искомую уязвимость и выбрать ее в таблице, нажав ЛКМ на идентификатор уязвимости;
- 4) На открывшейся странице **Сведения об уязвимости** просмотреть список агентов с выбранной уязвимостью;
- 5) При необходимости просмотреть программы с изучаемой уязвимостью следует нажать цифру в строке **Количество уязвимых программ**.

Откроется раздел **Список программ**, где аналитик может просмотреть все программы, в которых встречается найденная уязвимость. При нажатии ЛКМ на название любой программы произойдет переход на страницу **Сведения о**

программе, где аналитик может увидеть, на каких агентах эта программа встречается.

4.10.3. 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 3.

Таблица 3 –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)	Требуются ли действия со стороны пользователей атакуемой системы	Требуется (R)
			Не требуется (N)
	Влияние на другие компоненты системы (S)	Оказывает ли влияние атакуемая подсистема на другие компоненты	Не оказывает (U)
			Оказывает (C)
	Влияние на конфиденциальность (C)		Не оказывает (N)
			Низкое (L)
			Высокое (H)
	Влияние на целостность (I)	Влияние на надежность и гарантированную правдивость информации	Не оказывает (N)
			Низкое (L)
Высокое (H)			
Влияние на доступность (A)	Имеется в виду влияние на легкость доступа к информационным ресурсам	Не оказывает (N)	
		Низкое (L)	
		Высокое (H)	
CVSS 2.0	Способ получения доступа	Удаленность атакующего от уязвимого объекта	Сетевой (N)
			Смежная сеть (A)

			Локальный (L) (любые действия, не затрагивающие сеть)
Сложность получения доступа (АС)	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 (С)			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**).

4.11 Просмотр программ в списке исключений

Оператор поиска угроз не обладает правами для большинства операций с исключениями для программ. Для него доступны два основных 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.

Чтобы оператору просмотреть исключение для программы, ему необходимо перейти на страницу **Наборы исключений для программ** (рис. 33). 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.

Название набора	Количество записей	Привязано агентов
 Набор по умолчанию	53	403
linux-gittlab-runner	20	2
 тест	3	0
1 	0	0
import 	0	0
import 	0	0
empty 	0	0
1541	1	0
set_Exclusion_1 	12	1
set_4 	0	0
set_2 	0	0
software_Exclusion_(TI) 	11	3
 alexb	100	0
linux-test	20	8
 alexb	50	0
...	2	1

Рисунок 33 – Наборы исключений для программ

Информация на странице **Наборы исключений для программ** информация 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 и сетевых исключений происходит таким же образом, как и просмотр исключений для программ.

4.12 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. 34). Профили безопасности позволяют

настраивать нагрузку на систему, увеличивая или уменьшая поток событий, регистрируемых на агенте. Оператору не предоставляется возможность управлять профилями безопасности.

Название профиля	Привязано агентов
Профиль по умолчанию	386
linux	4
kaa_3	2
maxp_test	0
Roman_VM10	2
ssk	0
ПБА_II(Реакция на прямой доступ к жесткому диску - блок) (НЕ РЕДАКТИРОВАТЬ И НЕ УДАЛЯТЬ)	0
ПБА_II(детект. но с глуб скан) (НЕ РЕДАКТИРОВАТЬ И НЕ УДАЛЯТЬ)	0
test-ds-1	0
1	0
--1--	2
ПБА_new	0
test-kn-345	0
Test JP_07	6

Рисунок 34 – 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;

б) 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:

- заблокировать;
- заблокировать 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.

4.13 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 4.

Таблица 4 – Общий список полей событий

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Тип события	enum	t	По умолчанию	Общая
Время регистрации события	timestamp	time	По умолчанию	Общая
Действие, связанное с событием	enum	act	По умолчанию	Общая
Причина предпринятого действия	enum	rsn	По умолчанию	Общая
Правило, относящееся к событию	string	rul	По умолчанию	Общая
Идентификатор техники/тактики MITRE	string	mitre	По умолчанию	Общая
Критичность (уровень важности) события	enum	svrt (по умолчанию: 0)	По умолчанию	Общая
Уникальный идентификатор процесса	int (индекс в массиве GUID'ов)	uuid	Опционально	Общая
Уникальный идентификатор группы процессов	int (индекс в массиве GUID'ов)	huid	Опционально	Общая
Идентификатор процесса на агентской системе	unsigned	pid	По умолчанию	Общая

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Идентификатор родительского процесса на агентской системе	unsigned	ppid	По умолчанию	Общая
Полное имя исполняемого файла процесса	string MANGLED	app	По умолчанию	Общая
Номер сессии, в которой работает процесс на агентской системе	unsigned	sess (по умолчанию: 0)	По умолчанию	Общая
Имя пользователя, запустившего процесс	string	usr	По умолчанию	Общая
Домен (имя компьютера) пользователя, запустившего процесс	string	dom	По умолчанию	Общая
Подтип события	enum	st	По умолчанию	Общая
Поведенческие признаки процесса (первая группа)	uint64	rfo	Опционально	Общая
Поведенческие признаки процесса (вторая группа)	uint64	rf1	Опционально	Общая
Синтетическое событие	int (0/1)	syn	Опционально	Общая
Версия события	unsigned	efmt	Опционально	Общая
Протокол	enum	proto	По умолчанию	Сеть
Признак работы по IPv6	int (0/1)	ipv6	Опционально	Сеть
Идентификатор сетевого потока	int64	flow	Опционально	Сеть
Отправка или прием	int (0/1)	out	Опционально	Сеть
Размер полезных данных (payload) сетевого пакета	int64	size	Опционально	Сеть
Имя хоста, соответствующее удаленному IP-адресу	string	host	По умолчанию	Сеть
Тип DNS-запроса	enum	dnsq_t	Опционально	Сеть
Статус DNS-запроса	unsigned	dnsq_s	Опционально	Сеть

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Результат DNS-запроса	string	dnsq_r	Опционально	Сеть
Имя хоста из DNS-запроса	string	dnsq_h	Опционально	Сеть
Имя хоста (server_name) из сообщения SSL Client Hello	string	ssl_h	Опционально	Сеть
Удаленный IP-адрес	string	r_ip	По умолчанию	Сеть
Удаленный порт	unsigned	r_p	По умолчанию	Сеть
Локальный IP-адрес	string	l_ip	Опционально	Сеть
Локальный порт	unsigned	l_p	По умолчанию	Сеть
Имя хоста в индикаторе компрометации	string	ioc_h	Опционально	Сеть
Полное имя файла	string MANGLED	name	По умолчанию	Файлы
Время создания файла	timestamp	crtime	Опционально	Файлы, Процессы
Время последнего изменения файла	timestamp	chtime	Опционально	Файлы, Процессы
Размер файла	int64	fsize	Опционально	Файлы, Процессы
Тип файла	enum	ftype	Опционально	Файлы, Процессы
Атрибуты файла	unsigned	attr	Опционально	Файлы, Процессы
SHA-1 файла	string	sha1	Опционально	Файлы, Процессы
MD5 файла	string	md5	Опционально	Файлы, Процессы
SHA-256 файла	string	sha256	Опционально	Файлы, Процессы
Электронная подпись файла	string	sgnr	Опционально	Файлы, Процессы
Статус электронной подписи файла	enum	sgnr_s	Опционально	Файлы, Процессы
Оригинальное имя файла	string	ofn	Опционально	Файлы, Процессы
Компания-издатель файла	string	fcomp	Опционально	Файлы, Процессы
Версия файла	string	fver	Опционально	Файлы,

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
				Процессы
Описание файла	string	fdesc	Опционально	Файлы, Процессы
Продукт, к которому относится файл	string	fprod	Опционально	Файлы, Процессы
Тип упаковщика файла	string	pack	Опционально	Файлы, Процессы
Файл расположен в директории автозапуска	int (0/1)	arun	Опционально	Файлы
Новое имя файла	string MANGLED	fnew	Опционально	Файлы
Файл был заменен	int (0/1)	owrt	Опционально	Файлы
Предыдущее время создания файла	timestamp	old_t	Опционально	Файлы
Новое время создания файла	timestamp	new_t	Опционально	Файлы
Файл содержит атрибут "скрытый"	int (0/1)	hdn	Опционально	Файлы
Файл содержит атрибут "системный"	int (0/1)	sys	Опционально	Файлы
Операция совершается над альтернативным потоком данных файла	int (-/1)	ads	Опционально	Файлы
Для файла была создана резервная копия	int (-/1)	save	Опционально	Файлы
Доступ на удаление	int (-/1)	delete	Опционально	Файлы
Доступ на чтение	int (-/1)	read	Опционально	Файлы
Доступ на модификацию	int (-/1)	modify	Опционально	Файлы
Код оповещения	enum	detect	Опционально	Сеть, Файлы, Процессы, Реестр
Флаги исполняемого файла процесса	int64	exclf	Опционально	Сеть, Файлы, Процессы, Реестр

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Полное имя исполняемого модуля–инициатора операции	string MANGLED	who	Опционально	Файлы, Процессы, Реестр
Идентификатор нити–инициатора операции	unsigned	whotid	Опционально	Файлы, Процессы, Реестр
Стартовый адрес нити–инициатора операции	uint64	whoaddr	Опционально	Файлы, Процессы, Реестр
Флаги исполняемого модуля-инициатора операции	uint64	whof	Опционально	Файлы, Процессы, Реестр
Командная строка процесса	string	cmdl	По умолчанию	Процессы
Командная строка родительского процесса	string	cmdlp	По умолчанию	Процессы
Командная строка прародителя (grand parent)	string	cmdlg	Опционально	Процессы
Рабочий каталог процесса	string MANGLED	wdir	Опционально	Процессы
Уровень защиты процесса	unsigned	prot	Опционально	Процессы
Уровень доверия (integrity level) процесса	unsigned	integ	Опционально	Процессы
Время создания процесса	timestamp	when	Опционально	Процессы
Уникальный идентификатор родительского процесса	int (индекс в массиве GUID'ов)	parent	Опционально	Процессы
Уникальный идентификатор процесса-создателя	int (индекс в массиве GUID'ов)	caller	Опционально	Процессы
Идентификатор процесса-инициатора операции	unsigned	cpid	Опционально	Процессы
Полное имя процесса-инициатора операции	string MANGLED	cpath	Опционально	Процессы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
SID пользователя, создавшего процесс	string	sid	По умолчанию	Процессы
Код завершения процесса	unsigned	code	Опционально	Процессы
Уникальный идентификатор целевого процесса	int (индекс в массиве GUID'ов)	targ	Опционально	Процессы
Полное имя целевого процесса	string MANGLED	tpath	По умолчанию	Процессы
Идентификатор целевого процесса	unsigned	tpid	По умолчанию	Процессы
Флаги образа целевого процесса	uint64	targf	Опционально	Процессы
Поведенческие признаки целевого процесса (первая группа)	uint64	trfo	Опционально	Процессы
Поведенческие признаки целевого процесса (вторая группа)	uint64	trfi	Опционально	Процессы
Стек вызовов операции	string	trace	Опционально	Процессы
Имя модуля целевой нити	string	tmod	Опционально	Процессы
Имя функции целевой нити	string	tfunc	Опционально	Процессы
Полное имя файла образа	string MANGLED	path	По умолчанию	Процессы
Флаги нити	unsigned	tf	Опционально	Процессы
Флаги операции загрузки образа	unsigned	ldf	Опционально	Процессы
Флаги образа	int64	imgf	Опционально	Процессы
Базовый адрес образа	int64	base	Опционально	Процессы
Размер образа	unsigned	isize	Опционально	Процессы
Идентификатор целевой нити	unsigned	tid	Опционально	Процессы
Стартовый адрес целевой нити	int64	taddr	Опционально	Процессы
Имя открытого рабочего стола	string	desk	По умолчанию	Процессы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Запрашиваемые права	unsigned	dsrd	Опционально	Процессы
Предоставленные права	unsigned	grnt	Опционально	Процессы
Новый уровень защиты процесса	int	prot1	Опционально	Процессы
Новая командная строка	string	cmdln	Опционально	Процессы
Локальная сессия	int (0/1)	local	Опционально	Сессии
Имя оконной станции	string	win_stn	Опционально	Сессии
Номер сессии	unsigned	sess_id	Опционально	Сессии
Тип дистанционного управления	unsigned (опционально)	sess_opt	Опционально	Сессии
Тип сессии	unsigned (опционально)	sess_proto	Опционально	Сессии
Имя клиента	string (опционально)	sess_cl	Опционально	Сессии
IP-адрес клиента	string (опционально)	sess_claddr	Опционально	Сессии
Имя пользователя	string (опционально)	sess_usr	Опционально	Сессии
Имя домена\компьютера	string (опционально)	sess_dom	Опционально	Сессии
Путь ключа	string	key	По умолчанию	Реестр
Имя значения	string	val_n	По умолчанию	Реестр
Тип данных значения	enum	val_t	Опционально	Реестр
Размер данных значения	unsigned	val_s	Опционально	Реестр
Данные значения	string	val_d	Опционально	Реестр
Новое имя ключа	string	new	Опционально	Реестр
Имя файла-источника загружаемой в реестр информации	string MANGLED	src	Опционально	Реестр
Имя файла, в который записываются данные из реестра	string MANGLED	dst	Опционально	Реестр
Ключ/значение относится к категории автозапуска	int (-/1)	asep	Опционально	Реестр
WMI: Тип события	enum	wmi	По умолчанию	Система: WMI

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
WMI: Путь	string	wmi_pth	По умолчанию	Система: WMI
WMI: SID пользователя	string	wmi_sid	По умолчанию	Система: WMI
WMI: Пространство имен	string	ns	По умолчанию	Система: WMI
WMI: Путь до исполняемого файла	string MANGLED	exe_path	Опционально	Система: WMI
WMI: Имя файла	string MANGLED	fname	Опционально	Система: WMI
WMI: Имя фильтра событий	string	wmi_nm	Опционально	Система: WMI
WMI: Строка запроса	string	qstr	Опционально	Система: WMI
WMI: Имя файла скрипта	string MANGLED	scrfname	Опционально	Система: WMI
WMI: Текст скрипта	string	scrtxt	Опционально	Система: WMI
WMI: Имя источника	string MANGLED	sname	Опционально	Система: WMI
WMI: SMTP	string	smtp	Опционально	Система: WMI
WMI: Фильтр	string	flt	Опционально	Система: WMI
WMI: Потребитель	string	cnsn	Опционально	Система: WMI
WMI: Идентификатор процесса клиента	unsigned (по умолчанию 0)	wmi_clpid	Опционально	Система: WMI
WMI: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	wmi_cluid	Опционально	Система: WMI
WMI: Время создания процесса клиента	timestamp	wmi_cltime	Опционально	Система: WMI
WMI: Командная строка процесса клиента	string	wmi_clcmdl	Опционально	Система: WMI
WMI: Локальный запрос	int (-1)	wmi_local	Опционально	Система: WMI
WMI: Идентификатор созданного процесса	unsigned	wmi_crpid	Опционально	Система: WMI

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
WMI: Уникальный идентификатор созданного процесса	int (индекс в массиве GUID'ов)	wmi_cruuid	Опционально	Система: WMI
WMI: Время создания созданного процесса	timestamp	wmi_crtime	Опционально	Система: WMI
WMI: Командная строка созданного процесса	string	wmi_crcmdl	Опционально	Система: WMI
WMI: Имя машины, выполнившей запрос	string	wmi_cl	Опционально	Система: WMI
WMI: FQDN машины, выполнившей запрос	string	wmi_clfqdn	Опционально	Система: WMI
WMI: Имя пользователя клиента, выполнившего запрос	string	wmi_usr	Опционально	Система: WMI
WMI: Имя домена клиента, выполнившего запрос	string	wmi_dom	Опционально	Система: WMI
WMI: Имя вызываемого метода	string	wmi_mthd	Опционально	Система: WMI
Атаки на Kerberos: Подтип атаки	enum	atck	По умолчанию	Система: Атаки на Kerberos
Golden ticket: Причина	enum	goldent_r	По умолчанию	Система: Атаки на Kerberos
Golden ticket: Имя пользователя	string	goldent_u	Опционально	Система: Атаки на Kerberos
Golden ticket: Имя домена	string	goldent_d	Опционально	Система: Атаки на Kerberos
Golden ticket: IP-адрес	string	goldent_ip	Опционально	Система: Атаки на Kerberos
Silver ticket: Причина	enum	silvert_r	По умолчанию	Система: Атаки на Kerberos
Silver ticket: Имя пользователя	string	silvert_u	Опционально	Система: Атаки на Kerberos

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Silver ticket: Имя домена	string	silvert_d	Опционально	Система: Атаки на Kerberos
Silver ticket: IP-адрес	string	silvert_ip	Опционально	Система: Атаки на Kerberos
Kerberoasting: Причина	enum	kerberoasting_r	По умолчанию	Система: Атаки на Kerberos
Kerberoasting: Имя пользователя	string	kerberoasting_u	Опционально	Система: Атаки на Kerberos
Kerberoasting: Имя домена	string	kerberoasting_d	Опционально	Система: Атаки на Kerberos
Kerberoasting: IP-адрес	string	kerberoasting_ip	Опционально	Система: Атаки на Kerberos
AS-REP roasting: Причина	enum	asreproasting_r	По умолчанию	Система: Атаки на Kerberos
AS-REP roasting: Имя пользователя	string	asreproasting_u	Опционально	Система: Атаки на Kerberos
AS-REP roasting: Имя домена	string	asreproasting_d	Опционально	Система: Атаки на Kerberos
AS-REP roasting: IP-адрес	string	asreproasting_ip	Опционально	Система: Атаки на Kerberos
Новое время	timestamp	new_stime	Опционально	Система: Изменение системного времени
Предыдущее время	timestamp	prev_stime	Опционально	Система: Изменение системного времени
Причина завершения	unsigned	sht	Опционально	Система: Завершение работы
Уровень	unsigned	e_lvl	Опционально	Журналы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Дополнительные данные	JSON object	e_ex	Опционально	Журналы
Описание событий	string (опционально)	e_msg	Опционально	Журналы
Блок информации winlogbeat	JSON object	winlog	Опционально	Журналы
RPC: UUID интерфейса	int (индекс в массиве GUID'ов)	rpc_id	По умолчанию	Вызовы: RPC
RPC: Конечная точка	string	endp	По умолчанию	Вызовы: RPC
RPC: Сетевой адрес	string (опционально)	n_addr	Опционально	Вызовы: RPC
RPC: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	c_uuid	Опционально	Вызовы: RPC
RPC: PID процесса клиента	unsigned	c_pid	По умолчанию	Вызовы: RPC
RPC: Исполняемый файл процесса клиента	string MANGLED	c_path	По умолчанию	Вызовы: RPC
RPC: Уникальный идентификатор процесса сервера	int (индекс в массиве GUID'ов)	s_uuid	Опционально	Вызовы: RPC
RPC: PID процесса сервера	unsigned	s_pid	По умолчанию	Вызовы: RPC
RPC: Исполняемый файл процесса сервера	string MANGLED	s_path	По умолчанию	Вызовы: RPC
Количество открытий/созданий файлов с последующими обращениями к ним	unsigned	cf_ac	Опционально	Защита файлов
Количество открытых файлов из защищаемых каталогов	unsigned	cf_oc	Опционально	Защита файлов
Количество созданных процессом файлов после активации мониторинга	unsigned	cf_cc	Опционально	Защита файлов

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Количество удалённых файлов в защищаемых каталогах	unsigned	si_dc	Опционально	Защита файлов
Количество переименованных файлов в защищаемых каталогах	unsigned	si_rc	Опционально	Защита файлов
Количество перемещённых файлов в защищаемые каталоги	unsigned	si_mi	Опционально	Защита файлов
Количество перемещённых файлов из защищаемых каталогов	unsigned	si_mo	Опционально	Защита файлов
Количество файлов из защищаемых каталогов, которые только читали	unsigned	ro_fc	Опционально	Защита файлов
Количество файлов из защищаемых каталогов, в которые только писали	unsigned	wo_fc	Опционально	Защита файлов
Количество файлов из защищаемых каталогов, которые читали и писали	unsigned	rw_fc	Опционально	Защита файлов
Среднее значений файловой энтропии по чтению	unsigned	pr_re	Опционально	Защита файлов
Среднее значений файловой энтропии по записи	unsigned	pr_we	Опционально	Защита файлов
Правило блокировки процесса	unsigned	pr_lr	Опционально	Защита файлов
Реакция модуля на идентификацию шифровальщика	unsigned	pr_ra	Опционально	Защита файлов

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Количество файлов с нарушенной целостностью	unsigned	a_fcc	Опционально	Защита файлов
Количество файлов с превышенной энтропией	unsigned	a_eoc	Опционально	Защита файлов
Количество расширений файлов из которых читали	unsigned	exrac_	Опционально	Защита файлов
Количество расширений файлов в которые писали	unsigned	exwac_	Опционально	Защита файлов
Количество уникальных расширений файлов из которых только читали	unsigned	exurac	Опционально	Защита файлов
Количество уникальных расширений файлов в которые только писали	unsigned	exuwac	Опционально	Защита файлов
Категории файлов, к которым осуществлялся доступ	unsigned	gf_am	Опционально	Защита файлов
Категории файлов, из которых производилось чтение	unsigned	gf_rm	Опционально	Защита файлов
Категории файлов, в которые производилось запись	unsigned	gf_wm	Опционально	Защита файлов
Категории файлов, которые удалялись	unsigned	gf_dm	Опционально	Защита файлов
Группа, к которой относится файл	unsigned	gf_ai	Опционально	Защита файлов

Типы событий представлены в таблице 5.

Таблица 5 – 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 6.

Таблица 6 – 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)	rfo (опционально)
Поведенческие признаки процесса (вторая группа)	rfl (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 **uids** 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 **rfo**, **rfl**, **ta** и **pa** определяют поведенческий профиль процесса. Поле **rfo** – это runtime-флаги процесса (первая группа); **rfl** – 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 (**rfo**, **rfl**, **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 7.

Таблица 7 – 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: срабатывание компрометации индикатора Обнаружение: индикатора	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 8.

Таблица 8 – 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

Назначение	JSON
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 9.

Таблица 9 – 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

Код события	Имя события	Описание
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 10.

Таблица 10 – Поля событий монитора файловой системы

Назначение	JSON
Полное имя исполняемого модуля-инициатора операции	who
Идентификатор нити-инициатора операции	whotid
Стартовый адрес нити-инициатора операции	whoaddr
Флаги исполняемого модуля-инициатора операции	whof
Полное имя файла	name
Время создания файла	crttime
Время последнего изменения файла	chtime
Размер файла	fsize
Тип файла	ftype
Атрибуты файла	attr
SHA-1 файла	sha1
MD5 файла	md5
SHA-256 файла	sha256
Электронная подпись файла	sgnr
Тип упаковщика файла	pack
Файл расположен в директории автозапуска	arun
Новое имя файла	fnew
Файл был заменен	owrt
Время создания файла до изменения атрибутов	old_t
Время создания файла после изменения атрибутов	new_t
Файл содержит атрибут "скрытый"	hdn

Файл содержит атрибут "системный"	sys
Операция совершается над альтернативным потоком данных файла	ads
Для удаляемого файла была создана резервная копия	save
Код обнаружения	detect
Доступ на удаление	delete
Доступ на чтение	read
Доступ на модификацию	modify

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

Поле **ftype** принимает следующие значения, представленные в таблице 11.

Таблица 11 – 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 12.

Таблица 12 – 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 13.

Таблица 13 – 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 14.

Таблица 14 – 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 15.

Таблица 15 – 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
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

Поле	Тип	Расшифровка
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 16.

Таблица 16 – 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 17.

Таблица 17 – Поля событий монитора процессов

Назначение	JSON
Полное имя исполняемого модуля–инициатора операции	who
Идентификатор нити–инициатора операции	whotid
Стартовый адрес нити–инициатора операции	whoaddr
Флаги исполняемого модуля–инициатора операции	whof
Командная строка процесса	cmdl
Командная строка родительского процесса	cmdlp
Командная строка прародителя (grand parent)	cmdlg
Рабочий каталог процесса	wdir
Уровень защиты процесса	prot
Уровень доверия (integrity level) процесса	integ
Время создания процесса	when
Уникальный идентификатор родительского процесса	parent
Уникальный идентификатор процесса-создателя	caller
Идентификатор процесса-инициатора операции	cpid
Полное имя процесса-инициатора операции	cpath
SID пользователя, создавшего процесс	sid
Код завершения процесса	code
Уникальный идентификатор целевого процесса	targ
Полное имя целевого процесса	tpath
Идентификатор целевого процесса	tpid
Полное имя файла образа	path
Флаги операции загрузки образа	ldf
Флаги образа	imgf
Базовый адрес образа	base
Размер образа	isize
Идентификатор целевой нити	tid
Стартовый адрес целевой нити	taddr
Флаги операции с нитью	tf
Имя открытого рабочего стола	desk
Запрашиваемые права	dsrd
Предоставленные права	grnt
Новый уровень защиты процесса	prot1
Новая командная строка процесса	cmdl1
Размер файла	fsize
Тип файла	ftype
SHA-1 файла	sha1
MD5 файла	md5

Назначение	JSON
SHA-256 файла	sha256
Электронная подпись файла	sgnr
Статус электронной подписи	sgnr_s
Тип упаковщика файла	pack
Атрибуты файла	attr
Время создания файла	crttime
Время последней записи файла	chtime
Оригинальное имя файла	ofn
Компания-издатель файла	fcomp
Версия файла	fver
Описание файла	fdesc
Продукт, к которому относится файл	fprod
Код обнаружения	detect

5.7 События монитора системы

Подтипы событий (**st**) монитора системы представлены в таблице 18.

Таблица 18 – 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 19.

Таблица 19 – 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
WMI: Путь до исполняемого файла	exe_path
WMI: Имя файла	fname
WMI: Имя фильтра событий	wmi_nm

Назначение	JSON
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 20.

Таблица 20 – 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 21:

Таблица 21 – 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 22.

Таблица 22 – 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 23.

Таблица 23 – 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 24.

Таблица 24 – 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 25.

Таблица 25 – 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 26 – 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 27.

Таблица 27 – 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 28.

Таблица 28 – 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 29.

Таблица 29 – Подтипы событий монитора вызовов

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

События монитора вызовов (RPC-вызовы) представлены в таблице 30.

Таблица 30 – 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 статистики

Поля событий статистики работы системы представлены в таблице 31.

Таблица 31 – 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

5.11 События anti-ransomware-модуля

Подтипы событий и их текстовые описания представлены в таблице 32.

Таблица 32 – 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 33.

Таблица 33 – 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

Назначение	JSON
Количество расширений файлов, из которых читали	exrac_
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 задаётся (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 определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый 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 вирусов-шифровальщиков.
APT-атака	Целевая кибератака (таргетированная кибератака) – вид кибератаки, процесс которой контролируется вручную в реальном времени человеком, являющимся центром атаки. Целью данной атаки является хищение защищенной информации из информационной системы конкретной компании, организации или государственной службы.

Термин	Расшифровка термина
ATT&CK	База знаний компании MITRE Corporation, содержащая описание тактик, приемов и методов, используемых киберпреступниками.
Cmd	Команда для запуска интерпретатора команд.
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.

Термин	Расшифровка термина
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.
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.

Термин	Расшифровка термина
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.
TTP	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.
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».