RT Protect EDR

Руководство аналитика

Версия 1.0.24 от 14 октября 2024
Разработано компанией АО «РТ-Информационная безопасность»

RT Protect

Оглавление

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect EDR» Руководство Ааналитика
Версия документа	Версия 1.0.24 (актуально для версии агента 2.0.173.2673, версии фронтенда 2.40.8, версии бекенда 1.21.1-17)
Идентификация программы	«RT Protect EDR»
Идентификация разработчика	АО «РТ-Информационная безопасность»
Уровень доверия	Оценочный уровень доверия 4 (ОУД4)
Идентификация ПЗ	Профиль защиты систем обнаружения вторжений уровня узла типа «У» четвертого класса защиты. ИТ.СОВ.У4.ПЗ. Утвержден ФСТЭК России от 3.02.2012г. Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты ИТ.СКН.П4.ПЗ (утвержден ФСТЭК России от 01.12.2014)
Идентификация ОК	«Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
Ключевые слова	Система обнаружения вторжений, СОВ, ОУД4

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей, осуществляющих функции аналитика и взаимодействующих с программой «RT Protect EDR» (далее Программа) с целью обеспечения ИБ. В документе рассказывается об основных обязанностях аналитика, его возможностях в Программе: основных методах создания аналитических правил, работе с исключениями, профилями защиты и 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, название кнопок меню модуля администрирования Программы
	Обозначения кнопок меню, операций модуля администрирования Программы
Times New Roman/Times New Roman	Перечисление альтернативных вариантов, путь меню, путь файла
	Информация, требующая внимания пользователя
	Информация, связанная с важными конфигурационными настройками и особенностями работы EDR
	Рекомендации и предположения, которые могут помочь в работе с EDR

2. Общие сведения

2.1 Общие сведения о Программе

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

Программа имеет клиент-серверную архитектуру.

Клиентская часть Программы функционирует под управлением ОС согласно следующему списку:

– ОС Windows версий 7, 8, 8.1, 10;

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

– Linux (Ubuntu 18.04, Ubuntu 20.04.5 LTS, Astra SE 1.7_x86-64, Red OS 7.3, Debian GNU/Linux 11 (bullseye) [Linux 5.10.0-19-amd64 x86_64].

Серверная часть Программы функционирует под управлением ОС Linux (Ubuntu 20.04).

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

Примечание

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

Программа предназначена для обработки информации, не являющейся секретной.

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

Посредством интерфейса сервер может передавать на конечные компьютеры правила поведенческого анализа, ставить на контроль различные элементы системы, задавать реакцию на

определенные события, а также получать статистику системной активности хоста, собирать, обобщать и при необходимости предоставлять администратору (аналитику) возможность динамически ее отслеживать.

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

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

Взаимодействие с сервером происходит по протоколу, защищенному с помощью SSL.

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

Программа обеспечивает следующие функции в части СОВ:

– возможность собирать информацию о сетевом трафике, проходящем через контролируемые узлы ИС, о событиях, регистрируемых в журналах аудита операционной системы (ОС), прикладного ПО, о вызове функций, об обращении к ресурсам;

– возможность выполнять анализ собранных Программой данных о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

– возможность обнаруживать вторжения по отношению к контролируемым узлам ИС в режиме, близком к реальному масштабу времени, на уровне отдельных узлов;

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

– возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика и аномалий в действиях пользователя ИС, на заданном уровне эвристического анализа;

– возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;

– возможность уведомлять администратора Программы об обнаруженных вторжениях и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления;

– возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня, базовой эталонной модели взаимосвязи открытых систем;

– возможность автоматизированного обновления базы решающих правил;

– наличие интерфейса администрирования;

– возможность уполномоченным администраторам (ролям) управлять режимом выполнения функций безопасности Программы;

– возможность уполномоченным администраторам (ролям) управлять данными, используемыми функциями безопасности Программы;

– поддержка определенных ролей и их ассоциация с конкретными администраторами Программы и пользователями ИС;

– возможность управления данными функций безопасности Программы в части установления и контроля ограничений на эти данные;

– возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;

– предоставление возможности читать информацию из записей аудита;

– ассоциация каждого события аудита с идентификатором субъекта, его инициировавшего;

– ограничение доступа к чтению записей аудита;

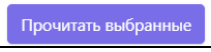
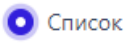
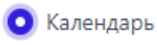
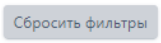
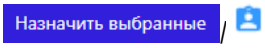
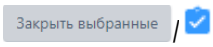
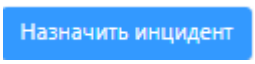
– поиск, сортировка, упорядочение данных аудита.

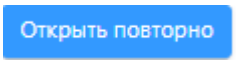
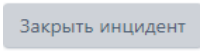
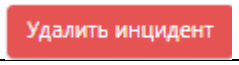
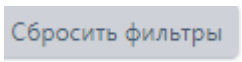
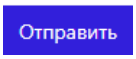
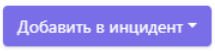
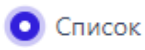
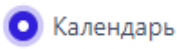
2.2 Используемые в графическом интерфейсе иконки

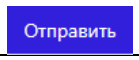
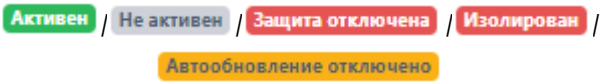
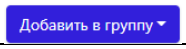
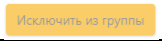
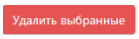
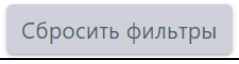
В таблице 3 представлено значение стандартных иконок, используемых в графическом интерфейсе Программы.

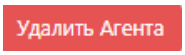
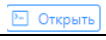
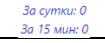
Таблица 3 – Используемые иконки и их назначение

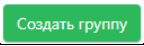
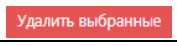
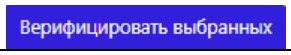
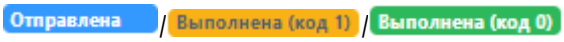
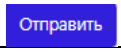
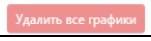
Иконка	Назначение
Иконки верхней панели административного модуля управления на сервере	
	Свернуть/раскрыть боковую панель
	Назначить темную тему оформления страницы

	Назначить светлую тему оформления страницы
	Перейти на страницу Оповещения
	Перейти на страницу Профиль пользователя (открывается при нажатии ЛКМ на имени профиля)
	Выйти из профиля пользователя (открывается при нажатии ЛКМ на имени профиля)
Иконки страницы «Оповещения»	
	Прочитать выбранные оповещения
	Прочитать все оповещения
	Выбрать оповещение
	Отметить оповещение как прочитанное
Иконки страницы «Администрирование»	
	Заблокировать/разблокировать пользователя
Иконки страницы «Инциденты»	
	Выбрать/отменить режим **Список** в настройке периода регистрации инцидента
	Выбрать/отменить режим **Календарь** в настройке периода регистрации инцидента
	Показать графики по динамике инцидентов
	Сбросить все фильтры на странице
	Назначить ответственного за решение выбранного инцидента/назначить инцидент (открыть повторно)
	Закрыть выбранные инциденты
	Выбрать инцидент
	Индикатор активности агента
	Индикатор, сигнализирующий о том, что обнаруженное событие было заблокировано/разрешено
	Индикатор, сообщающий о том, что детектируемое событие является обнаружением (событие с уровнем критичности от среднего и выше)
Иконки страницы «Инцидент»	
	Сохранить файл с отчетом в формате pdf
	Раскрыть дополнительную информацию о событии
	Выбрать событие в инциденте
	Назначить ответственного за решение выбранного инцидента
	Сохранить изменения после редактирования инцидента

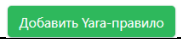
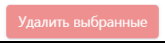
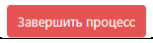
	Открыть инцидент повторно (активна, если инцидент закрыт)
	Закрыть инцидент (кнопка активна для новых и назначенных инцидентов)
	Удалить инцидент
	Создание комментария к инциденту
	Кнопки редактирования комментариев
	Индикатор, показывающий критичность события
	Индикатор, сигнализирующий о том, что обнаруженное событие было заблокировано/разрешено
	Создать исключение с помощью мастера исключений
	Исключить выбранные события из инцидента
Иконки страницы «Активность»	
	Сбросить значения всех фильтров на странице
	Показать примеры запросов на языке DSL
	Отправить DSL-запрос
	Добавить событие в инцидент
	Выбрать/отменить режим Список в настройке периода регистрации события на сервере
	Выбрать/отменить режим Календарь в настройке периода регистрации события на сервере
	Иконка с предупреждением о том, что DSL-запрос желательно изменить для уменьшения нагрузки на поисковую систему базы данных
	Показать/скрыть график распределения событий
	Раскрыть дополнительную информацию о событии
	Выбрать событие
	Загрузка файла с агента в файловое хранилище сервера
	Скопировать хеш в буфер обмена
	Перейти на страницу Процессы и модули для выбранного хеша

	Копирование информации в буфер обмена
	Индикатор, сигнализирующий о том, что обнаруженное событие было заблокировано/разрешено
	Иконка сигнализирующая о том, что вердикт TI – платформы по отношению к артефакту изменился
Иконки страницы «Агенты»	
	Отправить DSL-запрос
	Иконка с предупреждением о том, что DSL-запрос желательно изменить для уменьшения нагрузки на поисковую систему базы данных
	Раскрыть дополнительную информацию об агенте
	Выбрать агента
	Иконка, сигнализирующая о том, что агент функционирует в режиме NO_DRIVER (не работают защитные функции и нет возможности перевести машину с агентом в изоляцию)
	Иконка, информирующая об операционной системе, на которой установлен агент
	Иконки, сообщающие о функциональных состояниях агента
	Открыть терминал для отправки команды выбранному агенту
	Добавить выбранного агента в группу
	Применить настройки конфигурации
	Исключить выбранного агента из группы
	Удалить выбранного агента
	Перейти на страницу с инцидентами, зарегистрированными на агенте
	Скачать список с информацией о агентах в формате CSV
	Сбросить все фильтры выставленные на странице Агенты
	Применить конфигурацию
	Изолировать выбранных агентов
	Отменить изоляцию выбранных агентов
	Включить автоматическое обновление выбранных агентов
	Отключить автоматическое обновление выбранных агентов
	Включить защиту на выбранных агентах
	Выключить защиту на выбранных агентах
	Зафиксировать состояние ПО выбранных агентов в качестве золотого образа

	Отключить отслеживание соответствия состава ПО выбранных агентов в качестве золотого образа
	Включить защиту от удаления агента
	Отключить защиту от удаления агента
	Выполнить команду на выбранных агентах
	Состав ПО на агенте соответствует составу золотого образа
	Имеются отличия в составе ПО на агенте и золотом образе
	Защита от удаления на агенте включена
Иконки страницы «Агент»	
	Сохранить изменения в имени агента
	Скопировать идентификатор агента в буфер обмена
	Перейти к уязвимостям, найденным на агенте
	Кнопка удаления агента (после удаления агент попадает на верификацию, физически с машина)
	Применить конфигурацию набора или профиля для агента
	Перейти к набору или профилю агента
	Перейти к несохраненному набору или профилю агента
	Открыть консоль управления агентом
	Исключить агента из группы
	Изолировать агента/отменить изоляцию агента
	Включить/Выключить функции защиты; Включить/выключить автоматическое обновление агента
	Перейти на страницу зарегистрированных событий агента
	Перейти на страницу зарегистрированных инцидентов агента
	Открыть сканер уязвимостей
	Количество найденных на агенте уязвимостей
	Иконка, сообщающая пользователю о том, что на агенте присутствуют эксплойты (уязвимости, для которых есть готовые программные решения, позволяющие злоумышленникам их эксплуатировать)
	Переход на страницу уязвимости в банке данных угроз безопасности информации ФСТЭК
	Скачать (краткий/полный) отчет об агенте в формате PDF
Иконки страницы «Группы агентов»	
	Раскрыть состав группы
	Выбрать группу
	Удалить агента из группы

	Добавить агента в группу
	Редактировать название группы
	Создать новую группу агентов
	Удалить выбранные группы агентов
Иконки страницы «Верификация Агентов»	
	Раскрыть дополнительную информацию о верифицируемом агенте
	Выбрать агента
	Выполнить верификацию выбранных агентов
Иконки страницы «Терминал»	
	Отображение стадии выполнения команды терминала
	Флаг сортировки для выбора только активных агентов
	Прервать выполнение команды
	Отправить команду на исполнение
Иконки страницы «Графики»	
	Выбор ширины графика (50% или 100%)
	Флаг сортировки для выбора только активных агентов
	Добавить графики
	Удалить все графики
Иконки страницы «Хранилище»	
	Раскрыть дополнительную информацию о загруженном в хранилище файле
	Выбрать файл
	Скопировать информацию в буфер обмена
	Ссылка на страницу Процессы и модули для выбранного файла
	Открыть отчет TI-платформы (файл является безопасным)
	Открыть отчет TI-платформы (файл неизвестный, не удалось найти информацию о том, является файл безопасным или нет)
	Открыть отчет TI-платформы (информация о файле на платформе отсутствует или не проверялась
	Открыть отчет TI-платформы (файл отмечен платформой как вредоносный)
	Открыть отчет TI-платформы (анализ файла платформой выполняется в текущий момент)
	Просмотреть файл в программе просмотра файлов (в кодировке UTF-8 или в бинарном виде)
	Удалить файл

Удалить выбранные	Удалить выбранные файлы из хранилища
	Получить ссылку для скачивания файла на машину, с которой осуществляется доступ в модуль администрирования
Загрузить файл	Загрузить файл с машины, с которой осуществляется доступ в модуль администрирования
Иконки страницы «Наборы YARA-правил», «Наборы исключений для файлов», «Наборы исключений для программ», «Наборы журналов Windows»	
Добавить набор	Добавить новый набор индикаторов
	Применить все наборы индикаторов
Удалить выбранные наборы	Удалить выбранные наборы индикаторов
	Набор не сохранен
	Редактировать набор
	Удалить набор индикаторов
	Применить набор индикаторов
Иконки страницы «Индикаторы компрометации»	
Добавить индикатор	Добавить индикатор
Удалить выбранные	Удалить выбранные индикаторы
	Редактировать индикатор
	Удалить индикатор
	Копировать выбранные элементы в другой набор
	Экспортировать набор в файл
	Импортировать файлы из файла в набор
	Кнопка активации/деактивации правила
	Активировать выбранные элементы
	Деактивировать выбранные элементы
	Скопировать в буфер обмена
	Ссылка на процессы и модули
Иконки страницы «Индикаторы атак»	
Добавить индикатор	Добавить индикатор
Удалить выбранные	Удалить выбранные индикаторы
	Редактировать индикатор
	Удалить индикатор
	Копировать выбранные элементы в другой набор
	Экспортировать набор в файл
	Импортировать файлы из файла в набор
	Кнопка активации/деактивации правила
T1112	Перейти на страницу базы знаний MITRE ATT&CK, связанную с индикатором
	Активировать выбранные элементы

	Деактивировать выбранные элементы
Иконки страницы «YARA-правила», «Исключения для файлов», «Исключения для программ», «Журналы Windows»	
	Добавить правило
	Удалить выбранные правила
	Редактировать правило
	Удалить правило
	Копировать выбранные элементы в другой набор
	Экспортировать набор в файл
	Импортировать файлы из файла в набор
	Кнопка активации/деактивации правила
	Быстрый просмотр YARA-правил
Иконки страницы «Процесс»	
Все события процесса	Показать все события процесса
Ключевые события процесса (0)	Показать ключевые события процесса
	Изменить ориентацию дерева процессов
	Убрать информацию о процессе (оставить только дерево процессов)
	Загрузить в область отображения дополнительное количество процессов
	Кнопка «Завершить процесс»
	Кнопка «Восстановить файлы»
	Скопировать данные в буфер обмена
	Загрузить файл в файловое хранилище
	Ссылка на процессы и модули
Общие иконки для поиска и навигации по страницам	
	Выбрать количество отображаемых элементов на странице
	Переместиться на первую страницу списка
	Переместиться на последнюю страницу списка
	Текущая страница списка
	Переместиться на предыдущую страницу списка
	Переместиться на последующую страницу списка
	Номер страницы списка
	Перемещение при горизонтальной прокрутке вправо
	Перемещение при горизонтальной прокрутке влево
	Перемещение при вертикальной прокрутке вверх
	Перемещение при вертикальной прокрутке вниз
	Раскрыть окно краткой информации об элементе
	Скрыть окно краткой информации об элементе
	Сортировать информацию в столбце по убыванию

↑	Сортировать информацию в столбце по возрастанию
×	Удалить параметра фильтрации в поле
Иконки страницы «Профили защиты данных» и «Профили безопасности агента»	
⚠	Профиль не сохранен
	Редактировать профиль
	Удалить профиль
	Применить профиль
	Применить все профили
Добавить профиль	Добавить профиль
Удалить выбранные профили	Удалить выбранные профили
/	Выбрать/отменить выбор строки с названием профиля защиты
Иконки страницы «Профиль защиты данных» и «Профиль безопасности агента»	
	Отключить/включить модуль защиты данных Отключить/включить резервирование
Применить настройки профиля	Применить настройки профиля
Добавить каталог	Добавить каталог
	Удалить каталог
	Экспортировать профиль в файл
	Импортировать данные из файла в профиль
	Просмотреть поддерживаемые типы данных для резервирования
×	Удалить тип файла из списка для резервирования
	Применить профиль
Иконки страницы «Дистрибутивы»	
	Скачать дистрибутив с сервера управления
	Удалить дистрибутив с сервера управления
Загрузить дистрибутив	Загрузить дистрибутив на сервер управления
Сбросить фильтры	Сбросить все фильтры выставленные на странице
Иконки страницы «Лицензия»	
Загрузить файл лицензии	Кнопка загрузки файла лицензии
Загрузить лицензию	Кнопка загрузки лицензии в формате строки

3. Описание принципов безопасной работы Программы

3.1 Общая информация

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

– 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 **Аналитик** 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 Механизмы собственной безопасности агента RT Protect EDR

В агенте RT Protect EDR реализованы следующие механизмы собственной безопасности:

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

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

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

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

— контроль целостности кода агента в памяти;

— защита от несанкционированного доступа к функциям компонента ядра агента;

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

— ограничение межпроцессного взаимодействия с компонентами агента;

— контроль сетевого взаимодействия из прикладных компонентов агента;

— контроль дочерних процессов прикладных компонентов агента;

— контроль модулей, загружаемых в прикладные компоненты агента;

— защита от внедрения стороннего кода в прикладные компоненты агента;

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

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

3.3 Компрометация паролей

Под компрометацией паролей следует понимать следующее:

— физическую утерю носителя с парольной информацией;

— передачу идентификационной информации по открытым каналам связи;

— перехват пароля при распределении идентификаторов;

— сознательную передачу информации постороннему лицу.

При компрометации пароля пользователь обязан незамедлительно оповестить администратора Программы.

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

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

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

4. Общие сведения об управлении инцидентами

4.1 Общие положения

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

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

Управление инцидентами включает в себя следующие стадии:

– организация деятельности по управлению компьютерными инцидентами;

– обнаружение и регистрация компьютерных инцидентов;

– реагирование на компьютерные инциденты;

– анализ результатов деятельности по управлению компьютерными инцидентами.

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

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

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

– уязвимости в системном и/или прикладном ПО;

– трудности и проблемы при работе с ресурсами ИС (нештатном функционировании программных и аппаратных средств ИС, нарушения целостности информации и т.п.).

Основными видами инцидентов ИБ являются:

1) Разглашение конфиденциальной информации, либо угроза такого разглашения;

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

3) Несанкционированный доступ к ресурсам ИТ-инфраструктуры;

4) Компрометация учетных записей или паролей;

5) Вирусная атака или вирусное заражение;

6) Нарушение или сбой в работе системы резервного копирования.

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

Инциденты информационной безопасности классифицируются согласно таблице 4.

Таблица 4 – Классификация инцидентов ИБ

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

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

– информации об инциденте;

– критичности активов, вовлеченных в инцидент;

– прогнозируемой степени влияния инцидента на ключевые свойства активов.

Таблица 5 – Критичность инцидента ИБ

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

Основные цели реагирования на инциденты:

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

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

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

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

– координация реагирования на инцидент;

– подтверждение/опровержение факта возникновения инцидента ИБ;

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

– обеспечить сохранность и целостность доказательств возникновения инцидента;

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

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

4.2 Реагирование на инциденты

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

Рисунок 1 – Порядок реагирования на инциденты ИБ

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

Пример процедур реагирования аналитика на обнаруженный инцидент можно представить согласно следующему списку:

– изоляция хоста;

– остановка процесса;

– загрузка файла или файлов, связанных с инцидентом, в хранилище файлов;

– проверка файла/файлов средствами TI-платформы;

– предотвращение запуска файла;

– добавление файла в исключения (в случае ложноположительного срабатывания);

– внешний импорт индикаторов (доверенные источники/регулирующие органы);

– проверка инфраструктуры в реальном времени на основе индикаторов с возможностью реакции в «один клик»;

– создание индикаторов угроз с возможностью применения их на всех хостах сразу (в случае, если инцидент представляет реальную угрозу);

– поиск аналогичных событий на других хостах (при обнаружении подозрительной активности на хосте).

4.3 Примеры инцидентов информационной безопасности и их причин

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

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

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

Ниже приведены некоторые примеры инцидентов ИБ и их причин.

4.3.1. Отказ в обслуживании

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

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

– уничтожение ресурсов;

– истощение ресурсов.

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

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

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

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

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

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

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

4.3.2. Сбор информации

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

Подобные инциденты ИБ предполагают разведку с целью определения следующей информации:

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

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

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

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

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

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

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

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

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

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

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

– прямому или косвенному раскрытию или модификации информации;

– хищению интеллектуальной собственности, хранимой в электронной форме;

– нарушению учетности, например, при регистрации учетных записей;

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

Инциденты могут вызываться следующими факторами:

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

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

4.3.3. Несанкционированный доступ

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

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

1) Попытки извлечь файлы с паролями;

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

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

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

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

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

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

5. База знаний MITRE ATT&CK

5.1 Общие сведения и тактики

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

«Выполнение» – целью тактики является запуск злоумышленником вредоносного кода на локальной или удаленной системе. Часто техники, с помощью которых запускается вредоносный код, группируются с техниками из других тактик, чтобы достичь большего, например, исследования сети или кражи данных. Для наглядности можно привести такой пример: злоумышленник использует утилиту удаленного доступа, чтобы запустить Powershell-скрипт, который обнаруживает удаленные системы.

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

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

Примеры повышения привилегий:

– уровень System/root;

– локальный администратор;

– учетная запись пользователя с доступом как у администратора;

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

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

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

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

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

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

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

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

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

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

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

Общий вид матрицы с тактиками представлен на рисунке 2.

Enterprise tactics

Enterprise Tactics: 14

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

Рисунок 2 – Общий вид матрицы ATT&CK

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

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

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

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

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

5.2 Методология анализа киберугроз на основе ATT&CK

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

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

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

5.2.1. Идентификация поведения (шаг 1)

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

Какое поведение является самым распространенным?

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

Какие действия имеют наибольшее влияние?

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

Для какого поведения есть доступные данные?

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

Какое поведение следует детектировать как вредоносное?

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

5.2.2. Получение данных (шаг 2)

На этапе подготовки к созданию аналитики организация должна принять решение, какие данные необходимо обнаружить, собрать и сохранить, чтобы на основе этих данных разработать аналитику. Для этого необходимо определить, какие данные уже были собраны инструментами обнаружения и механизмами логирования. Во многих случаях правила и установки, по которым собираются данные, нуждаются в корректировке, иногда для сбора определенных данных требуется поменять инструменты и механизмы.

Обнаружение на конечных точках

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

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

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

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

Обнаружение на конечных точках должно основываться на идентификации действий после компрометации, так как информация о действиях атакующего внутри периметра имеет большую ценность. На рисунке 3 показано покрытие матрицы ATT&CK методами подхода, основанного на защите внешнего контура периметра.[1]

Рисунок 3 – Подход, основанный на защите внешнего контура периметра, и охват им методологии ATT&CK

[1] На рисунке представлено состояние матрицы атак MITRE на 2017 год.

Ячейки, обозначенные красным цветом, показывают невозможность защищающего предотвратить реализацию атак с применением указанных техник методологии ATT&CK, а ячейки желтого цвета показывают частичную способность предотвращения действий по представленным методам.

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

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

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

5.2.3. Создание аналитики (шаг 3)

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

Создание аналитики требует наличия программной и аппаратной платформы, а также специалистов, которые могут с ними работать. Исследователи MITRE выделяют следующие типы аналитики в методологии ATT&CK:

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

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

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

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

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

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

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

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

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

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

5.2.4. Создание сценария имитации действий злоумышленника (шаг 4)

Традиционное тестирование на проникновение концентрируется на определенной цели, чаще всего в таком сценарии «красная команда» пытается взять под контроль критически важные системы атакуемой сети.

В этом случае команда ограничена выбранной целью и может не учитывать множество дополнительных возможностей при поиске уязвимостей, не связанных с этой целью.

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

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

Во время выполнения тестов для «красной команды» можно назначать определённые цели, но действия ее специалистов должны быть сосредоточены на том, как они собираются достичь этой цели, и не важно, будет ли она достигнута. В этом случае «синяя команда» сможет провести полное тестирование защищаемой сети против наиболее вероятных техник, применяемых злоумышленниками.

Создание сценария

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

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

2) Поведение, которое злоумышленники будут использовать;

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

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

Сценарий имитации действий злоумышленника не обязательно должен быть подробным сценарием. Он должен быть достаточно подробным, чтобы дать «красной команде» направление, в котором нужно

подтвердить тестируемые защитные возможности. При этом сценарий должен быть и достаточно гибким, чтобы «красная команда» могла изменять свои действия по необходимости и применять тестовые вариации, которые еще неизвестны «синей команде». То есть в момент, когда «синяя команда» становится достаточно компетентной, чтобы предотвратить известные угрозы, у «красной команды» должна быть свобода действий для выхода за рамки чистой имитации.

В этом ей должна помочь «белая команда», которая может решить, какое еще поведение может быть протестировано, не уведомляя «синюю команду» о возможных действиях «красной команды». В таком сценарии «белая команда» также сохраняет возможность свободно сообщать «красной команде» детали о защищаемой инфраструктуре, чтобы в полной мере протестировать меры обнаружения против последовательности действий злоумышленников.

Пример сценария

В рассматриваемом сценарии «красная команда» использует функциональные возможности операционной системы Windows и доступные системные утилиты для выполнения определенных действий.

Пользовательские инструменты противника предоставляют доступ через конечные точки и канал C2, но противник предпочитает взаимодействовать с системами через интерактивный интерфейс командной оболочки.

«Синяя команда» разворачивает утилиту Sysmon от Microsoft Sysinternal для постоянного мониторинга действий Красной команды и сбора аргументов командной строки.

Цель этого сценария – проверить и разработать аналитику обнаружения компрометации на основе данных телеметрии, которые собирает Sysmon от конечных точек в действующей сети.

Сценарий высокого уровня:

1) «Красной команде» может быть поставлена конкретная конечная цель, например, получить доступ к определенной системе, учетной записи домена или сбор определенной информации для эксфильтрации.

2) «Красной команде» предоставляется доступ к внутренней системе для проверки компрометирующего поведения.

3) «Красной команде» предоставляется загрузчик или RAT на одной системе для имитации успеха предшествующих компрометирующих действий и получения точки входа.

4) «Красная команда» для продолжения тестирования на проникновение и сбора данных должна использовать методы обнаружения из модели ATT&CK, чтобы узнать больше информации о среде тестирования. Это делается с использованием доступных утилит Windows.

5) «Красная команда» сбрасывает учетные данные в исходную систему и пытается найти поблизости системы, в которых могут использоваться учетные данные.

6) «Красная команда» продвигается внутри защищаемого периметра, пока не будет получена целевая система/аккаунт/информация.

Сценарий высокого уровня используется для построения определенного плана для «красной команды» с использованием ATT&CK как руководства по эмуляции действий злоумышленника.

Выбор техник ориентирован на обычное применение в известных вторжениях, но допускаются некоторые вариации в техниках, используемых «красной командой», чтобы ввести дополнительное поведение.

На рисунке 4 показано матричное представление сценария ATT&CK. Ячейки, выделенные зеленым цветом, изображают техники, необходимые для достижения цели атаки.

Операция может проводиться не очень подробно, с помощью только основных приемов или в качестве более комплексного теста с «красной командой».

Ячейки, выделенные желтым цветом, представляют общие рекомендуемые методы для более полного сценария эмуляции действий противника (см. рис. 4).

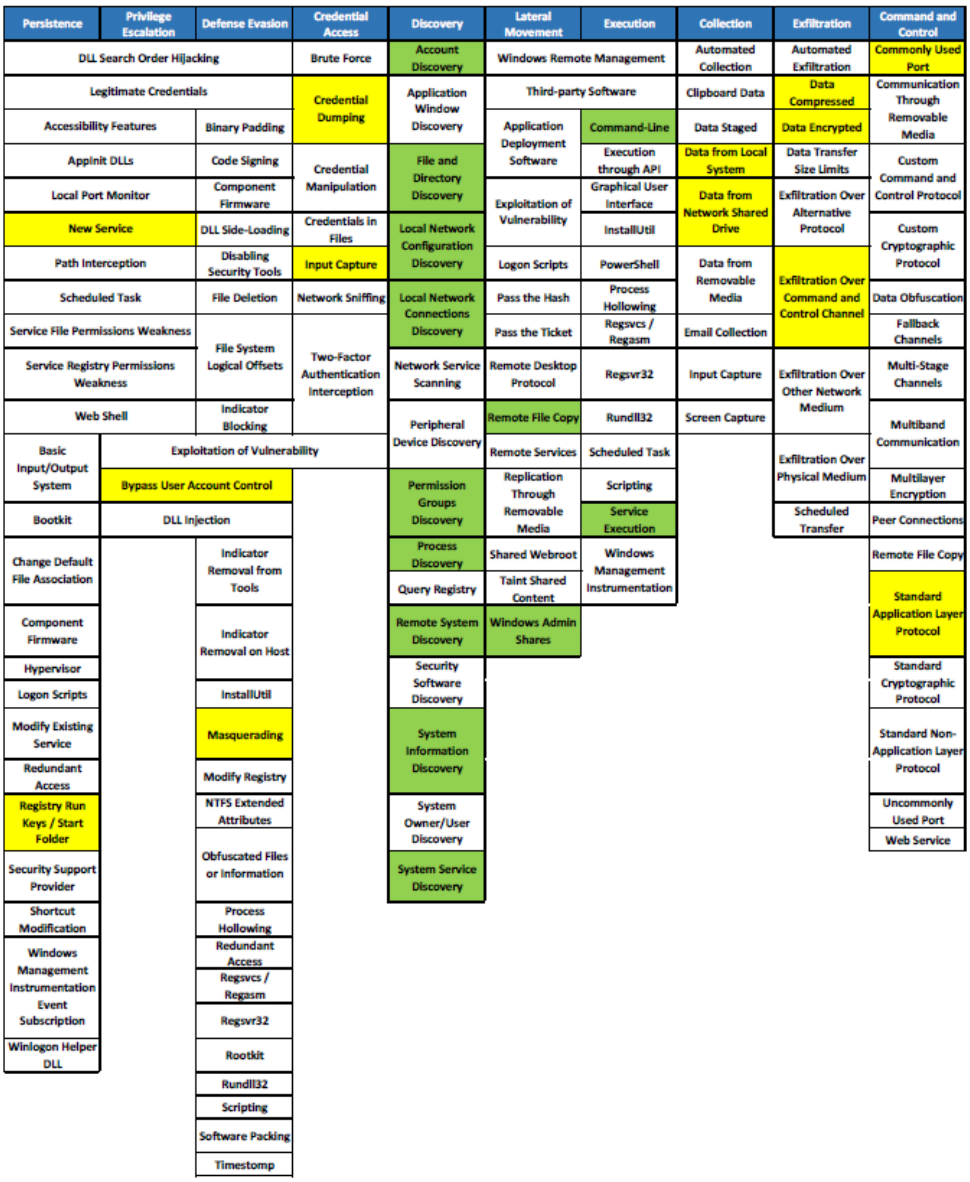


Рисунок 4 – Описание сценария атаки с помощью матрицы ATT&CK

Подробный разбор сценария

Ниже представлена последовательность действий в базе ATT&CK, с помощью которой можно проследить тактики и техники, отображаемые с помощью специальных инструментов и команд.

Пример высокоуровневой последовательности тактик и выбора техник:

Эмулируемый противник добивается исполнения через точку входа, которая может быть предоставлена командой аналитиков. Эта точка входа может представлять собой встроенный протокол в HTTP через TCP-порт 80, который также может использоваться для перемещения дополнительных инструментов в сеть.

Сопоставление техник и тактик представлено в таблице 6.

Таблица 6 – Сопоставление техник и тактик

Тактики ATT&CK	Техники	ID
Контроль и управление	Использование протокола прикладного уровня	T1071
Контроль и управление	Использование общего порта	T1043
Контроль и управление	Удаленное копирование файла	T1105

После установки запускается интерфейс командной строки через инструмент удаленного доступа (см. таблица 7).

Таблица 7 – Сопоставление тактики «Выполнение» и техник

Тактики ATT&CK	Техники	ID	Tool/ Command
Выполнение	Использование интерфейса командной строки	T1059	cmd.exe

Выполняется ряд техник тактики Discovery (**Исследование**) через интерфейс командной строки (см. таблица 8).

Таблица 8 – Сопоставление тактики «Исследование» и техник

Тактики ATT&CK	Техники	ID	Tool/ Command
Исследование	Исследование учетных данных	T1087	net localgroup administrators net group <groupname>/domain net user /domain
Исследование	Исследование файлов и каталогов	T1083	dir cd
Исследование	Исследование конфигурации локальной вычислительной сети	T1016	ipconfig /all
Исследование	Исследование соединений локальной сети	T1049	netstat -ano
Исследование	Исследование групповых разрешений	T1069	net localgroup net group /domain
Исследование	Исследование процессов	T1057	tasklist /v
Исследование	Исследование удаленной системы	T1018	net view
Исследование	Исследование информации о системе	T1082	systeminfo
Исследование	Исследование служб системы	T1007	net start

Тактики ATT&CK	Техники	ID	Tool/ Command

После освоения достаточной информации необходимо использовать нужные тактики и приемы.

Следующие методы основаны на предлагаемых действиях от ATT&CK для того, чтобы перейти к тактике «Постоянство» или «Повышение привилегий». После получения достаточных привилегий следует выгрузить учетные данные с помощью утилиты Mimikatz или попытаться получить учетные данные с помощью «кейлоггера» для захвата пользовательского ввода.

Сопоставление тактик «Закрепление» и «Доступ к учетным данным» и техник (см. таблицу 9).

Таблица 9 – Сопоставление техник и тактик

Тактики ATT&CK	Техники	ID
Закрепление	Новая служба	T1050
Закрепление	Registry Run Keys /Start Folder	T1060
Повышение привилегий, Уклонение от защиты	Прохождение контроля учетных данных пользователя	T1088
Доступ к учетным данным	Сбор учетных данных	T1003
Доступ к учетным данным	Захват ввода	T1056

Если полученные учетные данные и знания от техники «Исследование» достаточны, попытайтесь переместиться в сторону, чтобы выполнить главную цель этого сценария (см. таблицу 10).

Таблица 10 – Сопоставление тактик «Боковое движение» и «Исполнение с техниками

Тактики ATT&CK	Техники	ID	Tool/ Command
Перемещение внутри периметра	Разделение функций администратора Windows	T1077	net use * \\<remote system>\ADMIN$ <password> /user:<domain>\<account>
Перемещение внутри периметра	Удаленное копирование файла	T1105	<source path to file> <remote share destination>
Выполнение	Выполнение службы	T1035	psexec

Продолжить распространение с помощью предыдущих техник с целью использования конфиденциальной информации и ее эксфильтрации.

Файлы могут быть собраны и отфильтрованы с помощью следующих техник (см. таблицу 11).

Таблица 11 – Сопоставление тактик «Сбор информации» и «Эксфильтрация» с техниками

Тактики ATT&CK	Техники	ID
Сбор	Сбор данных из локальной системы	T1005
Сбор	Сбор данных из общего сетевого диска	T1039
Эксфильтрация	Сжатие данных	T1002
Эксфильтрация	Шифрование данных	T1022
Эксфильтрация	Эксфильтрация с помощью контроля и управления	T1041

5.2.5. Имитация угрозы (шаг 5)

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

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

5.2.6. Расследование атаки (шаг 6)

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

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

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

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

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

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

Совет

В RT Protect EDR для поиска скомпрометированных хостов используется раздел **Процессы и модули**.

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

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

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

5.2.7. Оценка действий (шаг 7)

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

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

5.3 Вывод по разделу

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

– детектирование после компрометации;

– фокус на анализе поведения;

– основан на модели угроз;

– итеративность;

– создание аналитики в реальных условиях.

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

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

6. Матрица противодействия киберугрозам MITRE D3FEND

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

Подобно матрице MITRE ATT@CK она содержит тактики и техники, только уже не те, что используются злоумышленниками для нанесения вреда инфраструктуре атакуемого, а те, что помогают эту инфраструктуру защитить (см. рис. 5).

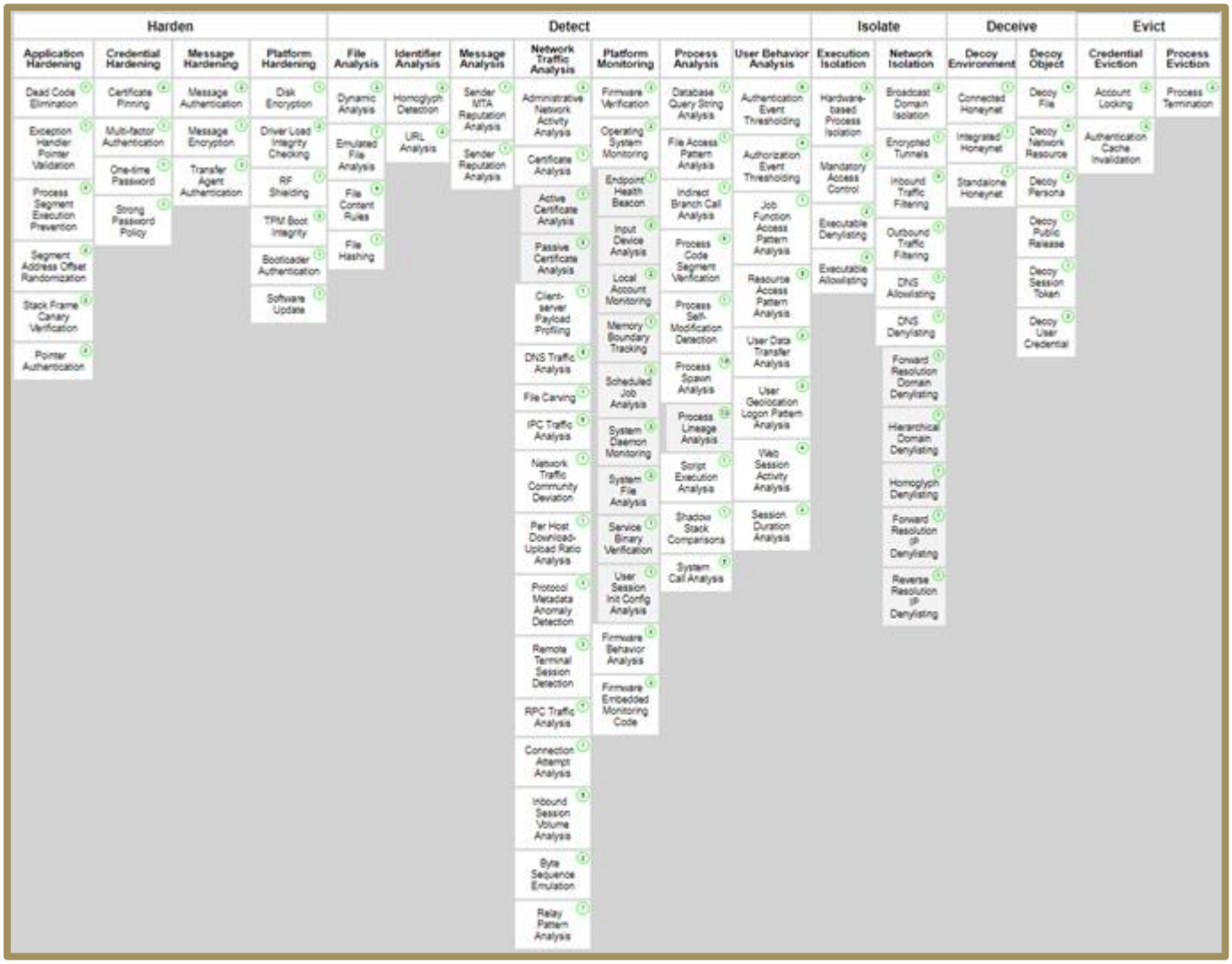


Рисунок 5 – Тактики и техники MITRE D3FEND (версия 0.9.3-BETA-1)

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

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

– программное укрепление;

– укрепление учетных данных;

– укрепление почтовой инфраструктуры;

– укрепление платформы.

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

– анализ файлов;

– анализ идентификаторов;

– анализ почтовых сообщений;

– анализ сетевого трафика;

– мониторинг программного обеспечения и устройств;

– анализ процессов;

– анализ поведения пользователей.

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

– изоляция выполнения;

– сетевая изоляция.

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

– приманка в виде окружения;

– приманка в виде объекта.

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

– удаление скомпрометированных учетных данных;

– уничтожение вредоносных процессов.

7. YARA

7.1 Общие сведения

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

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

Важно

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

7.2 Написание YARA-правил

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

Простейшее правило, которое можно написать для YARA:

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

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

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

Следующие ключевые слова зарезервированы и не могут использоваться в качестве идентификатора:

all , and , any , ascii , at , condition , contains , entrypoint , false , filesize , fullword , for , global , in , import , include , int8 , int16 , int32 , int8be , int16be , int32be , matches , meta , nocase , not , or , of , private , rule , strings , them , true , uint8 , uint16 , uint32 , uint8be , uint16be , uint32be , wide , xor

Правила обычно состоят из двух разделов:

– определение строк (strings definition);

– условие (condition).

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

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

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

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

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

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

7.3 Синтаксис и семантика YARA

7.3.1. Комментарии

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

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

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

7.3.2. Строки

В YARA есть три типа строк:

– шестнадцатеричные строки;

– текстовые строки;

– регулярные выражения.

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

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

7.3.3. Шестнадцатеричные строки

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

– подстановочные знаки;

– переходы (или прыжки);

– альтернативы.

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

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

Ниже представлен пример шестнадцатеричной строки с подстановочными знаками:

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

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

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

В некоторых случаях может потребоваться определить строки с фрагментами переменного содержания и длины. В таких ситуациях можно использовать прыжки вместо подстановочных знаков:

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

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

F4 23 01 02 03 04 62 B4;

F4 23 00 00 00 00 00 62 B4;

F4 23 15 82 A3 04 45 22 62 B4.

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

Допустимые прыжки:

FE 39 45 [0-8] 89 00;

FE 39 45 [23-45] 89 00;

FE 39 45 [1000-2000] 89 00.

Недопустимый прыжок:

FE 39 45 [10-7] 89 00.

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

Вышеупомянутая строка эквивалентна следующим строкам:

FE 39 45 [6-6] 89 00;

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

Начиная с YARA 2.0 также можно использовать неограниченные прыжки:

FE 39 45 [10-] 89 00;

FE 39 45 [-] 89 00.

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

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

```
rule AlternativesExample1
{
  strings:
```

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

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

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

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

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

7.3.4. Текстовые строки

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

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

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

Текстовые строки могут содержать следующее подмножество управляющих последовательностей, доступных в языке C (см. таблица 12).

Таблица 12 – Последовательности в текстовых строках

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

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

7.3.5. Строки без учета регистра

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

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

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

7.4 Модули YARA, доступные в EDR

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

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

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

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

PE – модуль позволяет создавать детализированные правила для исполняемых файлов с помощью атрибутов и функций формата PE-файла. Подробная информация о формате PE-файла содержится в документации Microsoft. Модуль содержит множество атрибутов, функций и переменных, подробно можно ознакомиться в документации YARA.

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

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

7.5 Подробнее о правилах

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

8. Общая информация о работе с инцидентами в Программе

8.1 Категории аналитиков ИБ

Роли аналитиков ИБ подразделяются в Программе на две категории:

– аналитик;

– оператор поиска угроз.

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

Оператор поиска угроз – основной функцией специалиста является поиск неизвестных или неочевидных угроз. Аналитик в роли специалиста по поиску угроз занимается в Программе созданием поисковых запросов или правил и анализом полученных результатов, которые могут указать на ту или иную вредоносную активность или направленную атаку в защищаемой ИТ-инфраструктуре. После этого оператор сможет создать инцидент, в который включит обнаруженные им события.

Примечание

Подробная информация о возможностях работы оператора поиска угроз содержится в документе «Руководство оператора поиска угроз».

При этом необходимо упомянуть, что аналитик обладает теми же самыми возможностями в плане проактивного поиска угроз, что и оператор поиска угроз. Любая организация, эксплуатирующая Программу, может гибко настраивать процесс мониторинга и защиты своей или сторонней инфраструктуры, выбирая, какую роль присвоить тому или иному специалисту, в то же время сохраняя за сотрудником с ролью аналитик возможности самого широкого спектра в сфере информационной безопасности.

8.2 Регистрация инцидентов

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

Способы регистрации инцидентов:

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

2) Создание инцидента вручную при проведении ретроспективных расследований.

Автоматическое создание инцидента проводится на основе правил и алгоритмов, в том числе и средствами машинного анализа. Инцидент выступает в качестве контейнера для событий, однозначно идентифицированных на стороне агента как подозрительные или вредоносные. Инцидент создается при обнаружении событий, критичность которых находится на уровне **Средняя** или выше. В дальнейшем такой инцидент может обогащаться событиями, в том числе более низкой критичности, в течение восьми часов после создания инцидента. Если инцидент взят в работу, то его наполнение событиями останавливается.

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

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

Совет

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

8.2.1. Варианты формирования инцидентов

Вариант 1

Инцидент создается при получении события, у которого значение поля **Критичность** равно или превышает определенный уровень критичности (**Средний** и выше). Инциденту в этом случае присваивается статус **Новый**. Последующие события, относящиеся к этой же пользовательской сессии, добавляются в уже созданный инцидент. Тем самым автоматически собираются все важные события в один инцидент.

События относятся к одной сессии, если у них одинаковое значение поля **sess**, и они принадлежат одной и той же загрузке агентского компьютера. После перезагрузки хоста, на котором установлен агент, события с теми же значениями поля **sess** добавляются в новый инцидент.

Критичность инцидента определяется максимальным уровнем критичности среди всех событий, входящих в этот инцидент.

Вариант 2

При анализе событий, обнаруживаемых на агентах, аналитик может найти подозрительную активность, которую пропустили автоматические средства. Для унификации работы с системой инцидентов аналитику предоставляется возможность самому создать инцидент из события/группы событий.

8.3 Атрибуты инцидентов

Инцидент имеет следующие атрибуты:

1) Внутренний сквозной порядковый номер (*#8219*);
2) Название;
3) Время регистрации;
4) Время действия (от начального события до конечного);

5) Группа/имя агента;

6) Критичность:

– «Информация»;

– «Низкая»

– «Средняя»;

– «Высокая»;

– «Критичная»;

7) Ответственный;

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

Совет

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

---

9) Статус:

– «Новый»;

– «Назначен»;

– «Закрыт»;

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

В случае создания инцидента вручную, ответственным за его решение назначается аналитик, создавший инцидент. Статус **Назначен** означает, что ответственный за инцидент сотрудник взял инцидент в работу и проводит расследование. Состояние инцидента **Закрыт** означает, что аналитик обработал события инцидента и закрыл его. Инцидент может открываться повторно, для этого необходимо в закрытом инциденте

нажать кнопку **Открыть повторно** или нажать кнопку  (**Назначение инцидентов (открыть повторно)**) на странице **Инциденты**.

Критичность инцидента, созданного автоматически, устанавливается равной критичности события-обнаружения, на основе которого создан инцидент. В остальных случаях дефолтное значение критичности **Высокая**.

Подробно работа с интерфейсом страницы **Инциденты** рассмотрена в подразделе 10.3.

8.4 Удаление инцидентов

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

Примечание

Вместе с инцидентом удаляются события, входящие в этот инцидент.

---

9. Модель данных в событиях активности

9.1 Общие сведения

События, зарегистрированные агентом, отправляются на сервер в формате JSON. Отправка событий с агента осуществляется блоками. Каждый блок содержит заголовок и массив событий разного типа. Каждое событие включает в себя 2 набора полей – общий набор и набор, специфичный для определенного вида события. Полный список полей событий и их JSON-представления, которые могут быть применены для написания DSL-запросов или индикаторов атак, представлен в таблице 13.

Таблица 13 – Общий список полей событий

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

Назначение	Тип данных	JSON	Подсистема
Поведенческие признаки процесса (первая группа)	uint64	**rf0**	Общая
Поведенческие признаки процесса (вторая группа)	uint64	**rf1**	Общая
Флаги исполняемого файла процесса	int64	**exclf**	Общая
Синтетическое событие (принимает значения true или false)	int (0/1)	**syn**	Общая
Версия события	unsigned	**efmt**	Общая
Протокол	enum	**proto**	Сеть
Признак работы по IPv6 (принимает значения true или false)	int (0/1)	**ipv6**	Сеть
Уникальный идентификатор сетевого потока	string (индекс в массиве GUID'ов в текстовой форме)	**fluuid**	Сеть
Идентификатор сетевого потока	int64	**flow**	Сеть
Отправка или прием (принимает значения true или false)	int (0/1)	**out**	Сеть
Размер полезных данных (payload) сетевого пакета	int64	**size**	Сеть
Имя хоста, соответствующее удаленному IP-адресу	string	**host**	Сеть
Тип DNS-запроса	enum	**dnsq_t**	Сеть
Статус DNS-запроса	unsigned	**dnsq_s**	Сеть
Результат DNS-запроса	string	**dnsq_r**	Сеть
Имя хоста из DNS-запроса	string	**dnsq_h**	Сеть
Имя хоста (server_name) из сообщения SSL Client Hello	string	**ssl_h**	Сеть
Удаленный IP-адрес	string	**r_ip**	Сеть
Удаленный порт	unsigned	**r_p**	Сеть
Локальный IP-адрес	string	**l_ip**	Сеть
Локальный порт	unsigned	**l_p**	Сеть
Имя хоста в индикаторе компрометации	string	**ioc_h**	Сеть
Флаги сетевого события	unsigned	**netf**	Сеть
Имя хоста в сетевом исключении	string	**excl_h**	Сеть
Полное имя файла	string MANGLED	**name**	Файлы, Защита данных
Время создания файла	timestamp	**crtime**	Файлы, Процессы
Время последнего изменения файла	timestamp	**chtime**	Файлы, Процессы
Размер файла	int64	**fsize**	Файлы, Процессы

Назначение	Тип данных	JSON	Подсистема
Тип файла	enum	**ftype**	Файлы, Процессы
Атрибуты файла	unsigned	**attr**	Файлы, Процессы
SHA-1 файла	string	**sha1**	Файлы, Процессы
MD5 файла	string	**md5**	Файлы, Процессы
SHA-256 файла	string	**sha256**	Файлы, Процессы
Электронная подпись файла	string	**sgnr**	Файлы, Процессы
Статус электронной подписи файла	enum	**sgnr_s**	Файлы, Процессы
Оригинальное имя файла	string	**ofn**	Файлы, Процессы
Компания-издатель файла	string	**fcomp**	Файлы, Процессы
Версия файла	string	**fver**	Файлы, Процессы
Описание файла	string	**fdesc**	Файлы, Процессы
Продукт, к которому относится файл	string	**fprod**	Файлы, Процессы
Тип упаковщика файла	string	**pack**	Файлы, Процессы
Файл расположен в директории автозапуска (принимает значения true или false)	int (0/1)	**arun**	Файлы
Новое имя файла	string MANGLED	**fnew**	Файлы
Файл был заменен (принимает значения true или false)	int (0/1)	**owrt**	Файлы
Предыдущее время создания файла	timestamp	**old_t**	Файлы
Новое время создания файла	timestamp	**new_t**	Файлы
Файл содержит атрибут "скрытый" (принимает значения true или false)	int (0/1)	**hdn**	Файлы
Файл содержит атрибут "системный" (принимает значения true или false)	int (0/1)	**sys**	Файлы
Операция совершается над альтернативным потоком данных файла (принимает значение только true)	int (-/1)	**ads**	Файлы
Для файла была создана резервная копия (принимает значение только true)	int (-/1)	**save**	Файлы

Назначение	Тип данных	JSON	Подсистема
Доступ на удаление (принимает значение только true)	int (-/1)	**delete**	Файлы
Доступ на чтение (принимает значение только true)	int (-/1)	**read**	Файлы
Доступ на модификацию (принимает значение только true	int (-/1)	**modify**	Файлы
Обмен именами (принимает значение только true) (поле доступно только в ОС Linux)	int (-/1)	**nxchg**	Файлы
Код оповещения	enum	**detect**	Сеть, Файлы, Процессы, Реестр
Полное имя исполняемого модуля–инициатора операции	string MANGLED	**who**	Файлы, Процессы, Реестр
Идентификатор нити–инициатора операции	unsigned	**whotid**	Файлы, Процессы, Реестр
Стартовый адрес нити–инициатора операции	uint64	**whoaddr**	Файлы, Процессы, Реестр
Флаги исполняемого модуля-инициатора операции	uint64	**whof**	Файлы, Процессы, Реестр
Стек вызовов операции	string	**trace**	Процессы
Командная строка родительского процесса	string	**cmdlp**	Процессы
Командная строка прародителя (grand parent)	string	**cmdlg**	Процессы
Рабочий каталог процесса	string MANGLED	**wdir**	Процессы
Уровень защиты процесса	unsigned	**prot**	Процессы
Уровень доверия (integrity level) процесса	unsigned	**integ**	Процессы
Время создания процесса	timestamp	**when**	Процессы
Уникальный идентификатор родительского процесса	int (индекс в массиве GUID'ов)	**parent**	Процессы
Уникальный идентификатор процесса-создателя	int (индекс в массиве GUID'ов)	**caller**	Процессы
Идентификатор процесса-инициатора операции	unsigned	**cpid**	Процессы
Полное имя процесса-инициатора операции	string MANGLED	**cpath**	Процессы
Код завершения процесса	unsigned	**code**	Процессы
Уникальный идентификатор целевого процесса	int (индекс в массиве GUID'ов)	**targ**	Процессы

Назначение	Тип данных	JSON	Подсистема
Полное имя целевого процесса	string MANGLED	**tpath**	Процессы
Идентификатор целевого процесса	unsigned	**tpid**	Процессы
Флаги образа целевого процесса	uint64	**targf**	Процессы
Поведенческие признаки целевого процесса (первая группа)	uint64	**trf0**	Процессы
Поведенческие признаки целевого процесса (вторая группа)	uint64	**trf1**	Процессы
Имя модуля целевой нити	string	**tmod**	Процессы
Имя функции целевой нити	string	**tfunc**	Процессы
Полное имя файла образа	string MANGLED	**path**	Процессы
Флаги нити	unsigned	**tf**	Процессы
Флаги операции загрузки образа	unsigned	**ldf**	Процессы
Флаги образа	int64	**imgf**	Процессы
Базовый адрес образа	int64	**base**	Процессы
Размер образа	unsigned	**isize**	Процессы
Идентификатор целевой нити	unsigned	**tid**	Процессы
Стартовый адрес целевой нити	int64	**taddr**	Процессы
Запрашиваемые права	unsigned	**dsrd**	Процессы
Предоставленные права	unsigned	**grnt**	Процессы
Новый уровень защиты процесса	int	**prot1**	Процессы
Новая командная строка	string	**cmdl1**	Процессы
Локальная сессия (принимает значения true или false)	int (0/1)	**local**	Сессии
Номер сессии	unsigned	**sess_id**	Сессии
Тип дистанционного управления	unsigned (опционально)	**sess_opt**	Сессии
Тип сессии	unsigned (опционально)	**sess_proto**	Сессии
Имя оконной станции	string	**win_stn**	Сессии
Имя клиента	string (опционально)	**sess_cl**	Сессии
IP-адрес клиента	string (опционально)	**sess_claddr**	Сессии
Имя пользователя	string (опционально)	**sess_usr**	Сессии
Имя домена\компьютера	string (опционально)	**sess_dom**	Сессии
Путь ключа	string	**key**	Реестр
Имя значения	string	**val_n**	Реестр
Тип данных значения	enum	**val_t**	Реестр
Размер данных значения	unsigned	**val_s**	Реестр
Данные значения	string	**val_d**	Реестр
Новое имя ключа	string	**new**	Реестр
Имя файла-источника загружаемой в реестр информации	string MANGLED	**src**	Реестр

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

Назначение	Тип данных	JSON	Подсистема
Golden ticket: Причина	enum	**goldent_r**	Система: Атаки на Kerberos
Golden ticket: Имя пользователя	string	**goldent_u**	Система: Атаки на Kerberos
Golden ticket: Имя домена	string	**goldent_d**	Система: Атаки на Kerberos
Golden ticket: IP-адрес	string	**goldent_ip**	Система: Атаки на Kerberos
Silver ticket: Причина	enum	**silvert_r**	Система: Атаки на Kerberos
Silver ticket: Имя пользователя	string	**silvert_u**	Система: Атаки на Kerberos
Silver ticket: Имя домена	string	**silvert_d**	Система: Атаки на Kerberos
Silver ticket: IP-адрес	string	**silvert_ip**	Система: Атаки на Kerberos
Kerberoasting: Причина	enum	**kerberoasting_r**	Система: Атаки на Kerberos
Kerberoasting: Имя пользователя	string	**kerberoasting_u**	Система: Атаки на Kerberos
Kerberoasting: Имя домена	string	**kerberoasting_d**	Система: Атаки на Kerberos
Kerberoasting: IP-адрес	string	**kerberoasting_ip**	Система: Атаки на Kerberos
AS-REP roasting: Причина	enum	**asreproasting_r**	Система: Атаки на Kerberos
AS-REP roasting: Имя пользователя	string	**asreproasting_u**	Система: Атаки на Kerberos
AS-REP roasting: Имя домена	string	**asreproasting_d**	Система: Атаки на Kerberos
AS-REP roasting: IP-адрес	string	**asreproasting_ip**	Система: Атаки на Kerberos
Новое время	timestamp	**new_stime**	Система: Изменение системного времени
Предыдущее время	timestamp	**prev_stime**	Система: Изменение системного времени
Причина завершения	unsigned	**sht**	Система: Завершение работы

Назначение	Тип данных	JSON	Подсистема
Уровень	unsigned	**e_lvl**	Журналы
Дополнительные данные	JSON object	**e_ex**	Журналы
Описание событий	string (опционально)	**e_msg**	Журналы
Блок информации **winlogbeat**	JSON object	**winlog**	Журналы
RPC: UUID интерфейса	int (индекс в массиве GUID'ов)	**rpc_id**	Вызовы: RPC
RPC: Конечная точка	string	**endp**	Вызовы: RPC
RPC: Сетевой адрес	string (опционально)	**n_addr**	Вызовы: RPC
RPC: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	**c_uuid**	Вызовы: RPC
RPC: PID процесса клиента	unsigned	**c_pid**	Вызовы: RPC
RPC: Исполняемый файл процесса клиента	string MANGLED	**c_path**	Вызовы: RPC
RPC: Уникальный идентификатор процесса сервера	int (индекс в массиве GUID'ов)	**s_uuid**	Вызовы: RPC
RPC: PID процесса сервера	unsigned	**s_pid**	Вызовы: RPC
RPC: Исполняемый файл процесса сервера	string MANGLED	**s_path**	Вызовы: RPC
Количество открытий/созданий файлов с последующими обращениями к ним	unsigned	**cf_ac**	Защита файлов
Количество открытых файлов из защищаемых каталогов	unsigned	**cf_oc**	Защита файлов
Количество созданных процессом файлов после активации мониторинга	unsigned	**cf_cc**	Защита файлов
Количество удалённых файлов в защищаемых каталогах	unsigned	**si_dc**	Защита файлов
Количество переименованных файлов в защищаемых каталогах	unsigned	**si_rc**	Защита файлов
Количество перемещённых файлов в защищаемые каталоги	unsigned	**si_mi**	Защита файлов
Количество перемещённых файлов из защищаемых каталогов	unsigned	**si_mo**	Защита файлов
Количество файлов из защищаемых каталогов, которые только читали	unsigned	**ro_fc**	Защита файлов
Количество файлов из защищаемых каталогов, в которые только писали	unsigned	**wo_fc**	Защита файлов
Количество файлов из защищаемых каталогов, которые читали и писали	unsigned	**rw_fc**	Защита файлов
Среднее значений файловой энтропии по чтению	unsigned	**pr_re**	Защита файлов
Среднее значений файловой энтропии по записи	unsigned	**pr_we**	Защита файлов
Правило блокировки процесса	unsigned	**pr_lr**	Защита файлов

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

Примечание

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

Типы событий представлены в таблице 14.

Таблица 14 – 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 15.

Таблица 15 – Поля общей части событий

Назначение	JSON	Тип
Тип события	**t**	unsigned
Время регистрации события (в формате UTC)	**time**	timestamp
Действие, связанное с событием (0 – блокировать, 1 – разрешить, 2 – продолжить наблюдение)	**act** (по умолчанию – 2)	unsigned
Причина предпринятого действия	**rsn**	unsigned
Правило, относящееся к событию	**rul**	string
Идентификатор техники/тактики MITRE	**mitre**	string
Критичность (уровень важности) события	**svrt** (по умолчанию – 0)	unsigned
Уникальный идентификатор процесса	**uuid**	int (индекс в массиве GUID'ов)
Уникальный идентификатор группы процессов	**hid**	string (индекс в массиве GUID'ов)
Уникальный идентификатор корреляции событий	**cid**	string (индекс в массиве GUID'ов)
Идентификатор процесса на агентской системе	**pid**	unsigned
Идентификатор родительского процесса на агентской системе	**ppid**	unsigned
Полное имя (вместе с путем) исполняемого модуля процесса	**app**	string MANGLED
Командная строка процесса	**cmdl**	string (index string 2650+)
Номер сессии, в которой работает процесс на агентской системе	**sess** (по умолчанию – 0)	unsigned
SID пользователя, запустившего процесс	**sid**	string
Издатель ЭП исполняемого файла процесса	**app_sgnr**	string
Имя пользователя, запустившего процесс	**usr**	string
Домен (имя компьютера) пользователя, запустившего процесс	**dom**	string
Подтип события (интерпретируется в зависимости от типа)	**st**	unsigned
Поведенческие признаки процесса (первая группа)	**rf0**	uint64
Поведенческие признаки процесса (вторая группа)	**rf1**	uint64
Флаги исполняемого файла процесса	**exclf**	uint64
Синтетическое событие (0 или 1)	**syn**	int (0/1)
Версия события	**efmt**	unsigned

В поле **time** передается UTC-время регистрации события. Система построена таким образом, что в штатной ситуации в пределах одного агента не бывает событий с одинаковым значением поля **time**. Если

события зарегистрированы в одно и то же время, то между ними вносится временной сдвиг, который для последующих событий компенсируется за счет естественного течения времени.

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

Критичность события может принимать следующие значения:

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

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

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

MORE_PROCESSING (код 2, значение по умолчанию, т.е. непосредственно в теле события этот код не передается) – трактуется по-разному в зависимости от контекста. В контексте события телеметрии означает, что

никакого действия, связанного с событием, не предпринято. В контексте обнаружения (alert) код 2 означает, что логика обнаружения не предписывает никакого действия, кроме фиксации самого факта обнаружения – обнаруженная активность не блокируется, что не отменяет самого факта ее обнаружения. Для события телеметрии поля **rsn** и **rul**, как правило (но необязательно), не заполняются, а для события-обнаружения поле **rul** содержит правило, идентифицирующее обнаружение. И тогда поле **rsn**, как и в других случаях, содержит причину, по которой установлена такая реакция на обнаружение.

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

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

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

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

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

Поле **syn** устанавливается в 1, если событие, которое в обычной ситуации отражает реально имеющую место активность агента, в данном конкретном случае является синтезированным, т.е. исскуственным. Например, если агентский модуль деактивируется, то он публикует синтетические события завершения процессов системы, за которыми он наблюдает и для которых были отправлены события старта процесса. И

наоборот, при запуске агентского модуля "на лету" сразу после установки (или его активации после деактивации), когда в системе уже работают те или иные процессы, агент публикает синтетические события создания этих процессов. Это позволяет сохранять целостную картину состояния агентской системы с точки зрения административного модуля в разных сценариях работы агента.

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

Расшифровки и коды поля **detect** представлены в таблице 16.

Таблица 16 – Расшифровка значений поля detect

Значение	Расшифровка
2001	Попытка чтения значения, содержащего конфиденциальную информацию
2002	Попытка дампа ключа, содержащего конфиденциальную информацию
4012	Подмена образа процесса в памяти: общая техника
4013	Нарушение функции защиты (фильтр создания/завершения процессов)
4014	Нарушение функции защиты (фильтр загрузки модулей)
4015	Нарушение функции защиты (фильтр создания/завершения нитей)
4016	Нарушение функции защиты (фильтр доступа к объектам)
4017	Нарушение функции защиты (фильтр реестровых операций)
4018	Нарушение функции защиты (фильтр файловых операций)
4019	Нарушение функции защиты (контроль фильтров)
4020	Нарушение функции защиты (верификация драйвера)
4021	Нарушение целостности системного компонента защиты
4022	Нарушение целостности прикладного компонента защиты
4023	Дампинг памяти процесса LSASS (кража credentials)
4024	Исполнение shell-кода (потенциальный эксплойт)
4025	Нарушение функции защиты (нет функции уничтожения нити)
4026	Кража описателя процесса LSASS (потенциальный дампинг памяти LSASS)
4027	Недопустимый доступ к критическому системному процессу
4028	Нарушение целостности компонента контроля USB устройств
4029	Обнаружена сигнатура вредоносного кода в памяти процесса
4030	Shellcode внутри прикладного компонента защиты

Расшифровки и коды поля **rsn** представлены в таблице 17.

Таблица 17 – Значения поля rsn

Значение	Расшифровка
4	Политика собственной безопасности
7	Политика в отношении создания нити в стороннем процесса

8	Политика в отношении доступа к стороннему процессу/нити
9	Политика в отношении входящих сетевых соединений
10	Сетевое исключение
11	Исключение для программ
12	Исключение для индикаторов атак
13	Сетевая сигнатура
14	Сетевая изоляция
15	YARA-правило
18	Процесс имеет характерные признаки вируса-шифровальщика
19	Файловый индикатор компрометации
20	Файловое исключение
21	Встроенный индикатор атак
22	Политика в отношении защищенных процессов
23	Статический анализ файла
26	Индикатор атак
32	Реакция на доступ к стороннему процессу/нити (профиль безопасности агента)
33	Реакция на создание нити в стороннем процессе (профиль безопасности агента)
35	Реакция на прямой доступ к жесткому диску (профиль безопасности агента)
37	Блокирующее действие отменено в текущем контексте
38	Сетевой индикатор компрометации
39	Глубокий анализ сетевого пакета
40	Политика противодействия вирусам-шифровальщикам
45	Блокирующее действие не реализовано
46	Блокирующее действие отменено в режиме "только детектирование"
47	Политика в отношении взаимодействия дружественных процессов
48	Политика доступа к USB-устройствам

9.2 События мониторинга сети

При любых сетевых взаимодействиях и проверках, которые осуществляются между агентом и удаленным компьютером, будь то матчинг индикаторов атак, индикаторов компрометации, в сетевых исключениях и т.д. важен прежде всего удаленный хост, его имя, IP-адрес и порт, то есть на него идет основное внимание в момент сетевого соединения.

Подтипы событий (**st**) и их текстовые описания представлены в таблице 18.

Таблица 18 – События монитора сети

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

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

Поля сетевых событий представлены в таблице 19.

Таблица 19 – Поля сетевых событий

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

9.3 События мониторинга файловых операций

Подтипы событий (**st**) мониторинга файловых операций и их текстовые описания представлены в таблице 20.

Таблица 20 – События мониторинга файловых операций

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

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

Поля событий мониторинга файловой системы представлены в таблице 21.

Таблица 21 – Поля событий мониторинга файловой системы

Назначение	JSON	Тип
Полное имя исполняемого модуля-инициатора операции	**who**	string MANGLED

Идентификатор нити-инициатора операции	**whotid**	unsigned
Стартовый адрес нити-инициатора операции	**whoaddr**	uint64
Флаги исполняемого модуля-инициатора операции	**whof**	uint64
Стек вызовов операции	**trace**	string
Полное имя файла	**name**	string MANGLED
Время создания файла	**crtime**	timestamp
Время последнего изменения файла	**chtime**	timestamp
Размер файла	**fsize**	int64
Тип файла	**ftype**	enum
Атрибуты файла	**attr**	unsigned
SHA-1 файла	**sha1**	string
MD5 файла	**md5**	string
SHA-256 файла	**sha256**	string
Электронная подпись файла	**sgnr**	string
Статус электронной подписи файла	**sgnr_s**	enum
Оригинальное имя файла	**ofn**	string
Компания-издатель файла	**fcomp**	string
Версия файла	**fver**	string
Описание файла	**fdesc**	string
Продукт, к которому относится файл	**fprod**	string
Тип упаковщика файла	**pack**	string
Файл расположен в директории автозапуска	**arun**	int (-/1)
Новое имя файла	**fnew**	string MANGLED
Файл был заменен	**owrt**	int (-/1)
Время создания файла до изменения атрибутов	**old_t**	timestamp
Время создания файла после изменения атрибутов	**new_t**	timestamp
Файл содержит атрибут "скрытый"	**hdn**	int (0/1)
Файл содержит атрибут "системный"	**sys**	int (0/1)
Операция совершается над альтернативным потоком данных файла	**ads**	int (-/1)
Для удаляемого файла была создана резервная копия	**save**	int (-/1)
Код обнаружения	**detect**	unsigned
Доступ на удаление	**delete**	int (-/1)
Доступ на чтение	**read**	int (-/1)
Доступ на модификацию	**modify**	int (-/1)
Обмен именами (доступен только в Linux)	**nxchg**	int (-/1)

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

Поле **ftype** принимает следующие значения, представленные в таблице 22.

Таблица 22 – Значение поля ftype

Значение	Описание
2	PE
3	Active content
4	PowerShell script

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

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

– 0 (нет подписи);

– 1 (есть подпись);

– 2 (неизвестно).

Примечание

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

9.4 События монитора реестра

Подтипы событий (**st**) мониторинга реестра и их текстовые описания представлены в таблице 23.

Таблица 23 – Подтипы событий мониторинга реестра

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

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

Поля событий монитора реестра представлены в таблице 24.

Таблица 24 – Поля событий мониторинга реестра

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

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

9.5 События системного журнала Windows (ETW)

Подтипы событий и их текстовые описания представлены в таблице 25.

Таблица 25 – Поля событий системного журнала Windows

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

События формата winlogbeat могут принимать значения, представленные в таблице 26.

Таблица 26 – 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
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

9.6 События мониторинга процессов

Подтипы событий и их текстовые описания представлены в таблице 27.

Таблица 27 – Подтипы событий мониторинга процессов и их тестовые описания

Код события	Имя события	Описание
0	Процессы: Загрузка драйвера	Загрузка драйвера **path**
1	Процессы: Старт процесса	Старт процесса командой **cmdl** из **cpath** (**cpid**), нить = **whotid** (из модуля **who**)
2	Процессы: Завершение процесса	Завершение процесса с кодом **code**
3	Процессы: Загрузка образа	Загрузка образа **path**

Код события	Имя события	Описание
6	Процессы: Доступ к процессу	Доступ к процессу **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd**-**grnt**}, нить=**whotid** (из модуля **who**)
7	Процессы: Создание нити в стороннем процессе	Создание нити **tid** в процессе **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
13	Процессы: Обнаружение: подмена командной строки*	Подмена командной строки с **cmdl1** на **cmdl**
16	Процессы: Обнаружение: изменение системной защиты процесса*	Изменение системной защиты процесса с **prot** на **prot1**
18	Процессы: Доступ к нити процесса	Доступ к нити **tid** процесса **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd**-**grnt**}, нить = **whotid** (из модуля **who**)
20	Процессы: Загрузка образа в сторонний процесс	Загрузка образа **path** в процесс **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
23	Процессы: Другие обнаружения*	Описание кода **detect**

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

Поля событий мониторинга процессов представлены в таблице 28.

Таблица 28 – Поля событий мониторинга процессов

Назначение	JSON	Тип
Полное имя исполняемого модуля–инициатора операции	**who**	string MANGLED
Идентификатор нити–инициатора операции	**whotid**	unsigned
Стартовый адрес нити–инициатора операции	**whoaddr**	uint64
Флаги исполняемого модуля–инициатора операции	**whof**	uint64
Командная строка родительского процесса	**cmdlp**	string
Командная строка прародителя (grand parent)	**cmdlg**	string
Рабочий каталог процесса	**wdir**	string MANGLED
Уровень защиты процесса	**prot**	unsigned
Уровень доверия (integrity level) процесса	**integ**	unsigned
Время создания процесса	**when**	timestamp
Уникальный идентификатор родительского процесса	**parent**	unsigned (индекс в массиве GUID-ов)
Уникальный идентификатор процесса-создателя	**caller**	unsigned (индекс в массиве GUID-ов)
Идентификатор процесса-инициатора операции	**cpid**	unsigned
Полное имя процесса-инициатора операции	**cpath**	string MANGLED
Код завершения процесса	**code**	unsigned
Уникальный идентификатор целевого процесса	**targ**	unsigned
Полное имя целевого процесса	**tpath**	string MANGLED
Идентификатор целевого процесса	**tpid**	unsigned

Назначение	JSON	Тип
Флаги образа целевого процесса	**targf**	uint64
Поведенческие признаки целевого процесса (первая группа)	**trf0**	uint64
Поведенческие признаки целевого процесса (вторая группа)	**trf1**	uint64
Стек вызовов операции	**trace**	string
Полное имя файла образа	**path**	string MANGLED
Флаги операции загрузки образа	**ldf**	unsigned
Флаги образа	**imgf**	uint64
Базовый адрес образа	**base**	uint64
Размер образа	**isize**	unsigned
Идентификатор целевой нити	**tid**	unsigned
Имя модуля целевой нити	**tmod**	string
Имя функции целевой нити	**tfunc**	string
Стартовый адрес целевой нити	**taddr**	uint64
Флаги операции с нитью	**tf**	unsigned
Запрашиваемые права	**dsrd**	unsigned (32 бита)
Предоставленные права	**grnt**	unsigned (32 бита)
Новый уровень защиты процесса	**prot1**	int
Новая командная строка процесса	**cmdl1**	string
Размер файла	**fsize**	int64
Тип файла	**ftype**	enum
SHA-1 файла	**sha1**	string
MD5 файла	**md5**	string
SHA-256 файла	**sha256**	string
Электронная подпись файла	**sgnr**	string
Статус электронной подписи	**sgnr_s**	enum
Тип упаковщика файла	**pack**	string
Атрибуты файла	**attr**	unsigned
Время создания файла	**crtime**	timestamp
Время последней записи файла	**chtime**	timestamp
Оригинальное имя файла	**ofn**	string
Компания-издатель файла	**fcomp**	string
Версия файла	**fver**	string
Описание файла	**fdesc**	string
Продукт, к которому относится файл	**fprod**	string
Код обнаружения	**detect**	unsigned

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

— 0 (нет);

— 1 (низкий);

— 2 (средний);

— 3 (высокий);

— 4 (системный);

— 5 (защищенный).

9.7 События мониторинга системы

Подтипы событий (**st**) мониторинга системы представлены в таблице 29.

Таблица 29 – Подтипы событий мониторинга системы

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

События мониторинга систем с кодом события 0 (WMI) представлены в таблице 30.

Таблица 30 – Поля мониторинга системы (код события 0)

Назначение	JSON	Тип
WMI: Тип события (создание = 0, удаление = 1, изменение = 2)	**wmi**	integer
WMI: SID пользователя	**wmi_sid**	string
WMI: Пространство имен	**ns**	string
WMI: Путь до исполняемого файла	**exe_path**	string MANGLED
WMI: Имя файла	**fname**	string MANGLED
WMI: Имя фильтра событий	**wmi_nm**	string
WMI: Строка запроса	**qstr**	string
WMI: Имя файла скрипта	**scrfname**	string MANGLED
WMI: Текст скрипта	**scrtxt**	string
WMI: Имя источника	**sname**	string MANGLED

Назначение	JSON	Тип
WMI: Путь	**wmi_pth**	string
WMI: SMTP	**smtp**	string
WMI: Фильтр	**flt**	string
WMI: Потребитель	**cnsm**	string
WMI: Идентификатор процесса клиента	**wmi_clpid**	unsigned
WMI: Уникальный идентификатор процесса клиента	**wmi_cluuid**	int
WMI : Время создания процесса клиента	**wmi_cltime**	timestamp (UTC)
WMI: Командная строка процесса клиента	**wmi_clcmdl**	string
WMI: Локальный запрос (0 или 1, по умолчанию 1)	**wmi_local**	int (-/1)
WMI: Идентификатор созданного процесса	**wmi_crpid**	unsigned
WMI: Уникальный идентификатор созданного процесса	**wmi_cruuid**	int (индекс в массиве GUID'ов)
WMI: Время создания созданного процесса	**wmi_crtime**	timestamp (UTC)
WMI: Командная строка созданного процесса	**wmi_crcmdl**	string
WMI: Имя машины, выполнившей запрос	**wmi_cl**	string
WMI: FQDN машины, выполнившей запрос	**wmi_clfqdn**	string
WMI: Имя пользователя клиента, выполнившего запрос	**wmi_usr**	string
WMI: Имя домена клиента, выполнившего запрос	**wmi_dom**	string
WMI: Имя вызываемого клиента	**wmi_mthd**	string

Важно

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

Пример строки события представлен в таблице 31.

Таблица 31 – 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**

События системы с подтипом **st:1** (Атаки на Kerberos) представлены в таблице 32.

Подтипы атак (**atck**) на Kerberos представлены в таблице 32:

Таблица 32 – 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 мониторинга системы атаки Golden ticket представлены в таблице 33.

Таблица 33 – Поля монитора системы (атаки golden ticket)

Назначение	JSON	Тип
Golden ticket: Причина	**goldent_r**	enum KERBEROS_ATTACK_REASON (integer)
Golden ticket: Имя пользователя	**goldent_u**	string
Golden ticket: Имя домена	**goldent_d**	string
Golden ticket: IP-адрес	**goldent_ip**	string

События мониторинга системы атаки Silver ticket представлены в таблице 34.

Таблица 34 – Поля монитора системы (атаки silver ticket)

Назначение	JSON	Тип
Silver ticket: Причина	**silvert_r**	enum KERBEROS_ATTACK_REASON (integer)
Silver ticket: Имя пользователя	**silvert_u**	string
Silver ticket: Имя домена	**silvert_d**	string
Silver ticket: IP-адрес	**silvert_ip**	string

События мониторинга системы атаки Kerberoasting представлены в таблице 35.

Таблица 35 – Поля монитора системы (атака Kerberoasting)

Назначение	JSON	Тип
Kerberoasting: Причина	**kerberoasting_r**	enum KERBEROS_ATTACK_REASON (integer)
Kerberoasting: Имя пользователя	**kerberoasting_u**	string
Kerberoasting: Имя домена	**kerberoasting_d**	string
Kerberoasting: IP-адрес	**kerberoasting_ip**	string

События мониторинга системы атаки AS-REP roasting представлены в таблице 36.

Таблица 36 – Поля мониторинга системы (атака AS-REP roasting)

Назначение	JSON	Тип
AS-REP roasting: Причина	**asreproasting_r**	enum KERBEROS_ATTACK_REASON (integer)
AS-REP roasting: Имя пользователя	**asreproasting_u**	string
AS-REP roasting: Имя домена	**asreproasting_d**	string
AS-REP roasting: IP-адрес	**asreproasting_ip**	string

Таблица 37 – Подтипы атак на Kerberos в зависимости от причины (enum KERBEROS_ATTACK_REASON)

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 38.

Таблица 38 – 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**

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

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

– 1 (штатное завершение работы компьютера);

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

– 3 (штатная остановка агента).

9.8 События пользовательских сессий

Подтипы событий и их текстовые описания представлены в таблице 39.

Таблица 39 – Подтипы событий пользовательских сессий

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

Примечание

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

Параметр **sess_opt** (тип дистанционного управления) может принимать одно из значений, указанных в таблице 40.

Таблица 40 – Типы дистанционного управления

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

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

– 0 (консольная сессия);

– 2 (RDP-сессия).

Поля событий мониторинга сессий представлены в таблице 41.

Таблица 41 – Поля мониторинга сессий

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

9.9 События монитора вызовов

Подтипы событий монитора вызовов представлены в таблице 42.

Таблица 42 – Подтипы событий монитора вызовов

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

События монитора вызовов (RPC-вызовы) представлены в таблице 43.

Таблица 43 – Поля монитора вызовов (RPC вызовы)

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

Поле **rpc_proto** принимает следующие значения:

1 – TCP;

2 – Named Pipes;

3 – LRPC;

4 – HTTP.

Поле **rpc_authsvc** принимает следующие значения:

0x09 – Negotiate;

0x0A – NTLM;

0x0E – SChannel;

0x10 – Kerberos;

0x14 – Kernel.

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

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

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

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

9.10 События anti-ransomware-модуля

Подтипы событий и их текстовые описания представлены в таблице 44.

Таблица 44 – 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 модуля защиты от вирусов-шифровальщиков представлены в таблице 45.

Таблица 45 – Поля событий anti-ransomware модуля

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

Назначение	JSON	Тип
Количество расширений файлов, в которые писали	**exwac_**	unsigned
Количество уникальных расширений файлов, из которых только читали	**exurac**	unsigned
Количество уникальных расширений файлов, в которые только писали	**exuwac**	unsigned
Категории файлов, к которым осуществлялся доступ	**gf_am**	unsigned
Категории файлов, из которых производилось чтение	**gf_rm**	unsigned
Категории файлов, в которые производилось запись	**gf_wm**	unsigned
Категории файлов, которые удалялись	**gf_dm**	unsigned

Битовая маска группы файлов:

1) Бит 0 – остальные;
2) Бит 1 – документы;
3) Бит 2 – документы текстового формата;
4) Бит 3 – электронные таблицы;
5) Бит 4 – презентации;
6) Бит 5 – архивы;
7) Бит 6 – изображения;
8) Бит 7 – видео;
9) Бит 8 – исполняемые модули;
10) Бит 9 – исходные коды;
11) Бит 10 – скрипты;
12) Бит 11 – аудио;
13) Бит 12 – базы данных;
14) Бит 13 – файлы-контейнеры.

9.11 События модуля контроля USB

Тип события – **Контроль USB** (**t**:9 в DSL). Подтипы событий (**st**) и их текстовые описания представлены в таблице 46.

Таблица 46 – Подтипы событий модуля контроля USB

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

Поля событий модуля контроля USB указаны в таблице 48.

Таблица 47 – События модуля контроля USB

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

9.12 События статистики

Поля событий статистики указаны в таблице 48.

Таблица 48 – События статистики

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

Максимальная скорость отправки событий (Кбит/сек)	unsigned	**netlimit**

Поле **shutdown** может принимать следующие значения:

1) 0 – агент работает в штатном режиме;
2) 1 – штатное завершение работы компьютера;
3) 2 – штатный переход компьютера в состояние сна или гибернации;
4) 3 – штатная остановка агента.

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

9.13 Битовые флаги

Битовые флаги сетевого события (**netf**) и расшифровки для них представлены в таблице 49.

Таблица 49 – Флаги сетевого события

Наименование флага	Расшифровка
EndpointWhiteListed	Доверенный эндпойнт
RequestDomainNameWhiteListed	Доверенное запрашиваемое доменное имя

Битовые флаги исполняемого файла процесса (**exclf**) и расшифровки для них представлены в таблице 50.

Таблица 50 – Флаги исполняемого файла процесса

Наименование флага	Расшифровка
DontSuppressEvents	Запрет принудительного подавления события
TaskSheduler	Планировщик задач
AllowCodeInjection	Разрешение внедрения кода в сторонние программы
AllowWrite	Разрешение записи памяти сторонних программ
Rundll32	DLL-хост rundll32
PowerShell	Интерпретатор powershell
Cmd	Командный интерпретатор cmd
MsiExec	Установщик программы msiexec
Explorer	Проводник explorer
CSS	Критический системный компонент

MsHta	Хост HTML-приложений mshta
Svchost	Хост служб svchost
Lsass	Системный компонент LSASS
AllowControlRead	Разрешение чтения памяти сторонних программ и управления ими
Prefetcher	Служба Prefetcher-a Windows
ControlPanel	Панель управления Windows
ScriptEngine	Скриптовый движок
ImageWow64	Компонент имеет 32-х битную и 64-х битную версию
HostProcess	Хост-процесс
WhoAmI	Утилита whoami
Csrss	Системный компонент CSRSS
TCB	Максимальное доверие
NTDLL	Системная библиотека NTDLL
Vssadmin	Утилита управления резервным копированием vssadmin
Wmic	Утилита администрирования wmic
Wbadmin	Утилита администрирования wbadmin
BcdEdit	Утилита управления параметрами загрузки BCDEdit
DiskShadow	Утилита управления резервным копированием Diskshadow
Icacls	Утилита управления правами доступа к файлам iCACLS
PsExec	Утилита удаленного администрирования PsExec
VerifyTrust	Подтверждение по электронной подписи
SkipAllEvents	Исключение всей телеметрии
Browser	Браузер
Office	Офисная программа
AllowDirectDiskWrite	Разрешение прямого доступа к диску для записи
AllowDirectDiskRead	Разрешение прямого доступа к диску для чтения
CSSFriendly	Право взаимодействия с критическими системными программами
SkipNetEvents	Исключение из телеметрии сетевых событий
SkipFsEvents	Исключение из телеметрии файловых событий
SkipRegEvents	Исключение из телеметрии событий реестра Windows
AVEngine	Антивирусный компонент
SkipPmEvents	Исключение из телеметрии событий поведения
Verclsid	Утилита Verclsid
Regsvr32	Утилита Regsvr32
FsUtil	Утилита FsUtil
TrustedDotNet	.NET-компоненты, которым есть доверие
CMSTP	Установщик профилей менеджера подключений Windows
WmiPrvSE	Хост WMI
InstallUtil	Утилита установки INF-файлов
Odbcconf	Утилита конфигурации ODBC

DismHost	Компонент DismHost
KnownDll	Известная DLL
DotNetNativeImage	Нативная версия .NET-сборки
KernelDll	Системная библиотека KERNEL32 или KERNELBASE
SupressFSChecks	Исключение анализа файловой активности
RegAsm	Утилита регистрации .NET-сборки
SupressNetChecks	Исключение анализа сетевой активности
Mmc	Консоль управления Windows
SupressloaMatch	Исключение матчинга индикаторов атак
Hh	Просмотрщик chm-файлов

Битовые флаги операции загрузки образа (**ldf**) и расшифровки для них представлены в таблице 51.

Таблица 51 – Флаги операции загрузки образа

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

Битовые флаги поведенческих признаков процесса первой группы (**rf0**) и расшифровки для них представлены в таблице 52.

Таблица 52 – Флаги поведенческих признаков процесса (первая группа)

Наименование флага	Расшифровка
ProcHiveRoot	Главный процесс группы
Wow64	32-х битный процесс в 64-х битной системе
Native	Доверенный процесс

Synthetic	Событие создания процесса синтезировано
Managed	.NET-процесс
RunWithUAC	UAC-процесс
DroppedByParent	Процесс создал родитель и запустил
LaterStage	Основные системные модули загружены
IsInjected	API-вызовы процесса контролируются
FromExplorer	В цепочке родителей есть EXPLORER
SuspiciousDirectory	Каталог запуска: RECYCLER, System Volume Information и т.п.
HiddenDirectory	Каталог запуска: скрытый
FromInet	Исполняемый файл загружен из Интернета
TempDirectory	Каталог запуска: временный
SystemTempDirectory	Каталог запуска: системный временный
NetworkDirectory	Каталог запуска: сетевой путь
RemovableMedia	Каталог запуска: съемный носитель
AutorunDirectory	Каталог запуска: автозапуск
SystemDirectory	Каталог запуска: системный
ProgramFilesDirectory	Каталог запуска: Program Files
NetMalwareSignature	Срабатывание ИК в сетевом трафике: сигнатура
BlacklistedNetworkAccess	Попытка обращения по сети к заблокированным IP-адресам/доменным именам
NetworkServer	Прослушивание сетевого порта кроме loopback
NetworkAccess	Сетевой обмен (кроме loopback)
LoopbackAccess	Сетевое взаимодействие по loopback
RawSocketUse	Использование raw-сокетов
NetIOC	Срабатывание ИК в сетевом трафике: IP-адрес/доменное имя
NtAllocateVirtualMemory	Выделение памяти в стороннем процессе
NtAllocateVirtualMemoryEx	Выделение памяти в стороннем процессе|расширенное
NtDeviceIoControlFile	Взаимодействие с драйверами
NtGetContextThread	Получение контекста нити стороннего процесса
NtMapViewOfSection	Проецирование секции в сторонний процесс
NtMapViewOfSectionEx	Проецирование секции в сторонний процесс|расширенное
NtProtectVirtualMemory	Изменение атрибутов защиты памяти стороннего процесса
NtQueryInformationThread	Получение информации о нити стороннего процесса
NtQueueApcThread	Отправка APC-нити стороннего процесса
NtQueueApcThreadEx	Отправка APC-нити стороннего процесса|расширенная
NtReadVirtualMemory	Чтение памяти стороннего процесса
NtResumeThread	Возобновление работы нити стороннего процесса
NtSetContextThread	Установка контекста нити стороннего процесса
NtSetInformationProcess	Управление сторонним процессом
NtSetInformationThread	Управление нитью стороннего процесса
NtSuspendThread	Приостановка работы нити стороннего процесса

NtUnmapViewOfSection	Отмена проекции секции стороннего процесса
NtUnmapViewOfSectionEx	Отмена проекции секции стороннего процесса|расширенная
NtWriteVirtualMemory	Запись памяти стороннего процесса
Tampering	Применение техник подмены исполняемых образов
PostModified	Исполняемый файл модифицирован после проецирования
Deleted	Исполняемый файл удален
Renamed	Исполняемый файл переименован
FromServices	В цепочке родителей есть диспетчер служб
FromBrowser	В цепочке родителей есть браузер
FromOffice	В цепочке родителей есть офисная программа
Protected	Защищенный процесс
Transacted	Транзакция на исполняемом файле
Trustlet	Изолированный процесс
WhiteListed	Известный легальный
Trusted	Подписан
Untrusted	Не подписан
Elevated	Повышенные привилегии
PreInitialUpdate	Событие предшествовало первичному обновлению аналитики

Битовые флаги поведенческих признаков процесса второй группы (**rf1**) и расшифровки для них представлены в таблице 53.

Таблица 53 – Флаги поведенческих признаков процесса второй группы

Наименование флага	Расшифровка
RegSecurityModify	Модификация security элементов реестра
RegStorePE	Запись потенциального исполняемого файла в реестр
InstallService	Регистрация службы в реестре
RegAsepModify	Модификация точек автозапуска реестра
MsHtaRun	Запуск утилиты mshta
Regsvr32Run	Запуск утилиты regsvr32
VerclsidRun	Запуск утилиты verclsid
SystemRestoreDisable	Выключение механизма восстановления системы
IcaclsRun	Запуск icacls
HhRun	Запуск просмотрщика chm-файлов
PsExecRun	Запуск psexec
PowerShellRun	Запуск powershell
CmdScriptRun	Запуск cmd /c
TaskManage	Запуск планировщика задач с параметрами /create или /change

MsiExecRun	Запуск msiexec
Rundll32Run	Запуск rundll32
ScriptRun	Запуск скриптового интерпретатора
WhoAmIRun	Выполнение команды whoami
ShellCodeExec	Выполнение shell-кода
ContainsManagedCode	Содержит .NET-код
MapRemoteView	Проецирование образа в сторонний процесс
DoSpoofParentId	Подмена родителя дочернему процессу
CreateRemoteThread	Создание нити в стороннем процессе
CmdLineTampering	Подмена командной строки
OpenThread	Открытие сторонней нити
OpenProcess	Открытие стороннего процесса
ControlPanelRun	Запуск панели управления Windows
CMSTPRun	Запуск установщика профилей диспетчера подключений Windows
InstallUtilRun	Запуск установщика INF-файлов
OdbcconfRun	Запуск утилиты администрирования ODBC
RegAsmRun	Запуск утилиты регистрации .NET-сборок
MmcRun	Запуск консоли управления Windows
Unprotected	Нештатно уменьшен уровень защиты
ProtectionElevated	Нештатно увеличен уровень защиты
HasRemoteView	Содержит спроецированный извне образ
Tampered	Подменен образ исполняемого файла
HasRemoteThread	Содержит нить, созданную извне
ThreadOpen	Открытие нити процесса извне
ProcessOpen	Открытие процесса извне
MemoryWritten	Память процесса записана извне
MemoryRead	Память процесса прочитана извне
MemoryMadeExecutable	Участок памяти процесса извне отмечен как исполняемый код
SpoofParentId	Подменен родительский процесс
RegisterTask	Создание файлов в каталоге задач
SetAutorun	Создание файлов в каталоге автозапуска
CreateMofFile	Создание *.mof-файлов в каталоге WMI
ReadSystemPEFile	Чтение системных исполняемых файлов, не связанное с их запуском
WriteExeFile	Запись в исполняемые файлы
NamedPipeClient	Клиент именованного канала
FileNameHasStreamComponent	В имени исполняемого файла присутствует компонент ntfs-потока
UnusualExeFileExtension	Имя исполняемого файла имеет нетипичное расширение
RandomFileName	Случайное имя файла
NamedPipeServer	Сервер именованного канала
CreateExeFile	Создание файлов с потенциально активным содержимым

Битовый флаг нити (**tf**) имеет только одно наименование **Float** с расшифровкой **Шелл-код**.

10. Основные операции в «RT Protect EDR»

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

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

Примечание

Подавляющая часть инцидентов в Программе формируются на основе аналитических правил (индикаторы атак, YARA-правила, индикаторы компрометации, встроенные правила на агенте, ML), а также в результате срабатываний TI-платформы.

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

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

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

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

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

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

На **Главной странице** аналитику доступен просмотр общей информации по контролируемой инфраструктуре (рис. 6):

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

– общее количество инцидентов и количество открытых инцидентов;

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

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

– количество открытых инцидентов;

– последние обнаруженные процессы и модули;

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

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

– динамика инцидентов;

– распределение инцидентов по критичности;

– топ 10 правил в инцидентах;

– топ 10 техник MITRE ATT&CK в инцидентах.

Для просмотра всех инцидентов, зарегистрированных в Программе, необходимо выполнить переход на страницу **Оповещения** (см. подробнее в подразделе 10.2) или страницу **Инциденты** (см. подробнее в подразделе 10.3).

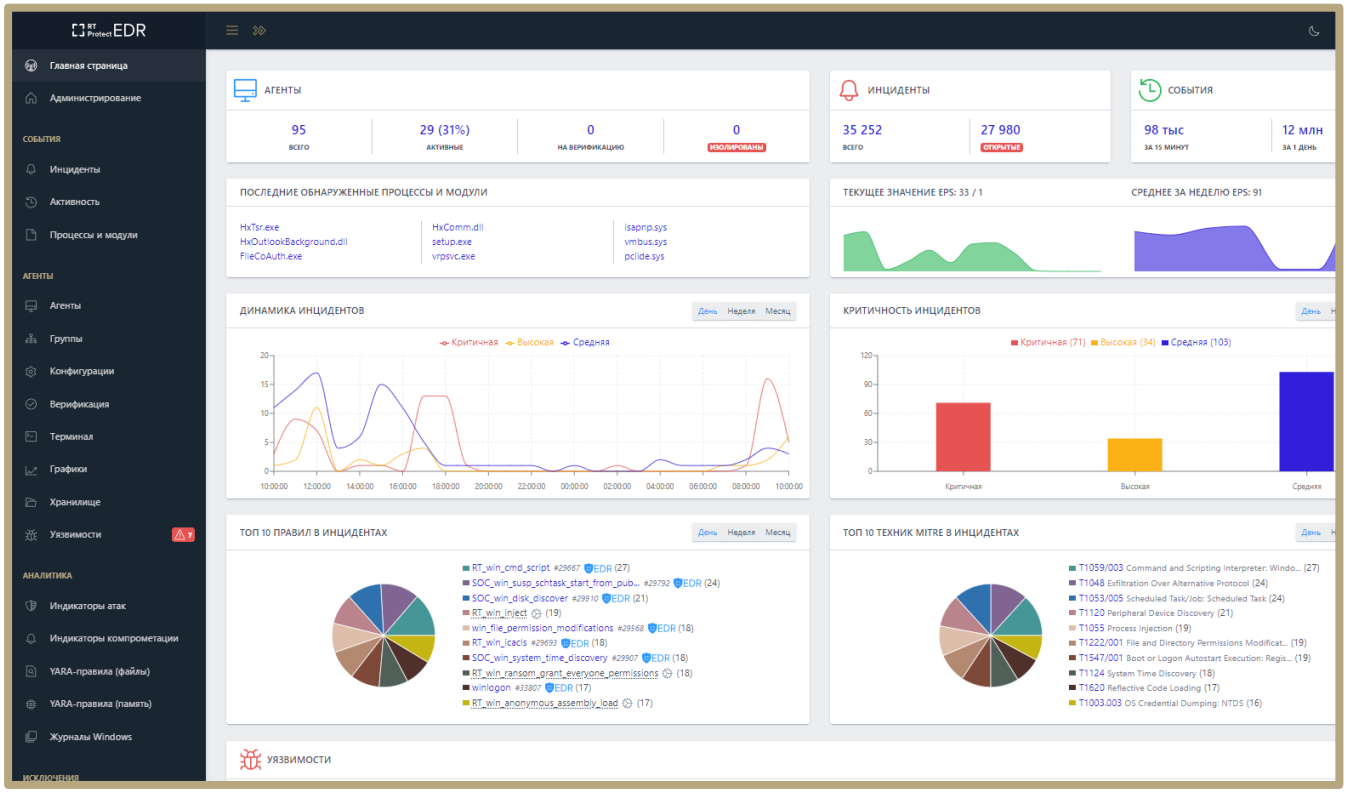


Рисунок 6 – Главная страница

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

1) Изолировать зараженного агента;

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

3) Восстановить данные на конечных точках с помощью команд терминала;

4) Завершить вредоносный процесс или восстановить файлы на странице **Процесс**;

5) Загрузить подозрительный файл в хранилище Программы;

6) Выяснить масштабы компрометации на странице **Процессы и модули**;

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

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

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

Если рассматривать работу аналитика с точки зрения проактивного поиска угроз, то наибольшую ценность для такого рода деятельности представляет страница **Активность**. Подробная информация о проактивном поиске на странице **Активность** содержится в подразделе 10.19.

10.1 Операции с профилем пользователя

Чтобы открыть меню операций с профилем пользователя, необходимо кликнуть на имя пользователя (Analyst) в верхней части страницы. Откроется меню, состоящее из двух пунктов:

1) **Профиль** (откроется страница, на которой аналитик может изменить данные своей учетной записи);
2) **Выход** (выход из учетной записи пользователя).

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

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

1) Установить в профиле флажок **Использовать двухфакторную аутентификацию**.
2) Нажать кнопку **Сохранить**.

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

В профиле аналитик может также поменять следующие данные:

1) Имя;
2) Фамилия;
3) Email.

Аналитик может в любой момент изменить пароль на странице своего профиля, для этого необходимо нажать кнопку **Сменить пароль** и в открывшемся окне ввести текущий и новый пароль с учетом требований, указанных в нижней части окна (рис. 7). Для завершения операции необходимо нажать кнопку **Сохранить**.

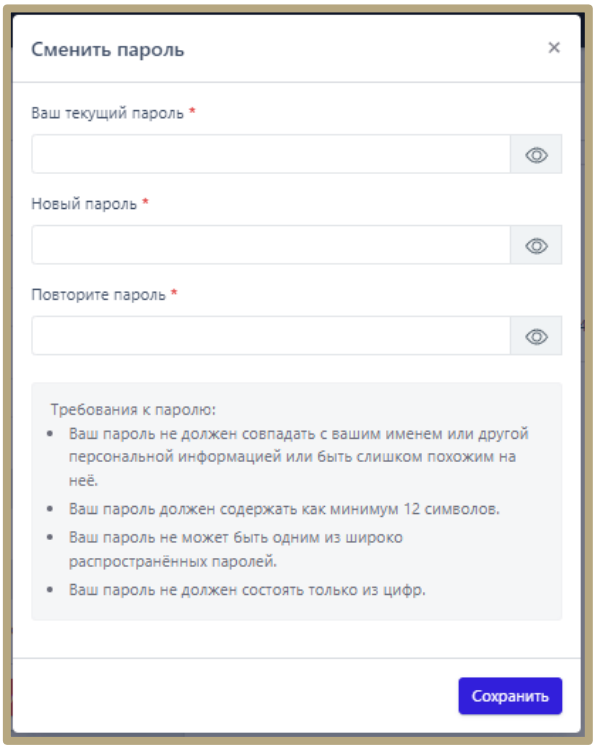


Рисунок 7 – Окно «Сменить пароль»

Чтобы выйти из текущего профиля, аналитику необходимо нажать кнопку пункта меню **Выход**, после чего откроется окно входа на сервер управления Программы (рис. 8).

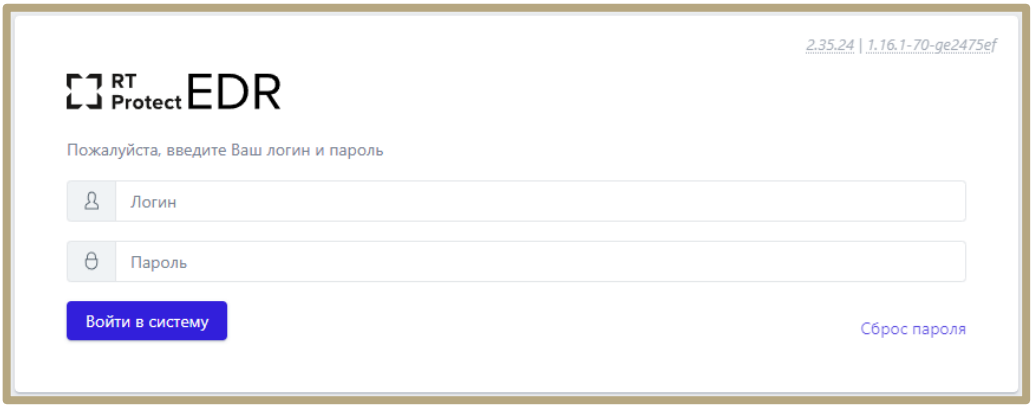


Рисунок 8 – Окно входа в Программу

В некоторых случаях аналитику может потребоваться восстановить пароль, в связи с тем, что он может его забыть. Для этого в окне входа в программу находится кнопка **Сброс пароля**, которая позволяет по логину отправить на почту запрос, содержащий ссылку на сброс пароля.

На электронную почту, указанную в профиле пользователя, будет направлено письмо, содержащее ссылку, при нажатии которой в браузере откроется окно. В этом окне аналитик может ввести новый пароль (рис. 9).

Рисунок 9 – Окно восстановления пароля

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

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

2) Должен содержать как минимум 12 символов;

3) Не должен быть одним из широко распространенных паролей;

4) Не должен состоять только из цифр.

10.2 Расследование инцидентов со страницы «Оповещения»

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

При появлении событий, несущих угрозу, в правой части окна, открытого в браузере модуля администрирования, появляется сообщение о возникновении инцидента (рис. 10).

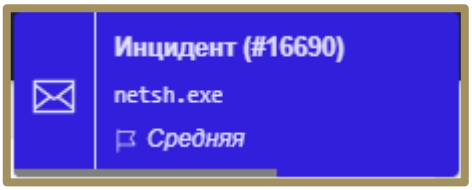


Рисунок 10 – Уведомление о возникновении инцидента

На странице **Оповещения** показывается информация о событиях, происходящих в защищаемой инфраструктуре (в том числе инциденты), в порядке регистрации их на сервере. При переходе в раздел **Оповещения** на вертикальной панели инструментов откроется страница, представленная на рисунке 11.

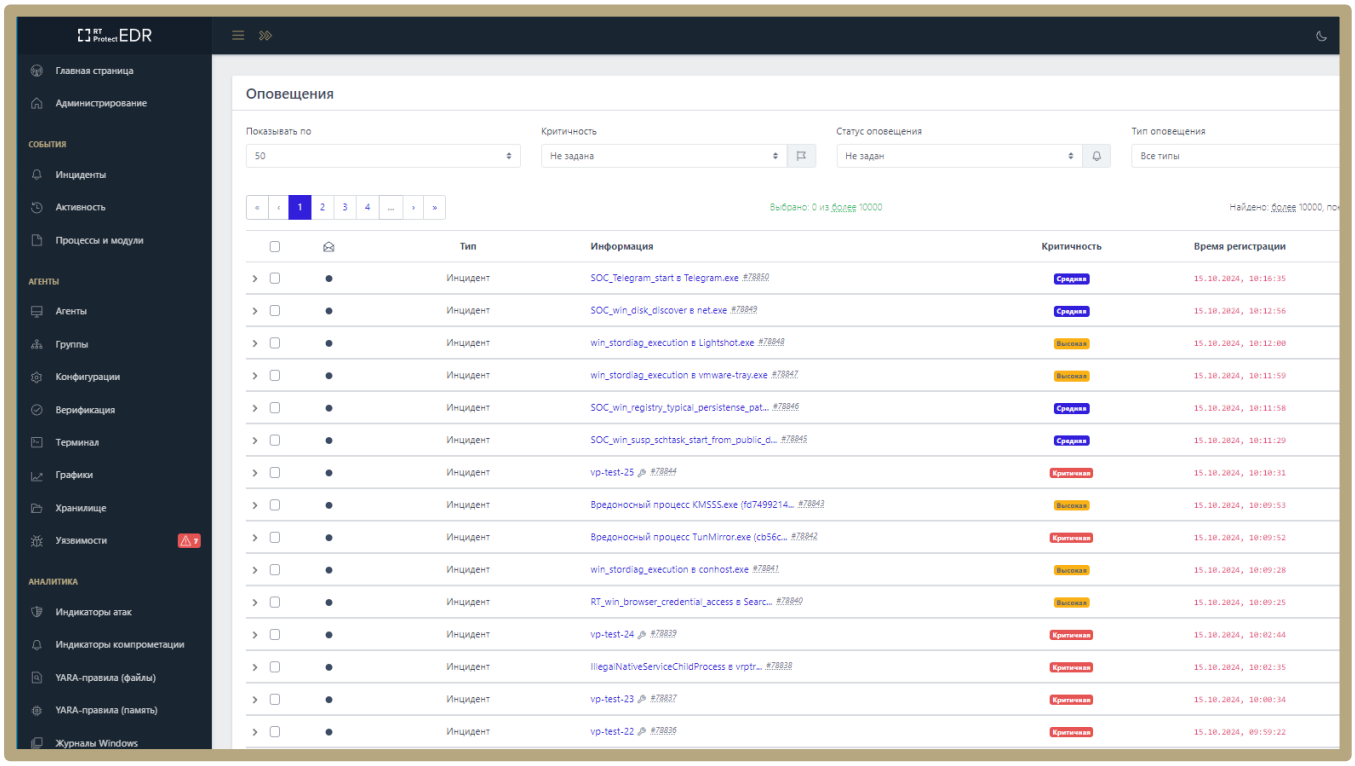


Рисунок 11 – Страница «Оповещения»

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

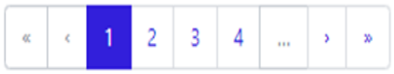
1) **Показывать по** (10, 20, 50, 100) – количество строк отображается согласно выбранному элементу;

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

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

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

Элементы навигации и информационные элементы, представленные в окне:



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

Выбрано: 0 из 8631

– количество выбранных элементов

Найдено: 8631, показано: с 1 по 10

– общее количество найденных оповещений, количество показанных на странице

– кнопка подтверждения (прочитать все выбранные оповещения)

– кнопка подтверждения (прочитать выбранные оповещения)

– кнопка выбора строки с оповещением

– кнопка навигации в окне фильтрации

– отметить как прочитанные

Аналитик при выборе интересующего оповещения (производится кликом по кнопке ›) может просмотреть дополнительную информацию по событию в открывшейся таблице (рис. 12). В зависимости от типа оповещения поля таблицы могут содержать разную информацию.

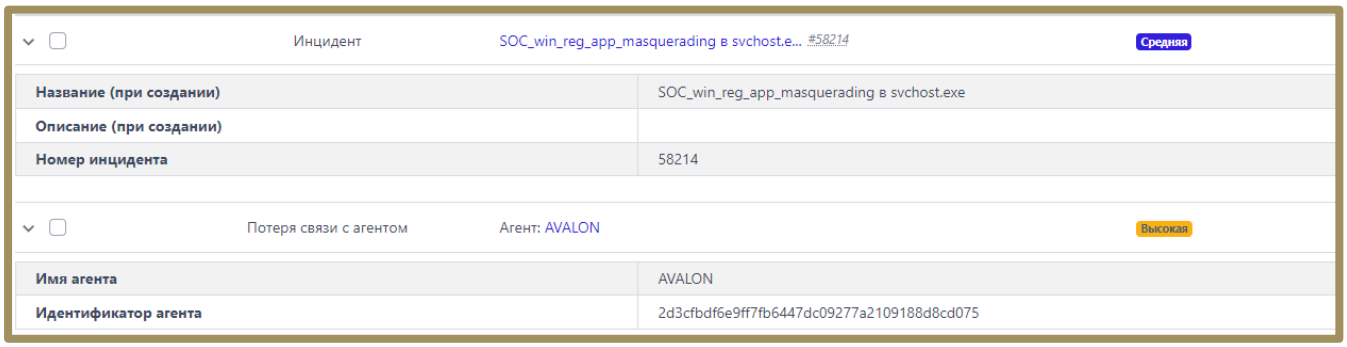


Рисунок 12 – Дополнительная информация о событии

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

Далее интерес для аналитика может представлять страница **Процесс** (рис. 13). Страница открывается при нажатии в области **Обнаружения** ссылки в виде имени процесса, связанного с событием. Событие-обнаружение может быть частью инцидента или единственным событием выбранного инцидента.

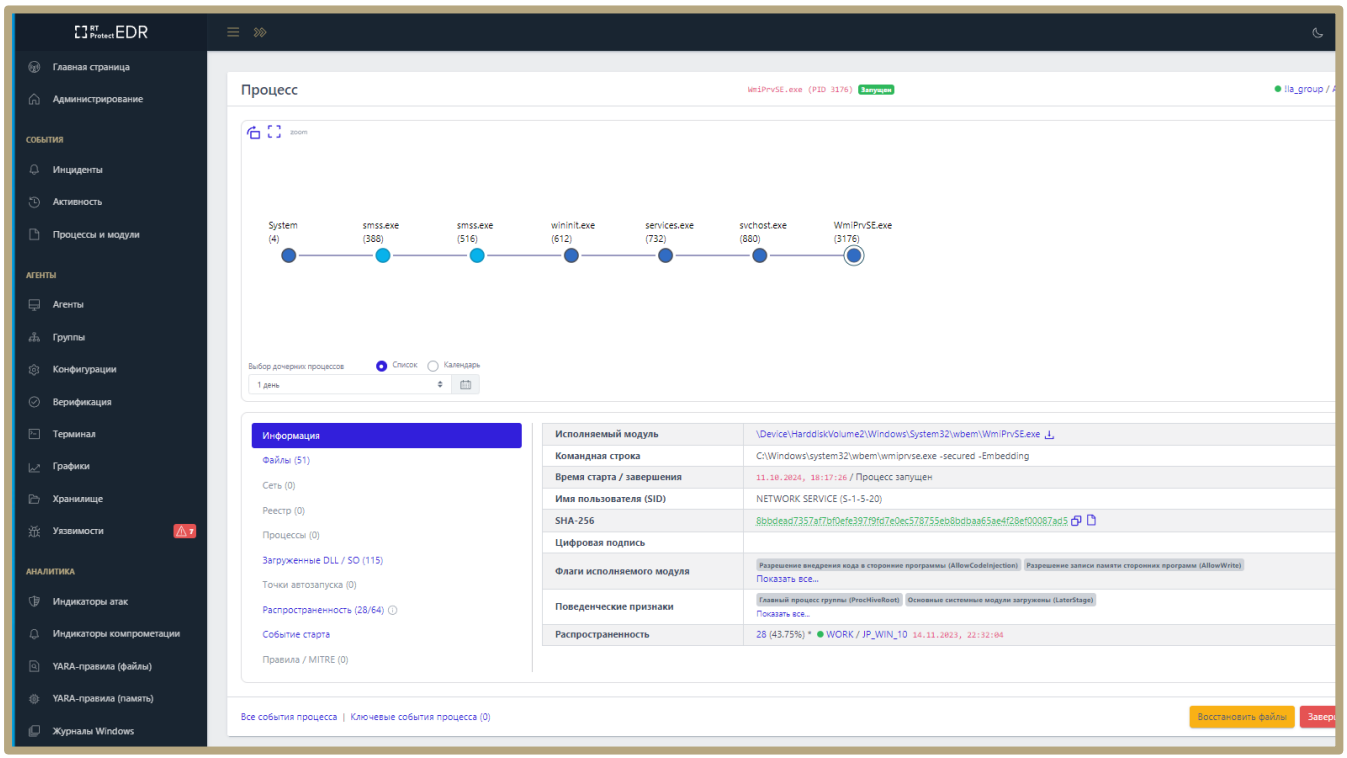


Рисунок 13 – Открытие страницы «Процесс»

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

10.2.1. Работа с деревом процессов

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

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

Аналитик может задавать временный интервал отображения дерева процессов, выбрав интервал из списка или задав его с помощью календаря.

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/SO**;

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) ;

_ Восстановить файлы ;

_ Завершить процесс .

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. 14). То есть в ключевые попадают события с критичностью низкая или выше, события, по которым есть правило, или события, где результирующим выбрано запрещающее действие.

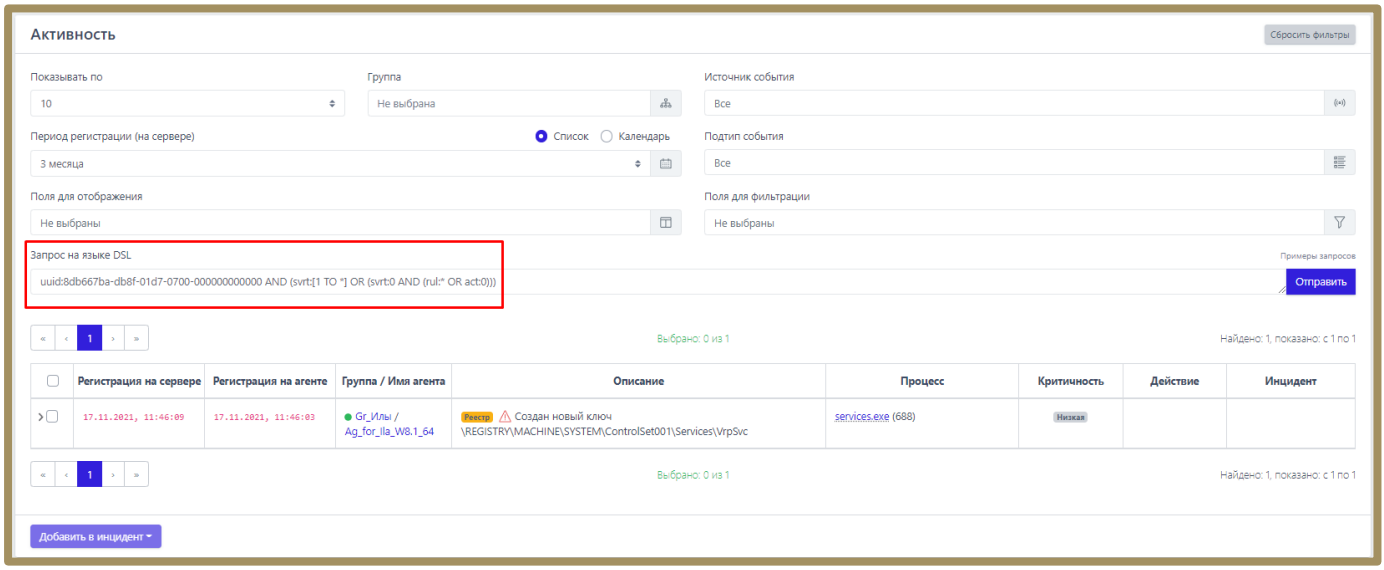


Рисунок 14 – Ключевые события процесса

Восстановить файлы – кнопка позволяет восстановить файлы, затронутые вредоносным процессом, если эти файлы были зарезервированы в соответствии с настройками каталогов в профиле защиты данных.

Завершить процесс – кнопка позволяет быстро остановить вредоносную активность процесса. Кнопка активна, если процесс находится в состоянии Запущен.

Вкладка «Информация»

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

1) **Исполняемый модуль**;
2) **Командная строка**;
3) **Время старта/завершения**;
4) **Имя пользователя (SID)**;
5) **SHA-256**;

6) **Цифровая подпись**;

7) **Флаги исполняемого модуля**;

8) **Поведенческие признаки**;

9) **Распространенность**.

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

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

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

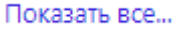
Имя пользователя (SID) – в поле отображается имя пользователя и идентификатор безопасности пользователя, от имени которого был запущен рассматриваемый процесс.

SHA-256 – в поле отображается хеш-сумма исполняемого файла, запустившего процесс. При нажатии ЛКМ на значение хеш-суммы пользователю показывается всплывающее окно с кратким отчетом TI-платформы об исполняемом файле. Рядом с хеш-суммой отображаются две кнопки. Первая кнопка позволяет скопировать хеш в буфер обмена (). Вторая позволяет перейти на страницу **Процессы и модули** для выбранной хеш-суммы ().

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

Флаги исполняемого модуля – в поле показаны флаги, с которыми исполняется программа, кнопка 

открывает дополнительную область с флагами исполняемого модуля процесса.

Поведенческие признаки – в поле показаны поведенческие признаки программы, кнопка 

открывает дополнительную область с поведенческими признаками процесса.

Распространенность – в поле отображается, на каком количестве агентов был обнаружен процесс, кроме того, просчитано процентное соотношение таких агентов к их общему количеству. Помимо этого, показан агент, на котором процесс был обнаружен впервые.

Вкладка «Файлы»

В таблице вкладки **Файлы** отображается информация о файлах, с которыми связан рассматриваемый процесс (рис. 15).

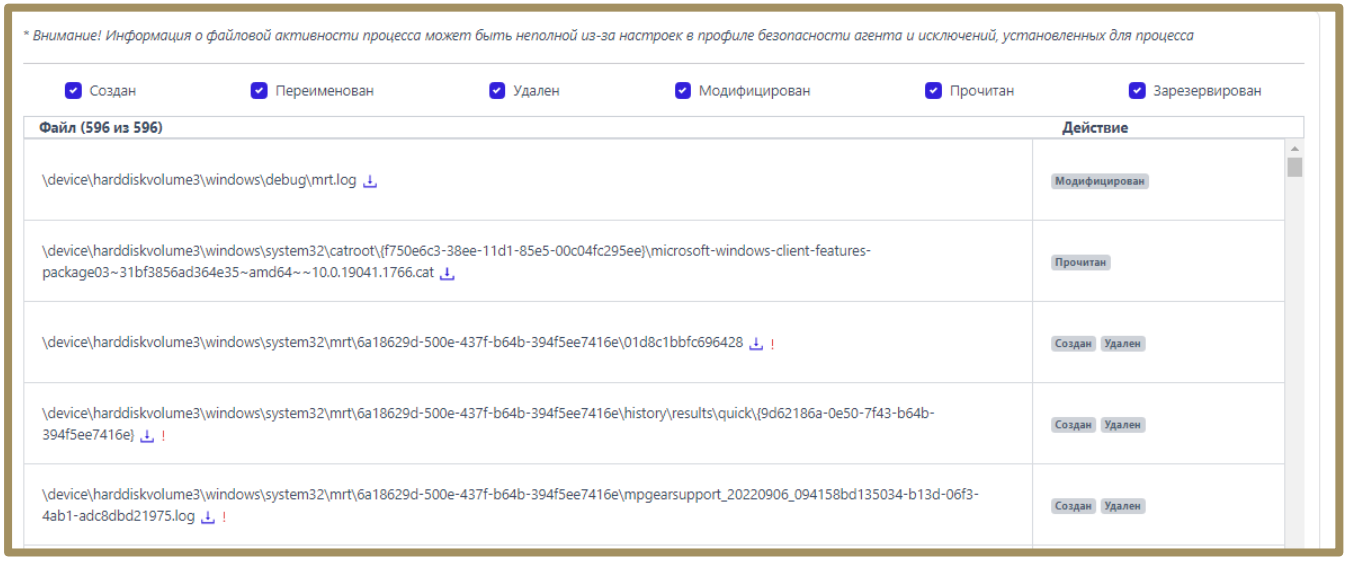


Рисунок 15 – Информация о файлах процесса

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

Если среди действий с файлом из списка было удаление, то он помечается значком !. При наведении курсора мыши на значок пользователю выводится предупреждающее сообщение (рис. 16).

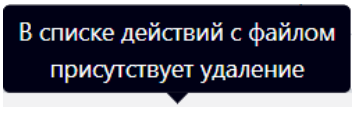


Рисунок 16 – Сообщение о присутствии в списке удаления файла

Вкладка «Сеть»

Во вкладке **Сеть** отображается информация о сетевых подключениях процесса:

1) **Входящие подключения**;

2) **Исходящие подключения**;

3) **DNS-запросы**.

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 TI-платформы (если это глобальный адрес).

Имя хоста – в поле отображается доменное имя конечной точки, с которой осуществлялось сетевое соединение, доменное имя также автоматически проверяется TI-платформой (если это не внутренний домен). При нажатии ЛКМ на значение имени аналитик может просмотреть отчет.

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.

Вкладка «Реестр»

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

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

1) **Путь ключа реестра** – в поле прописывается путь ключа реестра, с которым выбранный процесс производил те или иные действия;

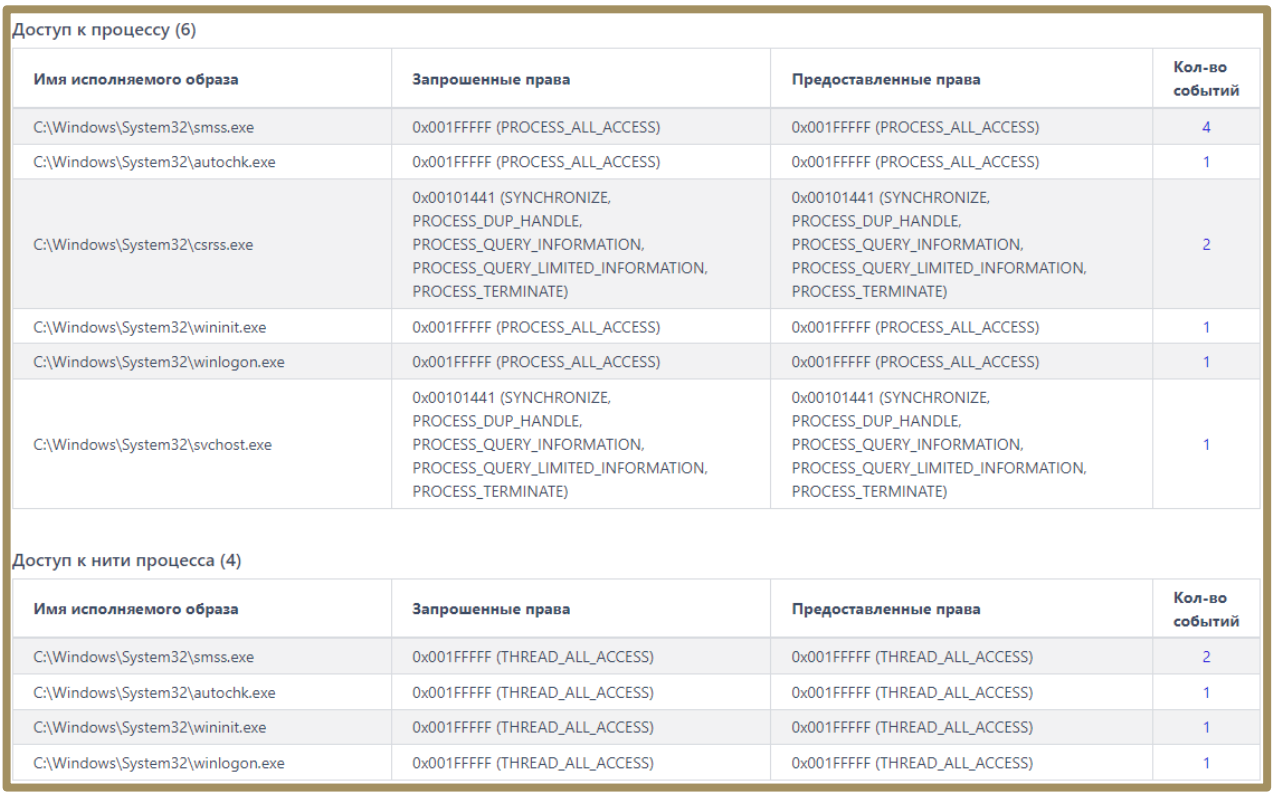
2) **Значение** – в поле отображается значение, которое было внесено выбранным процессом в ключ реестра;

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

Вкладка «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. 17).



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 17 – Информация на вкладке «Процессы»

Информация представлена в таблице, которая содержит следующие поля:

– **Имя исполняемого образа**;

– **Запрошенные права**;

– **Предоставленные права**;

– **Кол-во событий**.

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

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

Вкладка «Загруженные DLL/SO»

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

Важно

Если в профиле безопасности агента установлена опция **Исключать события загрузки известных модулей**, то в списке DLL этих модулей не будет. Подробный список известных DLL-библиотек содержится в пункте 10.20.2.

Информация о библиотеках, которые были загружены рассматриваемым процессом, представлена в таблице со следующими полями:

1) **Нативные** или **.NET** (содержит абсолютный путь нативной или .NET-библиотеки);
2) **Размер файла**;
3) **Подпись**;
4) **Размещение** (содержит базовый адрес DLL в файловой таблице);
5) **Хеш (SHA-256)**.

В поле с хеш-суммой аналитик может скопировать значение хеша в буфер обмена с помощью кнопки , а также перейти по ссылке () на страницу **Процессы и и модули**, чтобы изучить подробную информацию о выбранной библиотеке (когда и где обнаружена, распространенность в инфраструктуре и т.д.).

Рядом с названием библиотеки находится кнопка раскрытия дополнительной информации о событии, связанном с библиотекой ( ). При нажатии ЛКМ на кнопку открывается карточка событий, связанная с рассматриваемыми процессом и библиотекой.

Для процесса **%SYSTEM%** будет представлен список загруженных в процесс модулей ядра, дополнительная информация о которых также становится доступной при нажатии кнопки >.

Вкладка «Точки автозапуска»

Во вкладке **Точки автозапуска** отображается информация о точках автозапуска, созданных рассматриваемым процессом в реестре (рис. 18).

Реестр (21)

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

Рисунок 18 – Точки автозапуска

Примечание

Под точками автозапуска подразумеваются процессы, автоматически запускаемые на агентах при возникновении тех или иных условий, например, запуск программы при загрузке операционной системы.

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

Вкладка «Распространенность»

Во вкладке **Распространенность** отображается информация о распространении исполняемого модуля выбранного процесса в агентской сети.

При этом аналитику показывается, когда модуль 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.

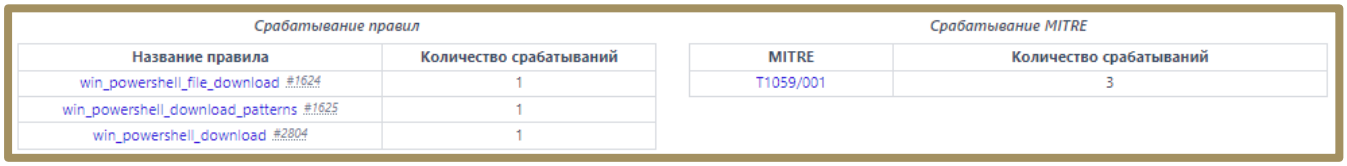
Вкладка «Событие старта»

Во вкладке «Событие старта» показана карточка события для старта процесса.

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

Вкладка «Правила/MITRE»

Во вкладке **Правила/MITRE** содержится информация о срабатываниях действующих в EDR правил, а также техник MITRE для выбранного процесса (рис. 19).



Срабатывание правил

Название правила	Количество срабатываний
win_powershell_file_download #1624	1
win_powershell_download_patterns #1625	1
win_powershell_download #2804	1

Срабатывание MITRE

MITRE	Количество срабатываний
T1059/001	3

Рисунок 19 – Правила/MITRE

10.2.2. Загрузка и проверка файлов в хранилище

На странице **Инцидент** аналитик может открыть карточку события, связанного с инцидентом и просмотреть дополнительную информацию об этом событии.

Чтобы просмотреть карточку события-обнаружения необходимо нажать на кнопку › (рис. 20).

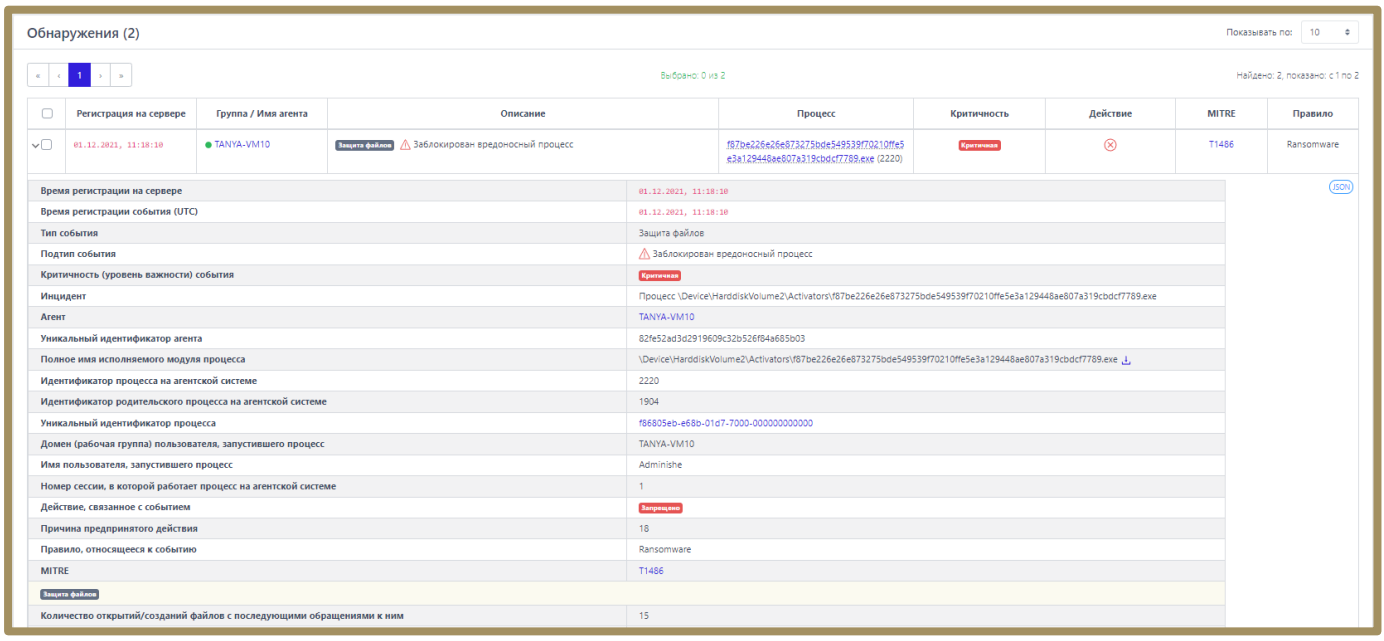


Рисунок 20 – Карточка с описанием события

Карточка событий содержит различные сведения в зависимости от типа и подтипа событий. Часть полей, отображаемых в карточке, являются общими для всех типов и подтипов событий.

В поле **Полное имя исполняемого модуля процесса** содержится путь до исполняемого файла. Аналитик может выгрузить файл с конечной точки и загрузить в файловое хранилище сервера EDR для проверки с помощью TI-платформы или программы просмотра файлов.

Для загрузки выбранного файла в файловое хранилище модуля администрирования необходимо нажать кнопку  (рис. 21).

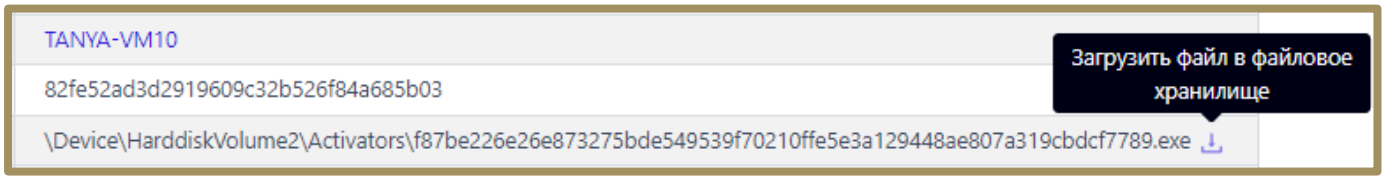


Рисунок 21 – Отправка файла на анализ

Для дальнейшего анализа файла следует перейти в раздел **Хранилище** (рис. 22) и с помощью представленных на странице фильтров найти нужный файл.

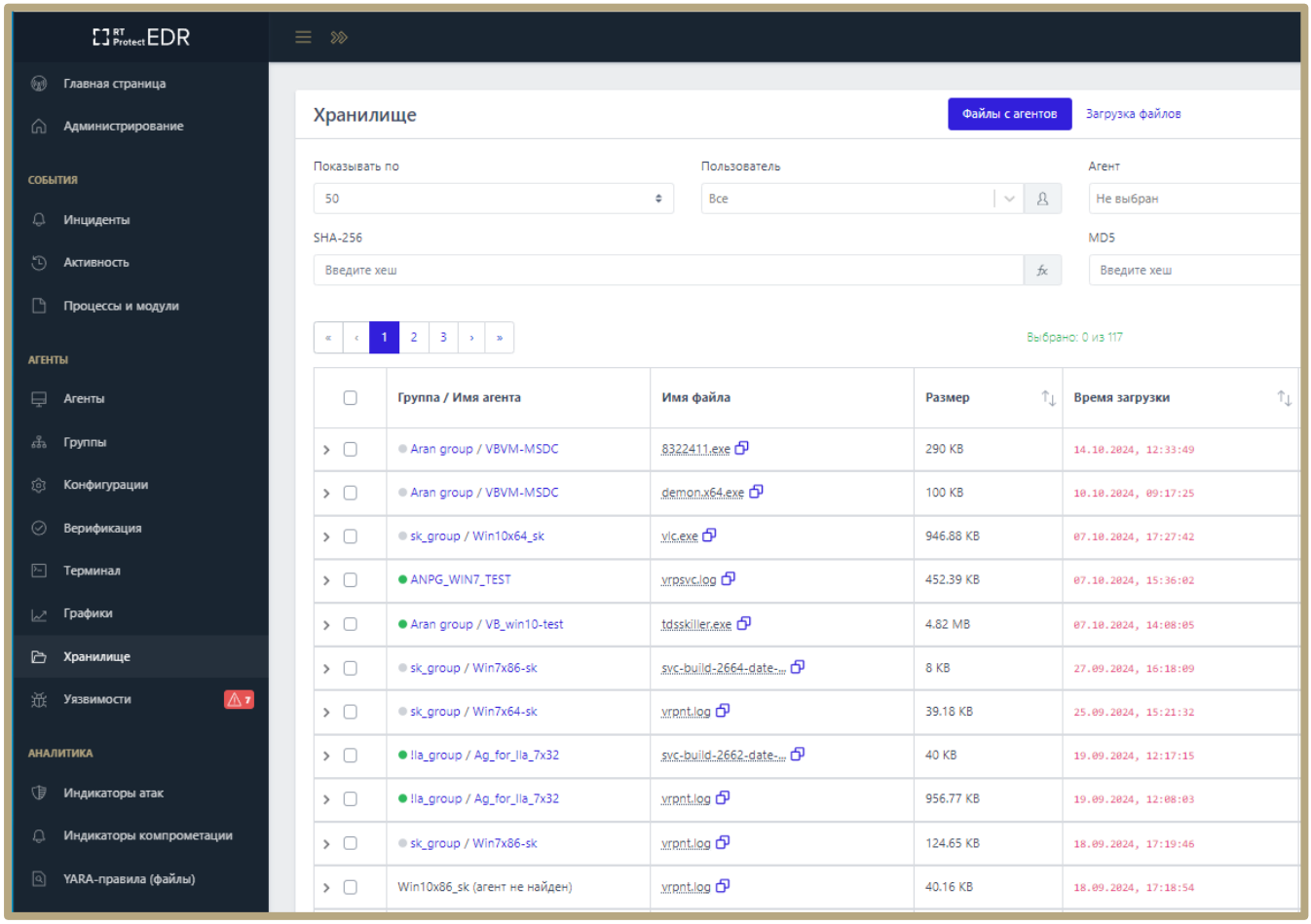


Рисунок 22 – Хранилище загруженных файлов

С загруженным в хранилище файлом возможно выполнить следующие действия для анализа:

– проверить с помощью базы данных TI-платформы (TI);

– просмотреть файл с помощью программы просмотра файлов (кнопка);

– удалить файл из хранилища (кнопка).

При нажатии кнопки TI (безопасный файл) в столбце **Результаты проверки** появляется окно с результатами анализа файла TI-платформой. Кнопка со значком TI обозначает вредоносный файл. Кнопка со значком TI обозначает продозрительный файл. Кнопка со значком TI обозначает проверку файла на TI-платформе в текущий момент времени. В случае загрузки файла, информация по которому отсутствует на TI-платформе, кнопка отчета файла отображается со значком TI. Нажатие кнопки открывает окно с кратким отчетом по артефакту, чтобы посмотреть полный отчет, необходимо нажать кнопку **Перейти к отчету**, после чего открывается страница подробного отчета TI-платформы о проверке загруженного файла (рис. 23).

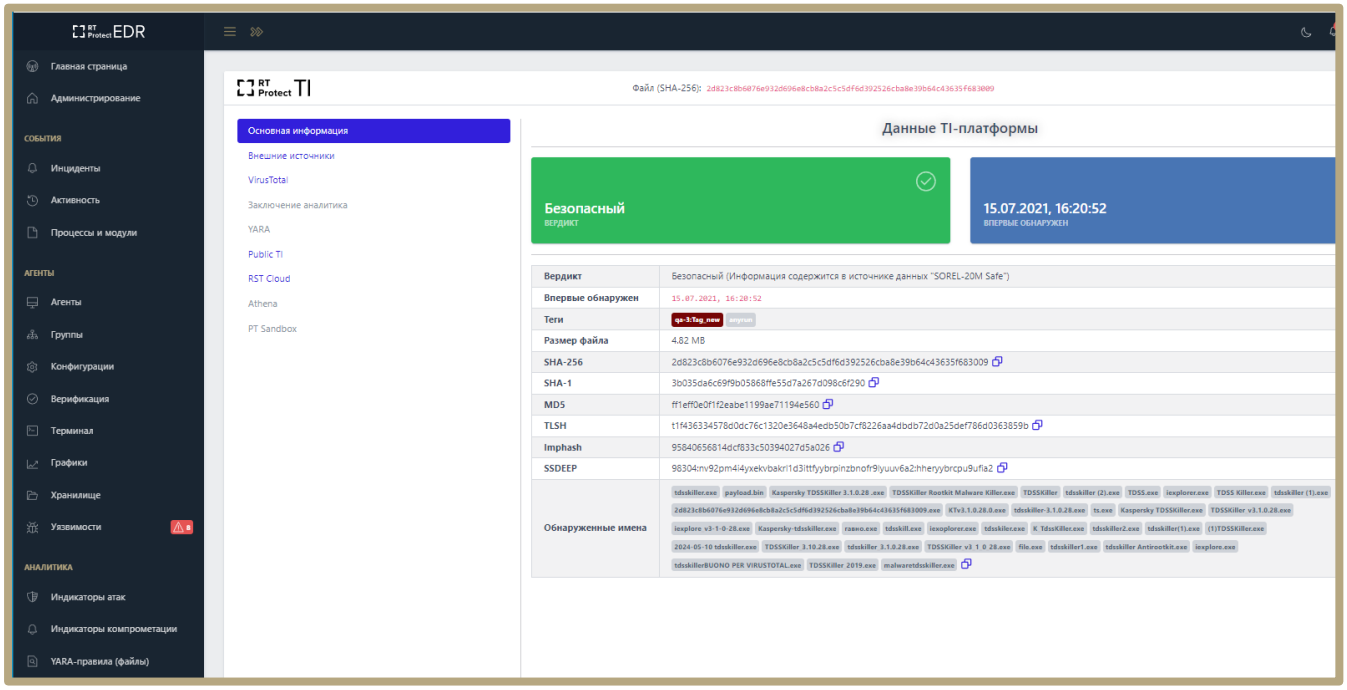


Рисунок 23 – Окно отчета проверенного файла

Отчет TI-платформы также можно посмотреть в формате JSON, нажав кнопку JSON.

В зависимости от артефакта страница отчета может содержать разную информацию, но всегда будет содержать вкладку **Основная информация,** где будет отображаться вердикт. На странице отчета могут быть показаны следующие вкладки:

1) **Внешние источники**;

2) **VirusTotal** (вкладка делится на две части: DETECTION с вердиктами вендоров и DETAILS с подробной информацией об артефакте);

3) **Заключение аналитика**;

4) **YARA**;

5) **Public TI** и другие (в зависимости от модулей, подключенных к TI-платформе).

После изучения файла аналитик может принять решение о дальнейших действиях: закрыть инцидент и внести файл в исключения, если произошло ложноположительное срабатывание, изолировать агента, на котором файл был обнаружен, воспользоваться терминалом для возврата зараженной системы в состояние до заражения, продолжить расследование с помощью фильтрации событий на странице **Активность** и т.д.

Кроме загрузки файлов с агентов аналитику доступна загрука файлов в **Хранилище** с компьютера, с которого осуществлен доступ в модуль администрирования. Для загрузки и просмотра таких файлов

необходимо перейти на вкладку **Загрузка файлов**. Кроме такой загрузки файла в **Хранилище** аналитик может скачать загруженный ранее файл (не тот, что был загружен с агента, а тот, что загружен на сервер управления с компьютера, с которого осуществлен доступ к серверу управления), используя значок **Получить ссылку на скачивание** ( ). При копировании ссылки в строку браузера скачивание файла произойдет автоматически.

10.3 Расследование с «Главной страницы» или страницы «Инциденты»

Главная страница административного модуля управления агентами на сервере представлена на рисунке 6. На странице аналитик может просмотреть сводную информацию обо всей инфраструктуре, подключенной к модулю управления:

– количество защищаемых агентов;

– количество событий в защищаемой инфраструктуре за последние 15 минут;

– общее количество инцидентов;

– список последних обнаруженных процессов и модулей;

– значение EPS (Event per Second), которое показывает количество приходящих от агентов событий в секунду (показывается текущее значение событий в секунду на всех агентах, а также на одном агенте, кроме того в отдельной области отображается среднее количество событий на всех активных агентах в секунду за неделю);

– информация об инцидентах (динамика и распределение по критичности);

– информация о самых часто встречающихся в инцидентах правилах;

– информация о самых часто встречающихся в инцидентах техниках MITRE;

– информация об уязвимостях.

В разделе **Главная страница** аналитик также может просмотреть, сколько пакетов с событиями находится в очереди для отправки на сервер, это может помочь выявить проблемы на сервере (например, очередь может образоваться, если жесткий диск сервера частично вышел из строя).

Совет

Первое, что желательно сделать аналитику при обнаружении инцидента, если инцидент не является ложноположительным срабатыванием – это перейти на страницу агента, на котором произошел инцидент, и настроить изоляцию агента.

Если произошло ложноположительное срабатывание, то аналитику необходимо создать исключающее правило.

Для детального изучения инцидента возможно перейти на страницу с инцидентами двумя способами:

1) Нажав значение количества инцидентов в области **Инциденты**;

2) Нажав в области **Критичность инцидентов** по иконкам (Критичная - 2 , Высокая - 2 и т.д.);

При выполнении любого из действий, описанных выше, откроется страница **Инциденты** (рис. 24). Аналитик может сразу перейти на страницу **Инциденты**, выбрав одноименный раздел на панели управления модуля администрирования (Инциденты).

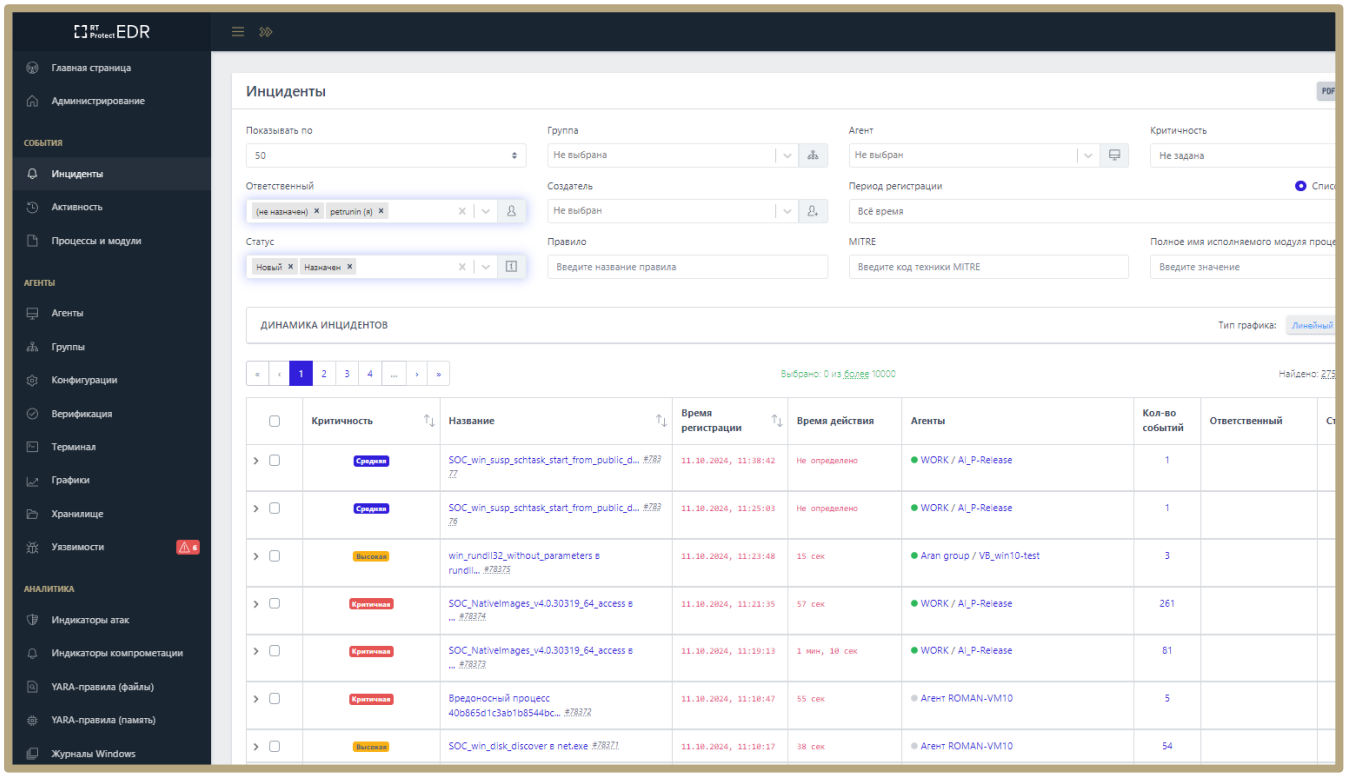


Рисунок 24 – Окно страницы «Инциденты»

В верхней части страницы отображается график, показывающий количество зарегистрированных инцидентов в течение выбранного периода (по умолчанию за все время). Открывается с помощью кнопки **Показать графики** ( ) в строке **Динамика инцидентов**. График можно поменять с линейного на столбчатый тип.

В поле кнопки выбора инцидентов содержится кнопка раскрытия дополнительной информации о событиях, включенных в инцидент ( ). При нажатии ЛКМ на значок снизу от строки инцидента открывается дополнительная информационная область, в которой пользователь может просмотреть важные данные об инциденте (рис. 25).

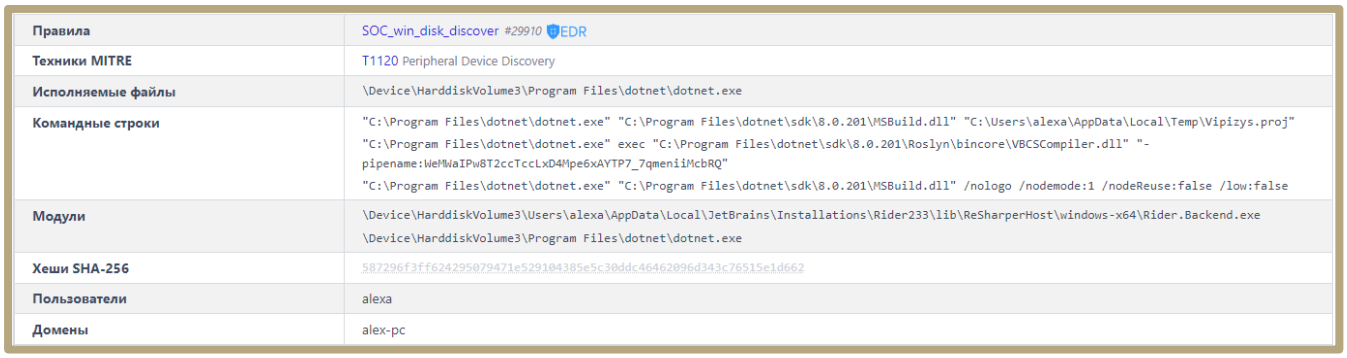


Рисунок 25 – Дополнительная информация об инциденте

В поле **Критичность** основной таблицы с инцидентами показывается информация о степени критичности инцидента. Всего предусмотрено пять уровней критичности: **Информация** (наименее критичный уровень инцидента), **Низкий**, **Средний**, **Высокий**, **Критичный** (наиболее критичный уровень инцидента).

В поле **Название** таблицы **Инциденты** находится имя, присвоенное инциденту и его номер. Инциденты, которые пользователи создают вручную, помечаются значком . Значок отображается рядом с названием. При нажатии ЛКМ на имени инцидента происходит переход на страницу **Инцидент**.

Для изменения названия инцидента в поле **Название** справа от имени инцидента содержится кнопка **Редактировать** ( ). Кнопка будет отображаться только для инцидента, у которого назначен ответственный за его решение пользователь. При нажатии кнопки открывается окно **Редактирование инцидента** (рис. 26).

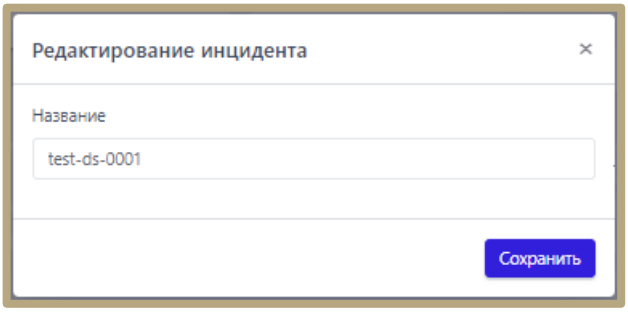


Рисунок 26 – Редактирование инцидента

Для изменения имени инцидента необходимо ввести произвольное имя в строке **Название**, после чего нажать кнопку **Сохранить** для завершения операции. После завершения операции в нижней части страницы отобразится всплывающее окно с сообщением.

В поле **Время регистрации** отображается информация о времени регистрации инцидента.

В поле **Время действия** отображается информация о времени, в течение которого происходил инцидент. Это время рассчитывается, как разница между временем, когда началось первое событие инцидента, и временем, когда закончилось последнее событие инцидента.

В поле **Агенты** отображается информация о группе, в которую входит агент, для которого создан инцидент и имя агента. При нажатии на имени группы или названии агента происходит переход к страницам **Группа** и **Агент**.

В поле **Кол-во событий** отображается информация о количестве событий, входящих в инцидент.

В поле **Ответственный** находится кнопка **Изменить** ( ), с помощью которой можно изменить пользователя, ответственного за решение инцидента. При нажатии кнопки **Изменить** открывается окно **Выбор ответственного по инциденту** (рис. 27).

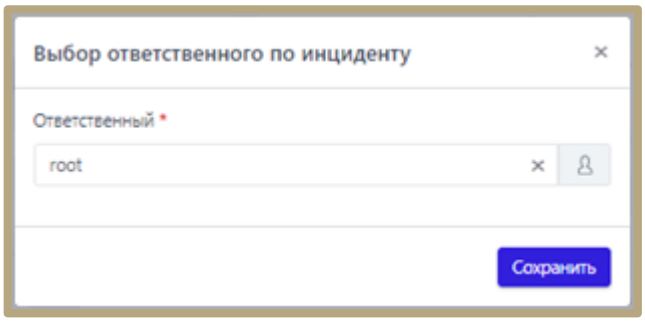


Рисунок 27 – Выбор пользователя, ответственного за решение инцидента

В случае, если ответственный за инцидент уже был назначен, то для выбора нового пользователя, ответственного за инцидент, необходимо в строке **Ответственный** удалить текущего пользователя, нажав в ней кнопку ×. Далее выбрать пользователя из списка, нажав ЛКМ на пустую строку поля **Ответственный**, или ввести в ней с клавиатуры имя нового пользователя, ответственного за инцидент.

Для завершения процедуры назначения ответственного пользователя следует нажать кнопку Сохранить, после чего в нижней части страницы отобразится всплывающее окно с сообщением.

В поле **Статус** отображается информация о текущем статусе инцидента. В зависимости от текущего статуса инцидента в поле будут отображаться различные кнопки, с помощью которых можно изменить некоторые параметры инцидента:

1) Закрыть инцидент – (активна при статусе **Назначен** или **Новый**);
2) Назначить или открыть инцидент повторно – (активна при статусе **Новый** и **Закрыт**);

Для закрытия инцидента необходимо нажать кнопку **Закрыть инцидент** () и в открывшемся окне **Закрытие инцидента** нажать кнопку **Сохранить**. Закрыть инцидент можно даже в случае, если для него не назначен ответственный.

После выполнения операции в нижней части страницы появится всплывающее окно с сообщением.

По умолчанию в окне **Закрытие инцидента** в поле **Комментарий** стоит запись [**Закрытие инцидента**], ее можно изменить на произвольный комментарий или сохранить статус инцидента без комментария. Поле **Комментарий** предусматривает возможность написания до 1000 символов. Информация, указанная пользователем в комментарии, отобразится на странице **Инцидент**.

Для того, чтобы назначить ответственного пользователя по новому инциденту, необходимо нажать кнопку **Назначить инцидент** () и в открывшемся окне **Назначение инцидентов** в поле **Ответственный** выбрать пользователя, ответственного за решение инцидента, после чего нажать кнопку **Сохранить**. После завершения операции по назначению ответственного за решение инцидента в нижней части страницы появится окно с сообщением.

Кроме назначения ответственного в окне **Назначение инцидента** пользователь может ввести произвольный комментарий в поле **Комментарий**, сохранить статус инцидента без комментария или оставить комментарий по умолчанию. Желательно, чтобы комментарий был информативным и отражал суть текущей

стадии работы с инцидентом. Информация, указанная пользователем в поле **Комментарий**, отобразится на странице **Инцидент**.

Для повторного открытия инцидента необходимо нажать кнопку **Назначить инцидент (открыть повторно)** (), после чего в открывшемся окне **Назначение инцидентов** нажать кнопку **Сохранить**, изменив или сохранив текущего пользователя в качестве ответственного за решение инцидента. При повторном назначении можно, как и при любой другой смене статуса, добавить комментарий, который отобразится на странице **Инцидент**.

Для фильтрации инцидентов по тем или иным признакам на странице **Инциденты** содержатся следующие фильтры:

1) **Показывать по**;
2) **Группа**;
3) **Агент**;
4) **Критичность**;
5) **Ответственный**;
6) **Создатель**;
7) **Период регистрации** (список или календарь)
8) **Статус**;
9) **Правило** (поиск по правилам, на основе которых создаются обнаружения);
10) **MITRE** (поиск по TTP);
11) **Полное имя исполняемого модуля процесса**.

Принцип работы с фильтрами не отличается от работы с фильтрами в разделе **Активность**.

В полях фильтров **Правило**, **MITRE**, **Полное имя исполняемого модуля процесса** поддерживается автоподставление символов wildcard (*) для фильтров по агрегированным полям.

Для фильтрации в поле фильтра **Правило**, следует писать название правила без расшифровки.

Пример:

MaliciousDomain в chrome.exe – правило с расшифровкой (MaliciousDomain – правило, по которому будут фильтроваться инциденты).

Фильтр **Период регистрации** в сравнении с фильтром **Период регистрации (на сервере)** на странице **Активность** содержит одно дополнительное значение **Всё время**, при выборе которого показываются все когда-либо зарегистрированные в Программе инциденты.

В поле фильтра **Статус** возможно выбрать следующие варианты статуса инцидента из всплывающего списка:

1) Новый;
2) Назначен;
3) Закрыт.

В поле фильтра **Ответственный** задаётся фильтрация инцидентов по пользователю, ответственному за решение инцидента. Сброс значений фильтров осуществляется с помощью кнопки Сбросить фильтры.

Для сортировки инцидентов в полях таблицы с инцидентами **Критичность**, **Название**, **Время регистрации** и **Статус** используются кнопки смешанной сортировки, сортировки по возрастанию и сортировки по убыванию.

Дополнительная область с событиями инцидента (рис. 28) содержит следующие показатели:

1) Время регистрации события инцидента;
2) Критичность инцидента/Действие, предпринятое программой;
3) Краткая сводка об инциденте;
4) Процесс, работа которого привела к созданию инцидента;
5) Идентификатор техники MITRE (опционально);
6) Сведения о правиле или исключении, на основе которого сформирован инцидент.

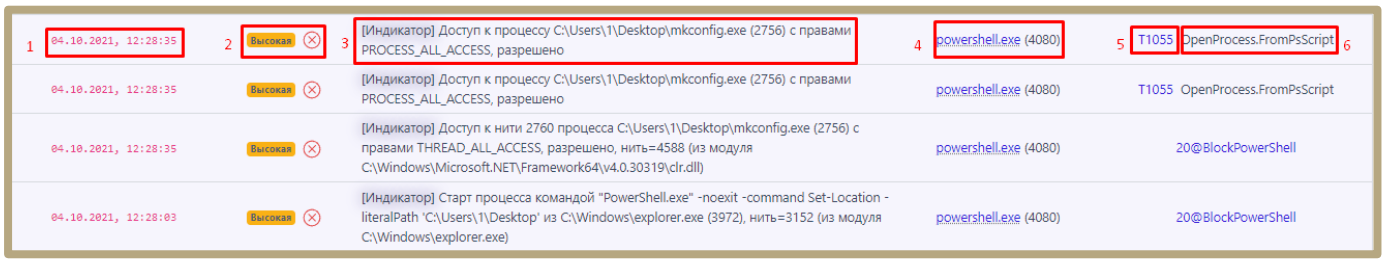


Рисунок 28 – Поля дополнительной области инцидента

Поле **Время** содержит информацию о времени обнаружения события, включённого в инцидент.

В поле **Критичность/Действие** отображается информация о степени критичности обнаруженного события инцидента. Предусмотрено пять степеней критичности событий:

– Информация;

– Низкая;

– Средняя;

– Высокая;

– Критичная.

Рядом с критичностью события отображается значок действия, связанного с событием. В Программе предусмотрено три вида действия, предпринимаемых в ответ на возникновение какого-либо события:

1) Блокировать (с указанием причины блокирования и правила, в соответствии с которым оно было выполнено) – обозначается значком  ;

2) Детектировать (с указанием причины обнаружения и правила, в соответствии с которым было детектировано событие) – обозначается значком  ;

3) Продолжать наблюдение (в этом случае поле будет пустым, это связано с тем, что событие не подпадает под действие какого-либо регулирующего правила).

В поле с названием обнаружения показана краткая информация о сути события, детектированного системой как вредоносное, опасное или требующее внимание пользователя.

В поле с именем процесса содержится ссылка в виде имени на модуль исполняемого файла процесса. Ссылка позволяет быстро перейти к странице **Процессы** и при необходимости завершить процесс или расследовать особенности его выполнения (см. пункт 10.2.1).

В поле с идентификатором **MITRE** отображается ссылка на идентификатор техники атаки из базы знаний MITRE ATT&CK, на которую указывает событие, включенное в инцидент. Информация в поле добавляется опционально.

В поле с обозначением имени правила указывается информация о правиле, в соответствии с которым Программа выполнила действие для события, добавленного в инцидент.

В нижней части страницы **Инциденты** содержатся кнопки для выполнения следующих операций:

– назначить ответственного за решение инцидентов;

– закрыть выбранные инциденты;

— удалить выбранные инциденты.

Чтобы назначить ответственного, необходимо выбрать один или несколько инцидентов с помощью кнопки выбора, отметив их флажками ( ), далее нажать кнопку **Назначить выбранные**, после чего в открывшемся окне **Назначение инцидентов** выбрать ответственного и нажать кнопку **Сохранить**.

Чтобы закрыть инциденты, необходимо выбрать один или несколько инцидентов с помощью кнопки выбора, отметив их флажками, далее нажать кнопку **Закрыть выбранные**, после чего в окне **Закрытие инцидентов** ввести произвольный комментарий и нажать кнопку **Отправить**. При назначении желательно оставить комментарий, который поможет ответственному за решение инцидента сотруднику приступить к выполнению своей задачи. Закрывать инциденты можно даже тогда, когда для них не назначены ответственные.

Для удаления инцидентов необходимо отметить флажками кнопки выбора соответствующих инцидентов и нажать кнопку **Удалить выбранные** в нижней части страницы **Инциденты**. Далее необходимо нажать в открывшемся окне кнопку **Начать удаление**, после чего подтвердить операцию. Начнется удаление инцидента. После завершения операции необходимо нажать кнопку **Закрыть**.

Процесс удаления инцидента возможно прервать. Для прерывания инцидента требуется нажать по иконке **Прервать удаление**. Удаление инцидента прервется на том инциденте, которому еще не отправлена команда на удаление, и в списке удаляемых инцидентов инцидент не помечен .

Процесс расследования инцидента с **Главной страницы** или из раздела **Инциденты** подразумевает действия, описанные в подразделе 10.2.

Для наглядности можно рассмотреть работу с интерфейсом Программы на примере, описывающем определенный сценарий с позиций работы аналитика.

Сценарий. Поиск инцидентов самой высокой критичности для произвольного агента на период регистрации инцидента 3 месяца.

Действия:

1) Поставить фильтр **Критичность** (Критичная);
2) Поставить фильтр **Период регистрации** (3 месяца);
3) Поставить фильтр **Агент** (произвольный агент).

После применения фильтров окно страницы **Инциденты** будет иметь вид (рис. 29).

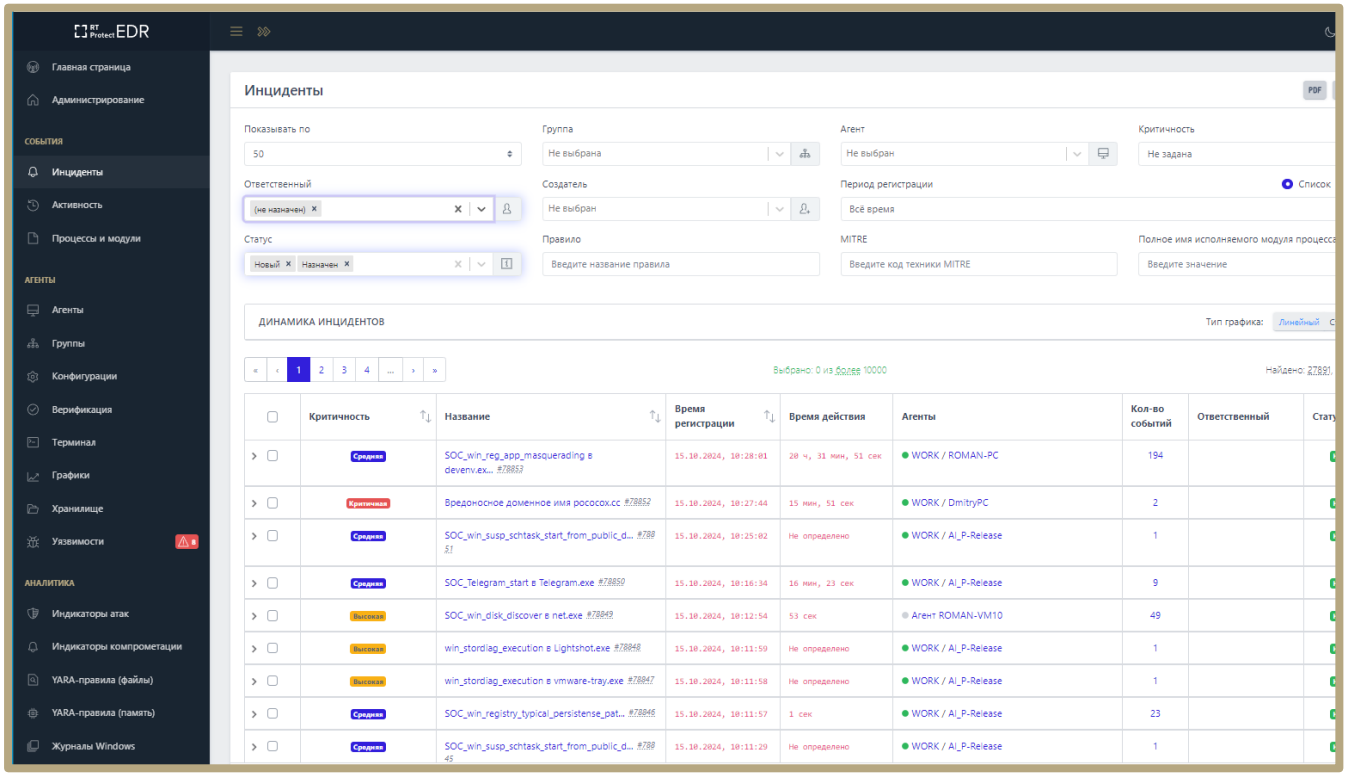


Рисунок 29 – Окно страницы «Инциденты»

10.3.1. Анализ инцидента.

Для начала анализа инцидента необходимо в столбце **Название** страницы **Инциденты** нажать левой кнопкой мыши по названию интересующего инцидента для перехода на страницу **Инцидент**.

В окне страницы **Инцидент** следует просмотреть общую информацию об инциденте и его событиях. Кратко ознакомиться с информацией о событии или событиях, составляющих инцидент, можно, нажав кнопку › в строчке напротив интересующего события/ий (рис. 30).

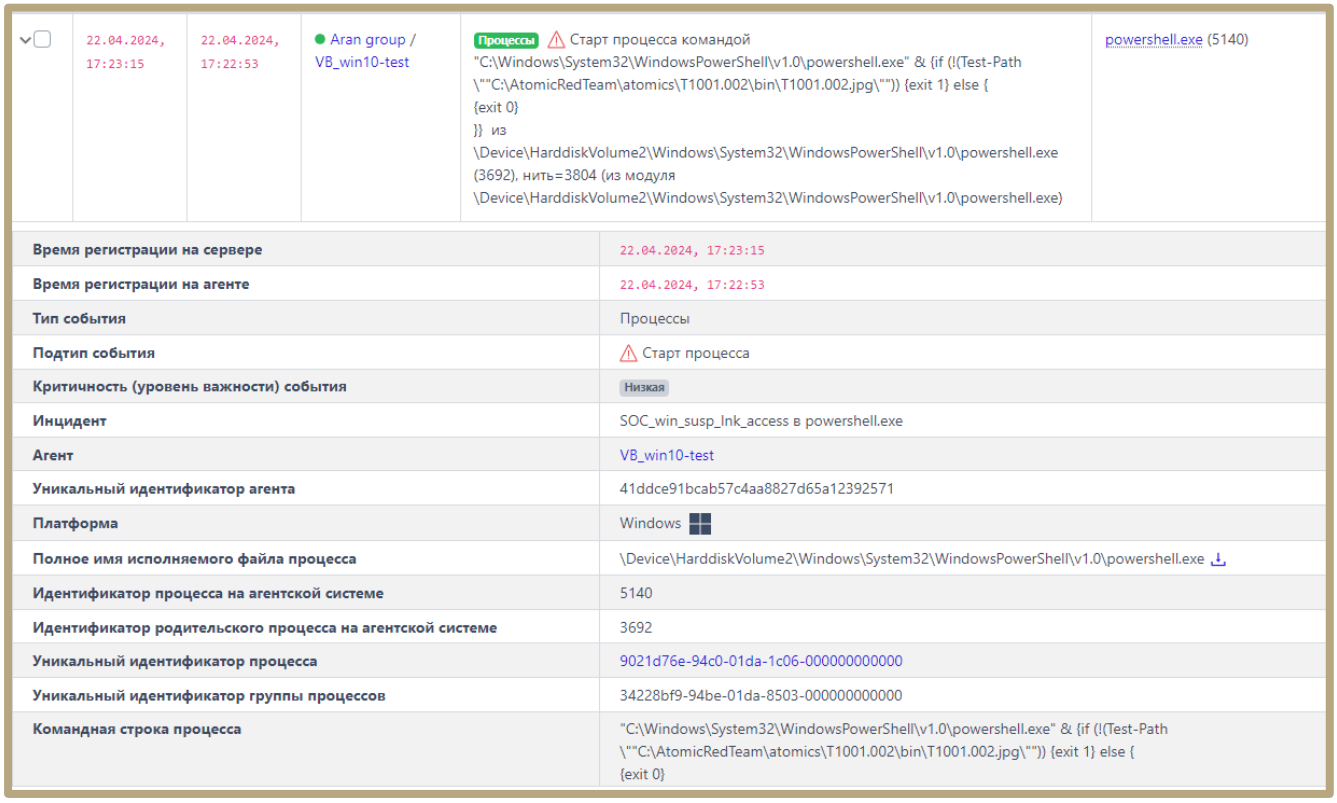


Рисунок 30 – Вызов всплывающего окна с информацией о событии

Дополнительная информация о выбранном событии содержится на странице в виде карточки события. Информация в окне о событии имеет различное содержание в зависимости от типа и подтипа события. Карточку события можно просмотреть в формате JSON, чтобы при необходимости составить правило для индикации атак. Сведения о метаданных, обнаруживаемых Программой и предоставляемых аналитику в карточках событий содержатся в разделе 9.

Справа от таблицы с данными находится кнопка JSON. Любой элемент или блок элементов в формате JSON можно скопировать, нажав кнопку . Для возврата к результатам отчета в формате HTML необходимо нажать ЛКМ на значок HTML.

Жизненный цикл каждого инцидента подразумевает прохождение трех стадий:

— новый инцидент;

— назначенный в работу;

— закрытый инцидент.

Совет

Если инцидент не представляет больше ценности для дальнейшей работы, его можно удалить. Для этого используется кнопка **Удалить инцидент** в области **Информация об инциденте**. При этом вместе с инцидентом удаляются и события, которые входят в этот инцидент.

В зависимости от статуса инцидента у страницы **Инцидент** функциональность может различаться. Для нового и закрытого инцидента недоступна функция редактирования инцидента. Чтобы отредактировать инцидент, необходимо назначить пользователя, ответственного за его решение. Страница **Инцидент** разделена на следующие области:

1) **Инцидент**;

2) **Комментарии**;

3) **Дополнительная информация;**

4) **Обнаружения**.

В области **Инцидент** пользователь может назначить инцидент на того или иного аналитика для дальнейшей работы или выполнить другие действия:

– редактировать инцидент;

– закрыть инцидент;

– открыть инцидент повторно;

– удалить инцидент;

– сохранить отчет об инциденте в файл формата pdf на компьютер, с которого осуществлен доступ в модуль администрирования (кнопка 

).

В области **Инцидент** отображаются следующие данные:

– название инцидента;

– критичность инцидента;

– ответственный за решение инцидента;

– статус инцидента;

– агент, на котором произошли события инцидента;

– время регистрации инцидента;

— время действия инцидента;

— описание.

Редактировать можно следующие параметры:

— название;

— ответственный;

— критичность;

— описание.

Примечание

Операции редактирования имени инцидента, критичности, описания, а также исключение событий из инцидента становятся доступными после назначения ответственного за инцидент.

После завершения редактирования необходимо нажать кнопку **Сохранить изменения**.

В области **Комментарии** пользователь может указать произвольный комментарий. Также комментарии указываются автоматически при переводе инцидента из одного статуса в другой, например, при назначении или закрытии инцидента.

Примечание

Поле **Комментарий**, как и поле **Описание**, позволяет ввод до 1000 символов.

Для добавления нового комментария следует нажать кнопку **Создать комментарий**, после чего открывается окно **Создать комментарий** (рис. 31).

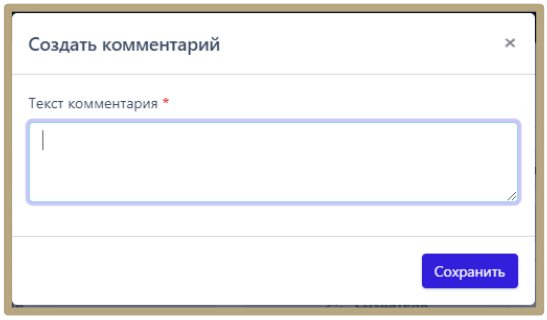


Рисунок 31 – Окно ввода комментария

Для добавления комментария к инциденту необходимо ввести в окне **Новый комментарий** текст комментария и нажать кнопку **Отправить**, после чего комментарий пользователя будет добавлен на страницу инцидента.

Для отмены ввода комментария следует в окне **Новый комментарий** нажать кнопку **Отмена** или **Закрыть окно** ( ).

В области **Дополнительная информация** представлена информация по инциденту с уточнением параметров, характеризующих инцидент, таких как наименование правила, на основе которого сформирован инцидент, имена исполняемых файлов и командные строки, участвующие в инциденте, затронутые инцидентом пользователи и домены, удаленные сетевые точки и локальные конечные точки, хеши, техники MITRE и т.д.

В области **Обнаружения** в табличном виде представлена информация о событиях, которые были включены в инцидент при его регистрации. Переход по страницам в таблице в случае, если события в инциденте не умещаются на одной странице, осуществляется с помощью пагинатора.

В верхней части области **Обнаружения** отображается информация об общем количестве событий в инциденте и фильтр **Показывать по** (можно задавать следующие значения: 10, 20, 50, 100).

В таблице с обнаружениями информация распределена по следующим полям:

1) **Регистрация на сервере**;
2) **Регистрация на агенте**;
3) **Группа/Имя агента**;
4) **Описание**;
5) **Процесс**;
6) **Информация**.

Регистрация на сервере – содержит информацию о годе, месяце, дне и точном времени регистрации обнаружения на сервере по стандарту UTC.

Регистрация на агенте – содержит информацию о годе, месяце, дне и точном времени регистрации обнаружения на агенте, то есть по текущему времени, которое установлено на машине с агентом.

Группа/Имя агента – в поле отображаются группа, в которой находится агент, и название агента, имена группы и агента служат гиперссылкой для перехода к соответствующим страницам.

Описание – содержит краткое описание события, которое системой определено как обнаружение или телеметрия, событие-обнаружение помечается значком .

Процесс – содержит имя процесса, действия которого привели к обнаружению Программой, имя процесса отображается в виде ссылки для перехода к странице **Процессы**.

В поле **Информация** показаны следующие данные по обнаружению:

– **Критичность/Действие**;

– **MITRE**;

– **Правило.**

Критичность/Действие – показывает уровень угрозы, которая исходит от обнаруженного события для защищаемой ИТ-инфраструктуры, для автоматических обнаружений это средний, высокий и критический уровень, а также в поле отображается действие, предпринятое в связи с обнаружением события. Программой предусмотрены три действия: блокировать, детектировать и продолжение наблюдения. В последнем случае поле останется пустым.

MITRE – в поле отображается идентификатор техники атаки MITRE ATT&CK, который соответствует событию, добавленному в инцидент (идентификатор назначается опционально).

Правило – в поле отображается наименование правила, в соответствии с которым событие было добавлено в инцидент.

В поле **Информация** также находится кнопка **Ложное срабатывание** ( ). Нажав на кнопку, пользователь может создать исключение для файла с помощью мастера исключений.

Создать исключение с помощью мастера можно не для всех инцидентов.

Общий вид окна при создании исключения с помощью мастера исключений для файла представлен на рисунке 32.

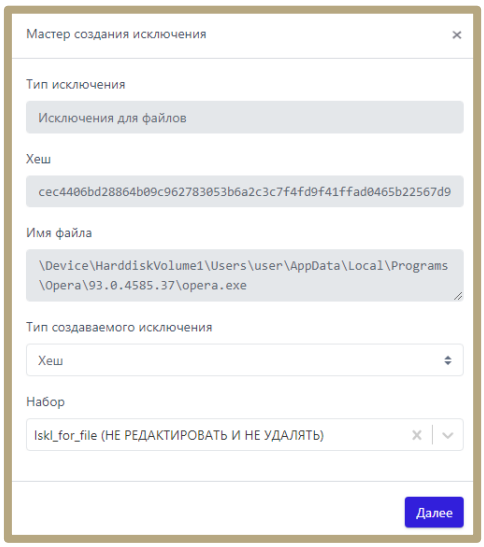


Рисунок 32 – Окно мастера создания исключений

В данном окне поля **Тип исключения**, **Хеш**, **Имя файла** устанавливаются автоматически из выбранного обнаружения, требуется определить только тип создаваемого исключения: исключение по хеш-сумме или исключение по имени файла. Также можно указать набор, в который следует добавить исключение.

Для дальнейшего создания исключения требуется нажать кнопку **Далее**, после чего произойдет переход к окну добавления исключения (рис. 33).

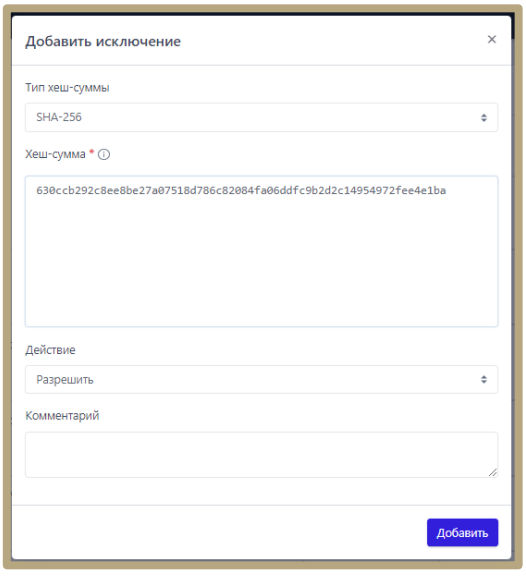


Рисунок 33 – Окно добавления исключения

Хеш-сумма заполняется автоматически из предыдущего окна. Чтобы завершить добавление исключения, требуется только определить действие (**Разрешить**/**Блокировать**) и нажать по кнопке **Добавить**.

После просмотра информации об инциденте аналитик может сохранить отчет о нем в файл формата pdf на компьютер, с которого осуществлен доступ в модуль администрирования. Для этого предусмотрена кнопка  в области **Информация об инциденте**.

Совет

Кроме фильтрации событий и просмотра дополнительной информации в расследовании инцидентов аналитику могут помочь данные киберразведки (Threat Intelligence), которые предоставляются TI-платформой.

Для просмотра дополнительных данных об артефактах, выявленных в инциденте можно просмотреть отчет TI-платформы. Платформа сопоставляет и анализирует данные компьютерных угроз из нескольких источников в режиме реального времени для поддержки защитных действий Программы. На данный момент платформой проверяются следующие артефакты:

1) Хеш файла;
2) Глобальный IP-адрес;
3) Глобальное имя домена.

Проверка выполняется в нескольких источниках, в зависимости от типа артефакта набор источников может отличаться:

1) Внешние источники;
2) VirusTotal;
3) Заключение аналитика;
4) YARA;
5) IOC;
6) Whois;
7) Public TI.

Примечание

Вердикты TI-платформы равнозначны с аналитикой сервера EDR. Например, если вердикт платформы по определённому хешу исполняемого файла будет отмечен как вредоносный, а на сервере EDR тот же хеш будет отмечен как безопасный, то будет создан инцидент. То же самое произойдет и в обратном случае, когда сервер EDR отмечает артефакт как вредоносный, а TI-платформа как безопасный. В то же время необходимо учитывать, что механизм сетевых исключений EDR позволяет переопределить вердикт TI-платформы с вредоносного на безопасный.

TI-платформа может предоставлять другие аналитические данные:

— индикаторы атак;

— заключения аналитика;

— индикаторы компрометации;

— YARA-правила;

— журналы Windows.

Если правила TI-платформы и правила сервера EDR будут дублировать друг друга, то в случае обнаружения вредоносных артефактов создадутся два независимых инцидента. Страницы отчета TI-платформы открываются на вкладке **Общая информация**, которая содержит сводные данные из всех доступных для выбранного артефакта источников (рис 34).

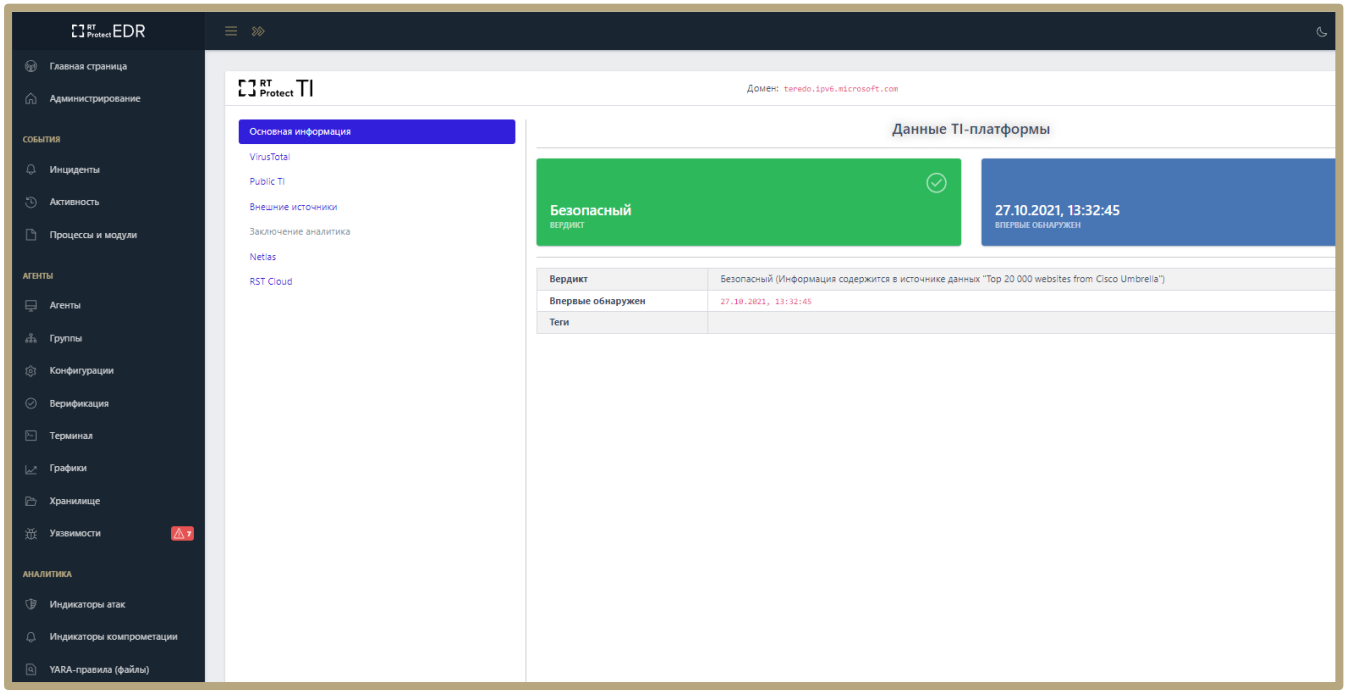


Рисунок 34 – Отчет TI-платформы

В верхней части страницы отчета отображается наименование и значение артефакта и вердикт TI-платформы. На левой панели отчета отображаются вкладки с наименованиями источников данных, от которых были получены сведения для вынесенного вердикта. На правой панели отчета отображается информация о выбранном артефакте.

Информация представлена в табличном виде. Поля таблицы могут содержать следующие данные:

1) Вердикт (безопасный/вредоносный/подозрительный/неизвестный/в процессе анализа);
2) Время обнаружения;
3) Размер файла;
4) Хеш, рассчитанный по алгоритму SHA-256;
5) Хеш, рассчитанный по алгоритму SHA-1;
6) Хеш, рассчитанный по алгоритму MD5;
7) Хеш, рассчитанный по алгоритму TLSH;
8) Хеш, рассчитанный по алгоритму Imphash;
9) Хеш, рассчитанный по алгоритму SSDEEP;
10) Обнаруженные имена.

Для значений хеш-сумм и обнаруженных имен доступна функция копирования в буфер обмена. Чтобы скопировать нужные значения в буфер обмена, необходимо нажать кнопку **Скопировать в буфер обмена**  в строке с выбранным значением хеш-суммы или обнаруженными именами.

Справа от таблицы с данными находится кнопка 

. Любой элемент или блок элементов в формате JSON можно скопировать, нажав кнопку  . Для возврата к результатам отчета в формате HTML необходимо нажать ЛКМ на значок 

.

10.3.2. Принципы работы TI-платформы в RT Protect EDR

TI-платформа осуществляет анализ хешей файлов, глобальных IP-адресов и доменных имен параллельно с остальными проверками, предусмотренными аналитическим инструментарием EDR.

Принцип работы с индикаторами компрометации в RT Protect EDR в интеграции с RT Protect TI выглядит следующим образом:

1) При обнаружении очередного артефакта агентом (попытка запуска процесса, установления сетевого соединения и т.д.) производится его анализ по наборам индикаторов компрометации на самом агенте;

2) Если артефакт присутствует в наборе, соответствующее действие блокируется в синхронном режиме (например, не допускается запуск процесса);

3) В ином случае информация об артефакте вместе с событием отправляется на сервер EDR;

4) Далее в рамках интеграции осуществляется обращение к TI-платформе для получения вердикта по артефакту, в случае получения заключения "Вредоносный", агенту направляется команда, например, на завершение процесса.

В любом из описанных случаев в EDR генерируется инцидент.

Наборы индикаторов компрометации для агентов могут формироваться как вручную на сервере EDR, так и получаться с TI-плаформы, на которой, в свою очередь, формироваться динамически (галочка "теневой набор" в соответствующем разделе аналитики EDR в веб-интерфейсе TI-платформы). Это позволяет хранить на агентах ограниченный, но актуальный набор индикаторов компрометации для синхронного реагирования на угрозы.

Также важно, что интеграции (например, VirusTotal) запускаются только при анализе соответствующих событий в веб-интерфейсе TI-платформы (переход на страницу отчета об артефакте). Таким образом, это

позволяет использовать ограниченные квоты только для исследуемых артефактов, а для анализа всех артефактов на потоке использовать базу данных, формируемую на основе подключенных фидов.

В рамках интеграции TI-платформы с решениями класса Sandbox возможна отправка потенциально вредоносных файлов с агента в TI-платформу и далее в песочницу (также данный функционал доступен из веб-интерфейса TI-платформы). Это осуществляется путём использования команды "GET" в консоли агента с параметром "/ti".

Если TI выносится вердикт о том, что в системе обнаружены вредоносный домен, IP-адрес или хеш исполняемого файла, автоматически выполняются следующие операции:

1) В Программе регистрируется инцидент;
2) Процесс вредоносного файла автоматически завершается;
3) Обращение к вредоносному домену или IP-адресу автоматически блокируется.

Примечание

На TI-платформе проверяются глобальные адреса и домены, проверка локальных адресов и доменов не предусмотрена.

При обнаружении подозрительного артефакта выполняется только детектирование события, при этом создается инцидент.

В некоторых случаях вердикт TI-платформы, присвоенный артефакту при первоначальном к нему обращении, может отличаться от назначенного впоследствии. В этой ситуации события с такими артефактами в разделе **Активность** помечаются значком .

Важной функцией TI-платформы является централизованное хранение и распространение до отдельных серверов EDR аналитических наборов и наборов с исключениями. К аналитическим относятся индикаторы атак, индикаторы компрометации, YARA-правила и журналы Windows, к наборам с исключениями относятся исключения для программ, исключения для файлов, сетевые исключения и исключения индикаторов атак.

Для применения на агентах наборы с правилами должны быть назначены в соответствующих конфигурациях. Эта операция выполняется на страницах **Агенты** (для назначения на большое количество

агентов или агентов, сгруппированных по определенным признакам) или **Агент**. После назначения и применения наборов правила, содержащиеся в них, будут работать на выбранных агентах.

Изменения наборов и сохранение новой конфигурации на TI-платформе для таких наборов приведет к автоматическому сохранению и применению новой конфигурации на агентах.

Аналитик не может изменять TI-наборы, но при этом может просматривать содержимое наборов, а также копировать и перемещать данные из наборов.

10.4 Просмотр списка пользователей на странице «Администрирование»

В разделе **Администрирование** аналитик может просмотреть подробную информацию о заблокированных и действующих пользователях.

Пользователи с ролью **Аналитик** могут просматривать информацию об учетных записях, зарегистрированных в Программе, но при этом не обладают возможностями редактирования или блокирования профилей, сброса пароля и другими возможностями, которые есть у пользователей с ролью **Администратор**.

Таблица с информацией о пользователях, представленная на странице **Администрирование**, включает в себя следующие поля:

1) **Имя пользователя**;

2) **Последнее время входа**;

3) **Имя**;

4) **Фамилия**;

5) **Email**;

6) **Роль**;

7) **Статус** (кнопка **Заблокировать**/**Разблокировать пользователя** показывает, какой статус пользователя в данный момент).

С помощью представленных на странице фильтров аналитик может фильтровать информацию о пользователях по следующим параметрам:

— количество записей на странице;

— имя пользователя (логин);

— имя (имя пользователя, указанное при регистрации);

– фамилия;

– email;

– роль пользователя.

Если требуется очистить страницу от значений, примененных в фильтрах, аналитик может воспользоваться кнопкой **Сбросить фильтры**.

10.5 Проверка распространенности программы в агентской сети

На странице **Процессы и модули** пользователь может просмотреть распространенность программы (модуля) в агентской сети, а также узнать вердикт TI-платформы по этой программе (рис. 35). Распространённость программы показывает, на каких агентах появлялся файл с определенной хеш-суммой.

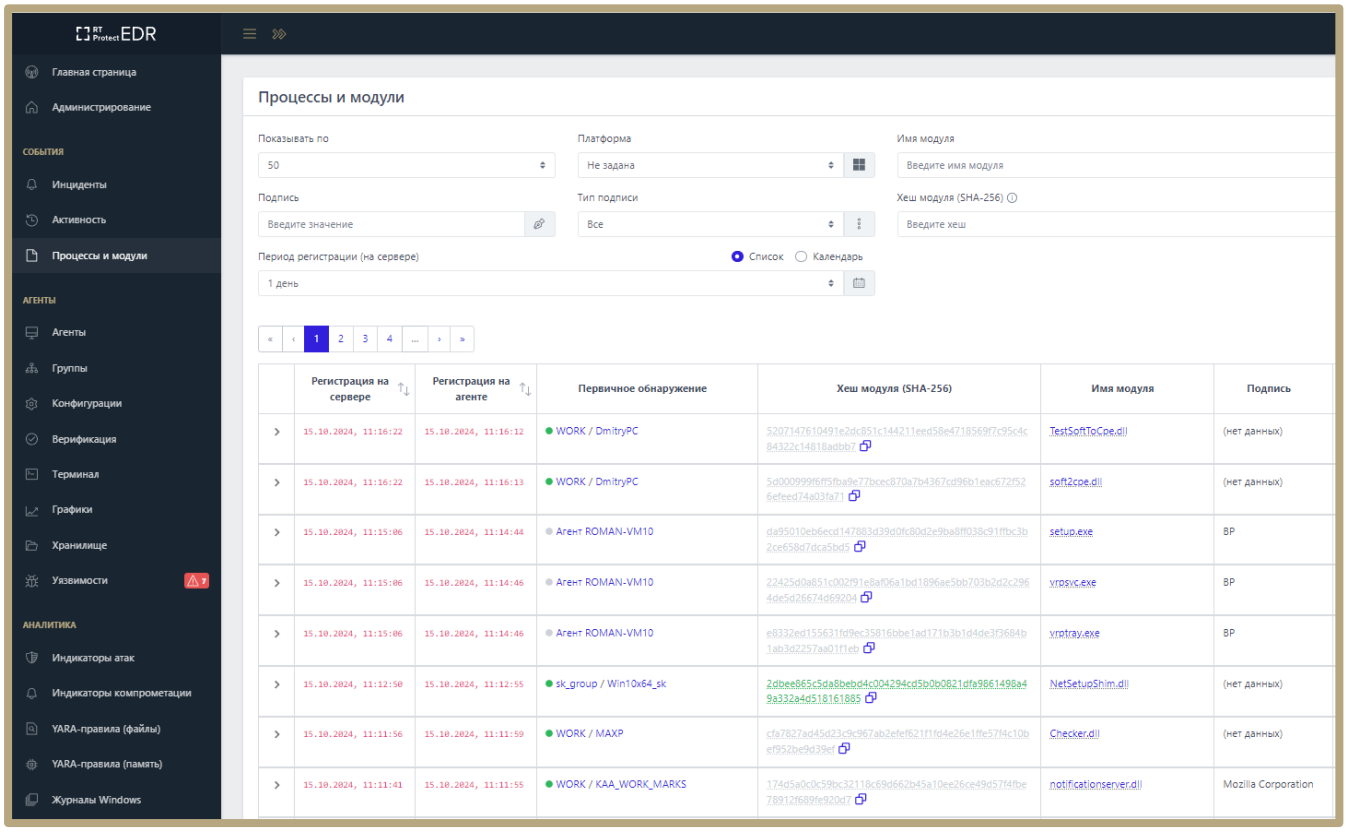


Рисунок 35 – Процессы и модули

Пользователь 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 или Linux);

5) Хеш модуля (SHA-256);

6) Период регистрации на сервере.

Важно

Поиск по фильтру **Хеш модуля (SHA-256)** производится только при вводе всей хеш-суммы, поэтому для фильтрации необходимо указывать хеш целиком.

Вердикт TI-платформы открывается, если пользователь нажмет поле с хеш-суммой исполняемого модуля. Первоначально открывается краткий отчет. Полный отчет доступен, если нажать кнопку **Перейти к отчету**. Пользователь может просмотреть дополнительную информацию из карточки события старта процесса или загрузки образа, 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).

Переход на страницу **Процессы и модули** может происходить с других страниц. Часто используемым на практике будет переход со страницы **Инцидент**, так как аналитику при обнаружении вредоносной программы требуется прежде всего выявить все конечные точки, на которые она уже установилась. Чтобы это сделать, аналитику необходимо найти в обнаружениях в карточке события кнопку рядом с хеш-суммой вредоносной программы.

Нажатие кнопки откроет страницу **Процессы и модули**, после чего в таблице в поле **Число агентов** следует нажать числовое значение, которое откроет новую вкладку **Агенты** с указанием конечных точек, на которых вредоносная программа установлена.

Изучение вредоноса можно продолжить, нажав числовое значение в поле **Совпадения по DSL**. Откроется страница **Активность** с предустановленным DSL-запросом, в котором будет указана хеш-сумма вредоноса. Информация, полученная по запросу, даст возможность узнать, как много эпизодов с обнаруженной программой происходило на зараженной конечной точке, как давно вредонос находится в зараженной системе.

Примечание

В некоторых случаях в процессе обнаружения всех конечных точек, на которых распространена программа, может возникнуть коллизия: на странице **Агенты** и на странице **Процессы и модули** отобразится разное количество конечных точек. Связано это с тем, что сервис **Процессы и модули** хранит все исторические данные о встреченных программах, а события на агентах хранятся в течение трех месяцев. В результате, при обнаружении модуля на агенте среди старых событий, которые уже удалены из EDR, такой агент отображаться в списке агентов с обнаруженной программой не будет.

10.6 Конфигурирование правил обнаружения

Для конфигурирования правил обнаружения и аналитику необходимо перейти в разделы панели управления, объединенные термином **Аналитика**. Здесь находятся следующие разделы:

1) **Индикаторы атак**;
2) **Индикаторы компрометации**;
3) **YARA-правила (файлы)**;
4) **YARA-правила (память)**;
5) **Журналы Windows**.

Разделы содержат наборы правил для обнаружения вредоносной активности в автоматическом режиме. В программе сохранены аналитические наборы, которые позволяют детектировать известные и неизвестные угрозы. Сервер EDR также получает аналитические наборы от TI-платформы (TI-данные).

В добавление к предустановленной экспертизе или экспертизе, получаемой от сервера с TI-информацией, аналитик может создавать и редактировать собственные наборы правил, чтобы эффективнее обнаруживать вредоносную или аномальную активность в рамках определенной, хорошо ему известной инфраструктуры.

В программе предусмотрено создание множественных наборов, то есть аналитик может назначить агенту произвольное количество аналитических наборов. То же самое касается и наборов с исключениями.

Примечание

Наборы аналитических правил и исключений, получаемые Программой от TI-платформы (внешние наборы), помечаются значком TI, если наборы синхронизируются, и значком TI, если синхронизации нет. Аналитик может удалять несинхронизируемые наборы. При этом синхронизируемые наборы удалять и изменять аналитик не может. Если синхронизация внешнего набора завершилась с ошибкой, то такой набор помечается значком TI.

К инструментам анализа событий относятся:

1) Индикаторы атак (ИА);
2) Индикаторы компрометации (ИК);
3) YARA-правила (для файлов и памяти процесса);
4) Журналы Windows.

Перечисленные компоненты передаются агенту в виде отдельных конфигурационных файлов и работают в режиме реального времени, при этом индикаторы компрометации и YARA-правила отвечают за статический анализ исполняемых файлов, а индикаторы атак за динамический анализ, то есть анализ во время выполнения программ.

Аналитика подразумевает назначение двух типов действий (в текущей реализации, в будущем этот список будет увеличиваться):

1) Блокировать;
2) Детектировать.

В случае с журналами Windows при обнаружении будет выполняться только детектирующее действие, а для YARA-правил только блокирующее.

По умолчанию файловая аналитика (подсчет хешей, матчинг индикаторов и др.) производится только для исполняемых файлов и только при их запуске или загрузке, если исполняемый файл – это динамически загружаемая библиотека. Опция профиля безопасности агента **Расширения файлов с потенциально активным содержимым** позволяет дополнительно указать расширения файлов (помимо исполняемых), для которых также требуется включить файловый анализ, который будет производиться в режиме реального времени при доступе к этим файлам.

В некоторых случаях при блокировании файлов может возникнуть коллизия, когда файл будет фактически заблокирован, но при этом открываться на машине с агентом. Происходит это вследствие того, что некоторые процессы могут кешировать файлы, предоставляя к этим файлам доступ после создания блокирующей аналитики, когда операция **чтение файла** становится недоступна.

В качестве примера приведем такой случай. Во время открытия произвольного pdf-файла программа-просмотрщик Windows glcnd.exe выполняет его чтение, после чего файл кешируется этим же процессом. Далее аналитик создает индикатор компрометации, блокирующий доступ к упоминаемому выше файлу. Вследствие того, что файл закеширован процессом glcnd.exe, он открывается, так как фактически чтения файла в таком случае не выполняется, при этом в списке инцидентов у нас появится инцидент о срабатывании индикатора компрометации. После завершения процесса glcnd.exe рассматриваемая коллизия исчезнет.

10.6.1. Индикаторы атак

Индикаторы атак в общем смысле – это правила, позволяющие идентифицировать характерные потенциально опасные с точки зрения ИБ поведенческие паттерны программ, работающих на компьютерах защищаемого контура. В отличие от индикаторов компрометации, которые являются артефактами уже свершившейся кибератаки на ИС, индикаторы атак характеризуют определенную стадию прогрессирующей в данный конкретный момент кибератаки. Это принципиальное отличие позволяет детектировать и реагировать на кибератаку (в том числе автоматически) непосредственно в момент ее развития, в том числе на самом раннем этапе.

Для иллюстрации сказанного можно провести аналогию с банком и грабителем. Индикаторы компрометации в таком случае – это улики, оставленные грабителем после совершения им преступления. А индикаторы атак – это характерные признаки грабителя, который охрана банка распознает через систему видеонаблюдения, когда грабитель только приближается к банку или входит в него.

В EDR-решениях индикаторы атак реализуются за счет алгоритмов, выявляющих в потоке событий от программ, работающих на защищаемых компьютерах, определенные события или их цепочки, и выделяющих их в форму обнаружений (detections) или предупреждений (alerts), назначая им уровень угрозы, реакцию и др. атрибуты, характеризующие потенциальную атаку. Например, «процесс word.exe порождает дочерний процесс powershell.exe», или «процесс svchost.exe устанавливает сетевое соединение с хостом malwarehost.com» и т.п. Для каждого из приведенных примеров можно назначить уровень угрозы, а также предписать схему реагирования, например, запретить указанное действие. Также можно связать с правилом идентификаторы техники и тактики из широко известного классификатора угроз MITRE ATT&CK. Можно добавить тэги и/или связать правило с той или иной APT-группировкой.

Процесс поиска в потоке событий определенной последовательности событий, удовлетворяющих некоторому условию, называется корреляцией событий или матчингом над потоком событий. Этот процесс может происходить в режиме реального времени (на стороне агента EDR, в рамках его потока событий) или в оффлайн-режиме на стороне сервера EDR. Первый вариант позволяет выполнить противодействие (если требуется) в режиме реального времени, не давая атаке шанса развиться, однако ограничен рамками событий только одного агента. Второй вариант не позволяет выполнить противодействие в режиме реального времени, т.к. требуется какое-то время, чтобы события, возникающие на агенте, были доставлены до сервера и обработаны им, перед тем как сервер сможет выполнить корреляцию. При этом возможно произвести корреляцию среди нескольких агентов и источников событий (как, например, в SIEM-системах). Автоматизированное реагирование в таком случае заключается в отправке команды по нейтрализации атаки от сервера к агенту. Весь процесс при этом, как правило, стремится выполниться за некоторое нормативное (но не гарантированное) сравнительно короткое время, чтобы прогресс атаки с момента ее обнаружения был минимальным.

ИА в системе RT Protect EDR представляют собой правила корреляции событий **на стороне агента в режиме реального времени**. При описании семантики ИА ниже будут использоваться термины модели данных событий RT Protect EDR (см. пункт **Поля модели данных**

ИА имеют следующие атрибуты (поля):

1. **Имя**. Кратко описывает суть выявляемой индикатором активности или угрозы (например, SuspiciousOfficeChildProcess и т.п.). Имя является уникальным и используется для идентификации ИА в разных ситуациях. Если ИА соответствует известному sigma-правилу, то «хорошим тоном» будет использование имени этого sigma-правила в качестве имени индикатора (например, proc_creation_win_powershell_download_patterns).

Примечание

При срабатывании индикатора его имя будет указано в поле **rul** сгенерированного события-обнаружения и может использоваться при написании программного исключения для борьбы с ложноположительными срабатываниями ИА в ситуации, когда непосредственно уточнить логику (условие срабатывания) индикатора не представляется возможным.

2. Тип. Тип ИА однозначно идентифицирует тип события, возникновение которого на агенте всякий раз будет являться поводом к матчингу индикатора. Например, если ИА имеет тип «Старт процесса», то каждый раз при запуске процесса агент будет анализировать это событие на предмет соответствия одному или нескольким ИА этого типа, назначенных ему. При срабатывании ИА в поток событий наряду с исходным событием будет вставлено соответствующее ему событие-обнаружение, в поле **Правило** (rul) которого будет указано имя индикатора, а в полях **Критичность** (svrt), **Действие** (act) и **MITRE** (mitre) будут перенесены значения соответствующих полей индикатора (см. ниже). Полный перечень доступных типов ИА в системе RT Protect EDR представлен в пункте **Типы индикаторов атак**

3. **Условие**. Условие является логическим выражением в терминах схемы событий RT Protect EDR и определяет условие срабатывания ИА при возникновении на агенте события заданного типа. Синтаксис и семантика условных выражений описывается в пункте **Синтаксис и семантика условных выражений индикаторов атак**.

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

5. **Действие**. Действие определяет автоматизированную реакцию на возникшее событие в случае срабатывания для него ИА. В качестве действия предусматривается возможность блокирования соответствующей исходной активности, приведшей к срабатыванию индикатора. Альтернативой является генерация события-обнаружения без реагирования (т.е. только детектирование).

6. **Режим**. Режим работы ИА определяет механику генерации события-обнаружения при срабатывании индикатора. Предусматриваются следующие режимы:

— обычный;

— без генерации события-обнаружения;

— с однократной генерацией события-обнаружения (в этом режиме для каждого процесса (приложения), в контексте которого сработал ИА, событие-обнаружение генерируется только один раз).

Для всех режимов реакция, если она предписана, выполняется всякий раз при срабатывании ИА.

7. **Классификатор MITRE ATT&CK**. Ссылка на классификатор угроз MITRE ATT&CK позволяет связать ИА с известной вредоносной техникой и тактикой, что впоследствии при срабатывании ИА из-за выявленной атаки на ИС позволяет аналитику наглядно видеть задействованные атакующими техники/тактики и получить по ним сводную справочную информацию из классификатора.

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

9. **Комментарий**. Развернутое описание активности, выявляемой ИА.

Если для некоторого исходного события срабатывает больше одного ИА, то результирующее действие (реакция) в отношении данного события определяется как «блокировать», если хотя бы один из сработавших ИА предписывает соответствующую реакцию.

Важно

В режиме работы агента «только детектирование» для всех ИА, назначенных ему, игнорируется предписываемое ИА блокирующее действие.

Типы индикаторов атак

В Программе представлено 29 типов ИА, а именно:

1) Установка исходящего сетевого соединения (CONNECT);
2) Прием входящего сетевого соединения (ACCEPT);
3) Инициирование защищенного SSL-соединения (сообщение SSL HELLO);
4) Открытие локального порта на прием входящих соединений (LISTEN);
5) Получение ответа сервиса DNS (DNS RESPONSE);
6) Создание нового файла (CREATE NEW);
7) Переименование файла (RENAME);
8) Удаление файла (DELETE);
9) Прямой доступ к диску (тому) на чтение (DISK READ);
10) Прямой доступ к диску (тому) на запись (DISK WRITE);
11) Создание именованного канала (CREATE NAMED PIPE);
12) Подключение к именованному каналу (CONNECT NAMED PIPE);
13) Доступ к файлу (ACCESS);
14) Создание альтернативного потока для файла (CREATE ALTERNATE DATA STREAM)
15) Создание ключа реестра (CREATE KEY);
16) Удаление ключа реестра (DELETE KEY);
17) Изменение значения реестра (SET VALUE);
18) Удалено значение ключа (DELETE VALUE);
19) Переименование ключа реестра (RENAME KEY);
20) Событие журнала системы (EVENT LOG) (на данный момент индикатор атак не поддерживается);
21) Загрузка драйвера (LOAD DRIVER);
22) Создание процесса (CREATE PROCESS);
23) Завершение процесса (STOP PROCESS);
24) Загрузка образа (LOAD IMAGE);
25) Доступ к стороннему процессу (OPEN PROCESS);
26) Создание нити (потока) в стороннем процессе (CREATE REMOTE THREAD);

27) Доступ к нити стороннего процесса (OPEN THREAD);

28) Загрузка образа в сторонний процесс (LOAD REMOTE IMAGE);

29) Загрузка сборки .NET (LOAD ASSEMBLY).

Важно

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

Создание индикаторов атак **Событие журнала** и **Загрузка .NET-сборки** в данный момент не поддерживается.

Синтаксис и семантика условных выражений индикаторов атак

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

Типы операндов

Операндами условных выражений ИА в Программе являются значения полей событий, адресуемые в выражении по именам полей, согласно модели данных событий.

Важно

Для каждого типа ИА при написании его условного выражения доступны только поля соответствующего ему типа события, а также дополнительно поля общей части событий.

В условных выражениях ИА (как и в модели данных событий) операнды могут иметь следующие типы:

– bool (true/false);

– uint (целочисленный беззнаковый разрядностью 64 бита);

– string (строковый);

– exclusion_flags (одноименная структура битовых флагов);

– runtime_flags0 (одноименная структура битовых флагов);

– runtime_flags1 (одноименная структура битовых флагов);

– load_image_flags (одноименная структура битовых флагов);

– create_remote_thread_flags (одноименная структура битовых флагов);

– time (время, временной штамп).

Примечание

Расшифровка и список доступных в Программе флагов приведены в разделе 9.11.

Состав операторов

Набор операторов, доступных в условных выражениях ИА RT Protect EDR достаточно типичен и включает в себя логические, арифметические, строковые, битовые и специальные операторы, а также операторы сравнения.

Логические операторы

! (not) – логическое отрицание (логическое «НЕ»);

&& (and) – конъюнкция (логическое «И»);

|| (or) – дизъюнкция (логическое «ИЛИ»).

Операторы сравнения

== (bool, число, строка);

!= (bool, число, строка);

> (число);

< (число);

>= (число);

<= (число);

iequals (строка) – сравнение без учета регистра.

Строковые операторы

matches – соответствие строки паттерну с учетом регистра, определяемому регулярным выражением с использованием символов * и ?;

startswith – проверка префикса строки с учетом регистра;

istartswith – проверка префикса строки без учета регистра;

endswith – проверка суффикса строки с учетом регистра;

iendswith – проверка суффикса строки без учета регистра;

contains – проверка вхождения подстроки с учетом регистра;

icontains – проверка вхождения подстроки без учета регистра.

Арифметические операторы

+ (в т.ч. унарный) – сложение или унарный «минус»;

- (в т.ч. унарный) – вычитание или унарный «плюс»;

* – умножение;

/ – деление;

% – остаток от деления;

<< – логический сдвиг влево;

>> – логический сдвиг вправо.

Битовые операторы

^ – побитовое исключающее «ИЛИ»;

& – побитовое «И»;

| – побитовое «ИЛИ»;

~ – побитовое «НЕ».

Специальные операторы

. (оператор разыменования);

(– открывающая скобка;

) – закрывающая скобка.

Для доступа к отдельным флагам структур типа exclusion_flags, runtime_flags0, runtime_flags1, load_image_flags и create_remote_thread_flags предназначен оператор разыменования. Для получения целочисленного значения структуры с флагами используется конструкция .value.

Примечание

Оператор разыменования позволяет обращаться к отдельным полям значений временных типов, а именно: Year, Month, DayOfWeek, Day, Hour, Minute, Second, Milliseconds, например: time.Year == 2022 && time.Month == 12.

Также оператор разыменования может использоваться применительно к строковым типам в следующих случаях:

– для перевода строки в нижний регистр (.lower) (пример: cmdl.lower matches "*something*");

– получения имени файла (.name) или пути (.path), если строка ссылается на полный путь с именем файла (пример: app.name iequals "myapp.exe" или app.path iendswith "\\windows\\system32\\");

– получения длины строки (.length) (пример: cmdl.length > 32).

Поля модели данных

Модель данных sysmon частично поддерживается в форме набора синонимов над мнемониками нативной модели RT Protect EDR. В событиях активности, получаемых от агентов, поля модели данных sysmon отсутствуют – они существуют только виртуально в условных выражениях ИА.

Полный перечень синонимов sysmon, а также их соответствие типам ИА и полям нативной модели данных событий описаны в таблице 54.

Таблица 54 – Модель данных sysmon

Имя	Тип поля	Тип ИА	Нативное имя
UtcTime	time	любой	time
ProcessId, SourceProcessId	uint	любой	pid
ParentProcessId	uint	любой	ppid
Image, SourceImage	string	любой	app

Имя	Тип поля	Тип ИА	Нативное имя
TerminalSessionId	uint	любой	sess
User	string	любой	sid
CommandLine	string	любой	cmdl
CallTrace	string	любой	trace
SourceThreadId	uint	любой	whotid
Protocol	uint	CONNECT ACCEPT LISTEN SSL HELLO DNS RESPONSE	proto
QueryName	string	DNS RESPONSE	dnsq_h
QueryStatus	uint	DNS RESPONSE	dnsq_s
QueryResults	string	DNS RESPONSE	dnsq_r
SourceIsIpv6, DestinationIsIpv6	bool	CONNECT ACCEPT	ipv6
SourceHostname	string	ACCEPT	*
DestinationHostName	string	CONNECT	*
SourceIp	string	CONNECT ACCEPT	*
SourcePort	uint	CONNECT ACCEPT	*
DestinationIp	string	CONNECT ACCEPT	*
DestinationPort	uint	CONNECT ACCEPT	*
Initiated	bool	CONNECT ACCEPT	*
ParentCommandLine	string	CREATE PROCESS	cmdlp
CurrentDirectory	string	CREATE PROCESS	wdir
ParentImage	string	CREATE PROCESS	cpath
FileVersion	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	fver
Description	string	CREATE PROCESS LOAD IMAGE LOAD DRIVER LOAD REMOTE IMAGE LOAD ASSEMBLY	fdecs

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

Имя	Тип поля	Тип ИА	Нативное имя
NewThreadId	uint	CREATE REMOTE THREAD OPEN THREAD	tid
StartAddress	uint	CREATE REMOTE THREAD	taddr
GrantedAccess	uint	OPEN PROCESS OPEN THREAD	grnt
TargetFilename, Device	string	CREATE NEW RENAME DELETE ACCESS	name
Archived	bool	DELETE RENAME	save
TargetObject	string	SET VALUE RENAME KEY DELETE KEY CREATE KEY	*
Details	string	SET VALUE	*
NewName	string	RENAME KEY	new

* поля являются виртуальными (соответствующие поля нативной модели данных событий отсутствуют).

Поле **Image** не совсем в точности соответствует полю **app**, так как в первом случае запись значения поля начинается с буквы диска, например C:*, а во втором случае значение начинается с Device\HarddiskVolume* с указанием номера диска, поэтому, если требуется указать именно букву диска, следует употреблять поле **Image**.

Нативные поля Программы для написания индикаторов атак описаны в таблице 55.

Таблица 55 – Поля для написания индикаторов атак

Наименование поля	Расшифровка	Тип ИА
act	Действие, связанное с событием	любой
time	Время регистрации события	любой
pid	Идентификатор процесса на агентской системе	любой
ppid	Идентификатор родительского процесса на агентской системе	любой
app	Полное имя исполняемого файла процесса	любой
cmdl	Командная строка процесса	любой
sess	Номер сессии, в которой работает процесс на агентской системе	любой
rf0	Поведенческие признаки процесса (первая группа)	любой

Наименование поля	Расшифровка	Тип ИА
rf1	Поведенческие признаки процесса (вторая группа)	любой
exclf	Флаги исполняемого файла процесса	любой
sid	SID пользователя, создавшего процесс	любой
app_sgnr	Издатель ЭП исполняемого файла процесса	любой
agent_build_number	Номер сборки агента	любой
history	История сработавших индикаторов атак	любой
proto	Протокол	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
ipv6	Признак работы по IPv6	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
out	Отправка (1) или прием (0)	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
size	Размер полезных данных (payload) сетевого пакета	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
host	Имя хоста, соответствующее удаленному IP	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
ssl_h	Имя хоста (server_name) из сообщения SSL Client Hello	Сеть: SSL HELLO
dnsq_h	Имя хоста из DNS-запроса	Сеть: DNS-ответ
dnsq_t	Тип DNS-запроса	Сеть: DNS-ответ
dnsq_s	Статус DNS-запроса	Сеть: DNS-ответ
dnsq_r	Результат DNS-запроса	Сеть: DNS-ответ
r_p	Удаленный порт	Сеть: Исходящее подключение Сеть: Входящее подключение

Наименование поля	Расшифровка	Тип ИА
		Сеть: SSL HELLO Сеть: DNS-ответ
r_ip	Удаленный IP-адрес	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: SSL HELLO Сеть: DNS-ответ
l_p	Локальный порт	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
l_ip	Локальный IP-адрес	Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
who	Полное имя исполняемого модуля–инициатора операции	Файлы: Создан новый файл Файлы: Файл переименован Файлы: Удален файл Файлы: Прямой доступ к диску (тому) на чтение Файлы: Прямой доступ к диску (тому) на запись Файлы: Создан именованный канал Файлы: Подключение к именованному каналу Файлы: Доступ к файлу Файлы: Создан альтернативный поток для файла Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован Процессы: Загрузка драйвера Процессы: Старт процесса Процессы: Завершение процесса Процессы: Загрузка образа Процессы: Доступ к процессу Процессы: Создание нити в стороннем процессе Процессы: Доступ к нити процесса Процессы: Загрузка образа в сторонний процесс

Наименование поля	Расшифровка	Тип ИА
whof	Флаги исполняемого модуля–инициатора операции	Файлы: Создан новый файл Файлы: Файл переименован Файлы: Удален файл Файлы: Прямой доступ к диску (тому) на чтение Файлы: Прямой доступ к диску (тому) на запись Файлы: Создан именованный канал Файлы: Подключение к именованному каналу Файлы: Доступ к файлу Файлы: Создан альтернативный поток для файла Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован Процессы: Загрузка драйвера Процессы: Старт процесса Процессы: Завершение процесса Процессы: Загрузка образа Процессы: Доступ к процессу Процессы: Создание нити в стороннем процессе Процессы: Доступ к нити процесса Процессы: Загрузка образа в сторонний процесс Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
whotid	Идентификатор нити–инициатора операции	Файлы: Создан новый файл Файлы: Файл переименован Файлы: Удален файл Файлы: Прямой доступ к диску (тому) на чтение Файлы: Прямой доступ к диску (тому) на запись Файлы: Создан именованный канал Файлы: Подключение к именованному каналу Файлы: Доступ к файлу Файлы: Создан альтернативный поток для файла

Наименование поля	Расшифровка	Тип ИА
		Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован Процессы: Загрузка драйвера Процессы: Старт процесса Процессы: Завершение процесса Процессы: Загрузка образа Процессы: Доступ к процессу Процессы: Создание нити в стороннем процессе Процессы: Доступ к нити процесса Процессы: Загрузка образа в сторонний процесс Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
whoaddr	Стартовый адрес нити–инициатора операции	Файлы: Создан новый файл Файлы: Файл переименован Файлы: Удален файл Файлы: Прямой доступ к диску (тому) на чтение Файлы: Прямой доступ к диску (тому) на запись Файлы: Создан именованный канал Файлы: Подключение к именованному каналу Файлы: Доступ к файлу Файлы: Создан альтернативный поток для файла Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован Процессы: Загрузка драйвера Процессы: Старт процесса Процессы: Завершение процесса Процессы: Загрузка образа Процессы: Доступ к процессу Процессы: Создание нити в стороннем процессе

Наименование поля	Расшифровка	Тип ИА
		Процессы: Доступ к нити процесса Процессы: Загрузка образа в сторонний процесс Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
trace	Стек вызовов операции	Файлы: Создан новый файл Файлы: Файл переименован Файлы: Удален файл Файлы: Прямой доступ к диску (тому) на чтение Файлы: Прямой доступ к диску (тому) на запись Файлы: Создан именованный канал Файлы: Подключение к именованному каналу Файлы: Доступ к файлу Файлы: Создан альтернативный поток для файла Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован Процессы: Загрузка драйвера Процессы: Старт процесса Процессы: Завершение процесса Процессы: Загрузка образа Процессы: Доступ к процессу Процессы: Создание нити в стороннем процессе Процессы: Доступ к нити процесса Процессы: Загрузка образа в сторонний процесс Сеть: Исходящее подключение Сеть: Входящее подключение Сеть: Открытие локального порта на прием (LISTEN) Сеть: SSL HELLO Сеть: DNS-ответ
wdir	Рабочий каталог процесса	Процессы: Старт процесса
cmdlp	Командная строка родительского процесса	Процессы: Старт процесса

Наименование поля	Расшифровка	Тип ИА
cmdlg	Командная строка прародителя (grand parent)	Процессы: Старт процесса
when	Время создания процесса	Процессы: Старт процесса
cpath	Полное имя процесса-инициатора операции	Процессы: Старт процесса
prot	Уровень защиты процесса	Процессы: Старт процесса
base	Базовый адрес образа	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс
isize	Размер образа	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс
crtime	Время создания файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
chtime	Время последнего изменения файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
fsize	Размер файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
ftype	Тип файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
attr	Атрибуты файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу Файлы: Создан новый файл

Наименование поля	Расшифровка	Тип ИА
sha1	SHA-1 файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
md5	MD5 файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
sha256	SHA-256 файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
sgnr	Электронная подпись файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
sgnr_s	Статус электронной подписи файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
pack	Тип упаковщика файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
ofn	Оригинальное имя файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
fcomp	Компания-издатель файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа

Наименование поля	Расшифровка	Тип ИА
		Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
fver	Версия файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
fdesc	Описание файла	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
fprod	Продукт, к которому относится файл	Процессы: Старт процесса Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс Файлы: Доступ к файлу
path	Полное имя файла образа	Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс
imgf	Флаги образа	Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс
ldf	Флаги операции загрузки образа	Процессы: Загрузка драйвера Процессы: Загрузка образа Процессы: Загрузка образа в сторонний процесс
tpath	Полное имя целевого процесса	Процессы: Загрузка образа в сторонний процесс Процессы: Доступ к процессу Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе
tpid	Идентификатор целевого процесса	Процессы: Загрузка образа в сторонний процесс Процессы: Доступ к процессу Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе

Наименование поля	Расшифровка	Тип ИА
targf	Флаги образа целевого процесса	Процессы: Загрузка образа в сторонний процесс Процессы: Доступ к процессу Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе
trf0	Поведенческие признаки целевого процесса (первая группа)	Процессы: Загрузка образа в сторонний процесс Процессы: Доступ к процессу Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе
trf1	Поведенческие признаки целевого процесса (вторая группа)	Процессы: Загрузка образа в сторонний процесс Процессы: Доступ к процессу Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе
tid	Идентификатор целевой нити	Процессы: Доступ к нити процесса Процессы: Создание нити в стороннем процессе
taddr	Стартовый адрес целевой нити	Процессы: Создание нити в стороннем процессе
tf	Флаги нити	Процессы: Создание нити в стороннем процессе
dsrd	Запрашиваемые права	Процессы: Доступ к процессу Процессы: Доступ к нити процесса
grnt	Предоставленные права	Процессы: Доступ к процессу
asep	Ключ/значение относится к категории автозапуска	Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован
key	Путь ключа	Реестр: Создан новый ключ Реестр: Удален ключ Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа Реестр: Ключ переименован
val_n	Имя значения	Реестр: В значение ключа записаны данные Реестр: Удалено значение ключа
val_t	Тип данных значения	Реестр: В значение ключа записаны данные

Наименование поля	Расшифровка	Тип ИА
val_s	Размер данных значения	Реестр: В значение ключа записаны данные
val_d	Данные значения	Реестр: В значение ключа записаны данные
new	Новое имя ключа	Реестр: Ключ переименован
name	Полное имя файла	Файлы: Создан новый файл Файлы: Файл переименован Файлы: Удален файл Файлы: Прямой доступ к диску (тому) на чтение Файлы: Прямой доступ к диску (тому) на запись Файлы: Создан именованный канал Файлы: Подключение к именованному каналу Файлы: Доступ к файлу Файлы: Создан альтернативный поток для файла
fnew	Новое имя файла	Файлы: Файл переименован
delete	Доступ на удаление	Файлы: Доступ к файлу
read	Доступ на чтение	Файлы: Доступ к файлу
modify	Доступ на модификацию	Файлы: Доступ к файлу
save	Для файла была создана резервная копия	Файлы: Удален файл
ads	Операция совершается над альтернативным потоком данных файла	Файлы: Удален файл Файлы: Файл переименован Файлы: Создан новый файл Файлы: Доступ к файлу
arun	Файл расположен в директории автозапуска	Файлы: Файл переименован Файлы: Создан новый файл
owrt	Файл был заменен	Файлы: Файл переименован

Аналитик может создавать инидикаторы атак, используя только представленные в таблицах 54 и 55 поля, использование других полей из модели данных, которые обнаруживаются EDR и представлены в событиях активности, не приведет к срабатыванию индикатора атаки. При этом при создании такого индикатора Программа укажет на необходимость изменения условия, но даст возможность такой индикатор сохранить.

Совет

В рамках отдельного процесса в модели данных RT Protect EDR доступно создание последовательных цепочек индикации, когда один индикатор атаки ссылается на срабатывание другого индикатора, для этого в условии используется поле history и соответствующие операторы, ссылающиеся на название индикатора атаки, например, `history contains "RT_win_fake_lsass".`

Создание индикатора атак с помощью интерфейса модуля администрирования

В графическом интерфейсе RT Protect EDR правила индикации атак представлены в виде таблицы со сгруппированными наборами индикаторов.

Таблица наборов индикаторов имеет следующие столбцы (рис. 36):

1) **Название набора**;

2) **Количество записей** (правил в наборе);

3) **Привязано агентов** (количество агентов, которым назначен данный набор правил);

4) **Управление**, в поле содержатся следующие кнопки:

– кнопка редактирования названия набора ;

– кнопка удаления набора ;

– кнопка применения правил набора .

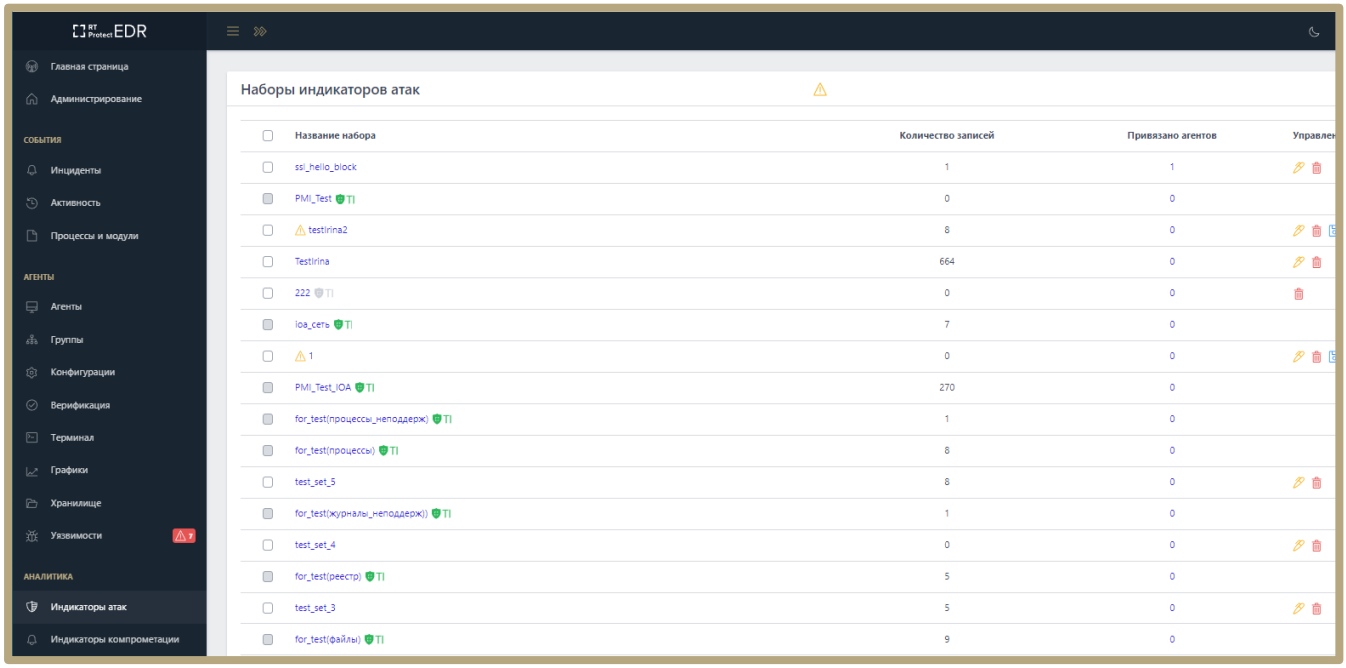


Рисунок 36 – Наборы индикаторов атак

На странице **Индикаторы атак** имеется возможность добавления/редактирования как самого набора, так и правил, входящих в набор, а также копирование индикатора из одного набора в другой. Правила в наборе представлены в виде таблицы со следующими столбцами (рис. 37):

1) Кнопка выбора (чекбокс);
2) Имя индикатора;
3) Тип индикатора (указывает на тип события);
4) Критичность/Действие, назначенные индикатору;
5) Идентификатор техники матрицы атак MITRE;
6) Дата создания/Автор индикатора;
7) Последнее изменение/Пользователь, внесший последнее изменение в индикатор;
8) Управление (содержит кнопки активации/деактивации индикатора / , а также кнопки **Редактировать** и **Удалить**).

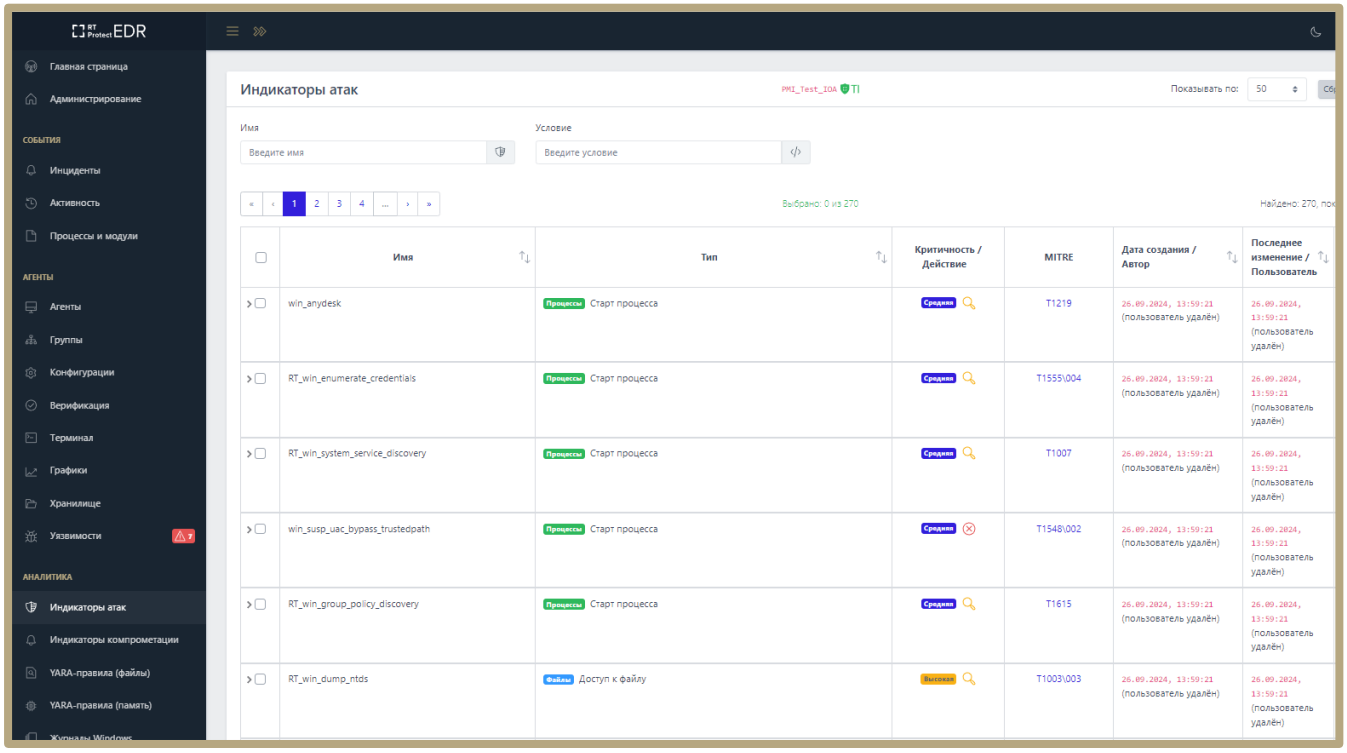


Рисунок 37 – Страница с правилами индикации атак, входящими в набор

Рядом с кнопкой выбора содержится значок раскрытия дополнительной информации об индикаторе , которая содержит следующие поля (рис. 38):

1) **Условие**;

2) **Описание**;

3) **Комментарий**.

Рисунок 38 – Дополнительная информация об индикаторе атак

Для добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы.

Добавить индикатор можно двумя способами (рисунок 39):

1) Создать новый индикатор;

2) Импортировать индикатор из sigma-правила.

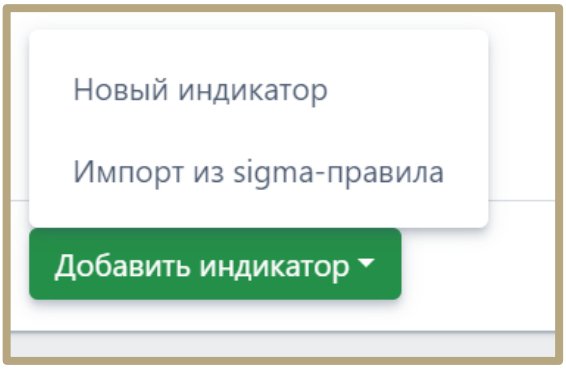


Рисунок 39 – Окно выбора способа добавления индикатора атаки

При выборе способа **Новый индикатор** откроется окно **Добавить индикатор.**

В открывшемся окне **Добавить индикатор** (рис. 40) следует прописать условия, на основании которых будет срабатывать правило.

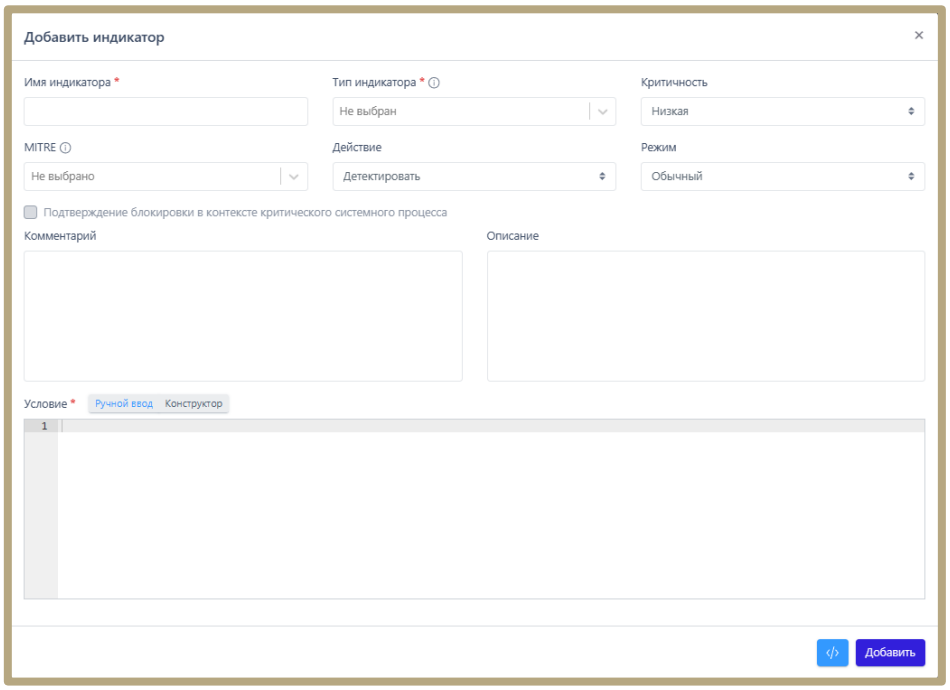


Рисунок 40 – Добавление индикатора

В окне **Добавить индикатор** имеются поля, отмеченные символом * . Этот символ означает, что при добавлении индикатора поля не могут быть пустыми. При попытке добавления индикатора с незаполненными полями индикатор не будет добавлен, а незаполненные поля будут выделены красной рамкой (рис. 41).

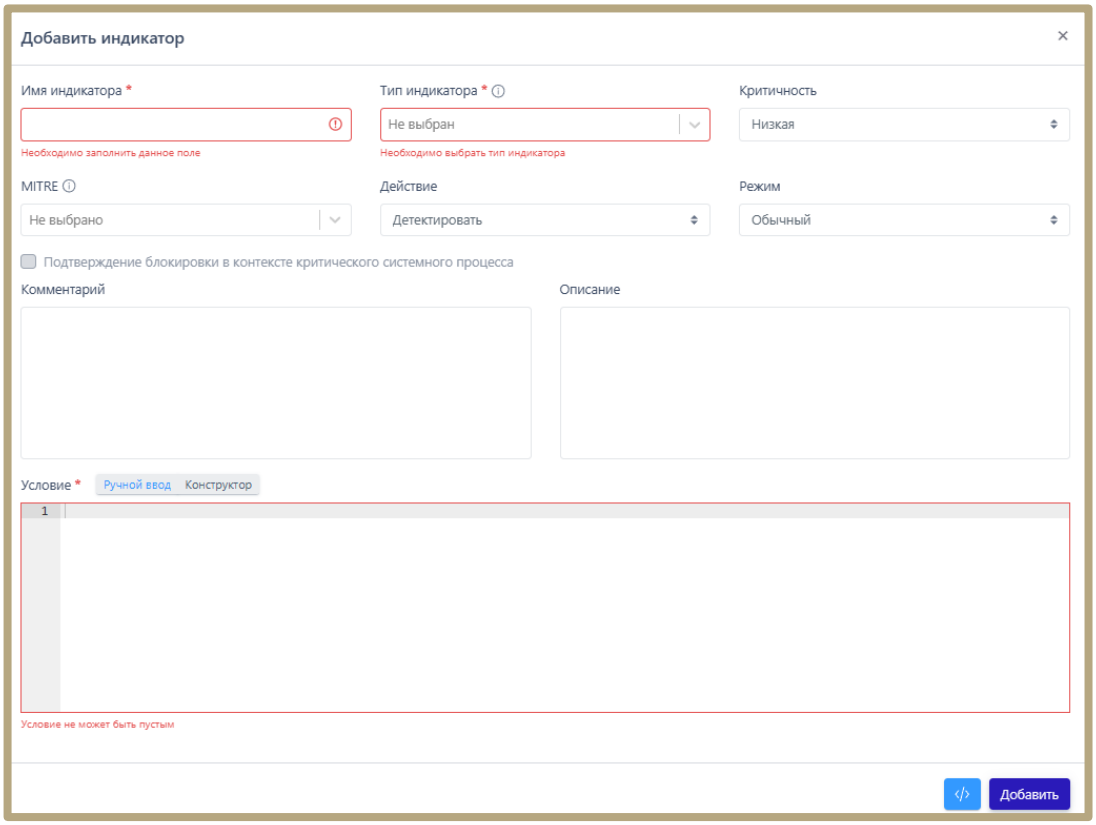


Рисунок 41 – Вид окна при добавлении индикатора с незаполненными полями

Важно

При создании индикатора атаки в ОС Windows для всех типов индикаторов, кроме типа **Старт процесса**, возможно написать такой индикатор, при срабатывании которого будет блокироваться критический системный процесс, что крайне опасно и может привести к блокировке всей работы и установке ОС в состояние «Синего экрана».

При установке галочки в поле **Подтверждение блокировки в контексте критического системного процесса** аналитик должен осознавать, что он соглашается с тем, что описанное выше состояние допустимо и может произойти на хосте, для которого будет применяться данный индикатор.

Для ОС Windows критическими системными считаются следующие процессы:

1) Процесс System (ядро ОС);

2) Процесс с ненулевым уровнем защиты (PPL, Windows 8.1+);

3) Trustlet-процесс Windows 10+ (https://learn.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes)

4) Процессы: csrss.exe, smss.exe, lsass.exe, services.exe, wininit.exe, winlogon.exe, logonui.exe, lsm.exe, sppsvc.exe (идентифицируются по полному пути);

5) Библиотека lsm.dll (идентифицируется по полному пути) внутри хост-процесса (svchost.exe).

Заполнение поля **Условие** можно выполнить двумя способами:

— ручной ввод условия;

— ввод условия с помощью конструктора.

Переключение между способами осуществляется с помощью кнопок **Ручной ввод** и **Конструктор** (Ручной ввод Конструктор). Выбранный способ написания условия подсвечивается синим цветом. Вид окна при написании условия в режиме **Ручной ввод** представлен на рисунке 42.

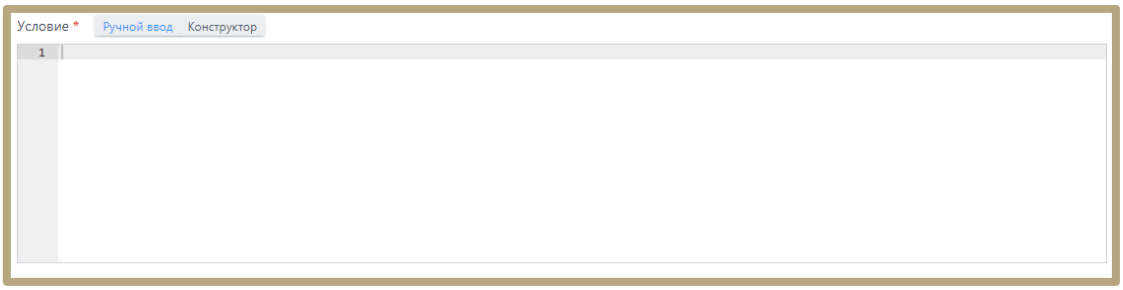


Рисунок 42 – Написание условия с помощью ручного ввода

Вид окна при написании условия с помощью инструмента **Конструктор** представлен на рисунке 43.

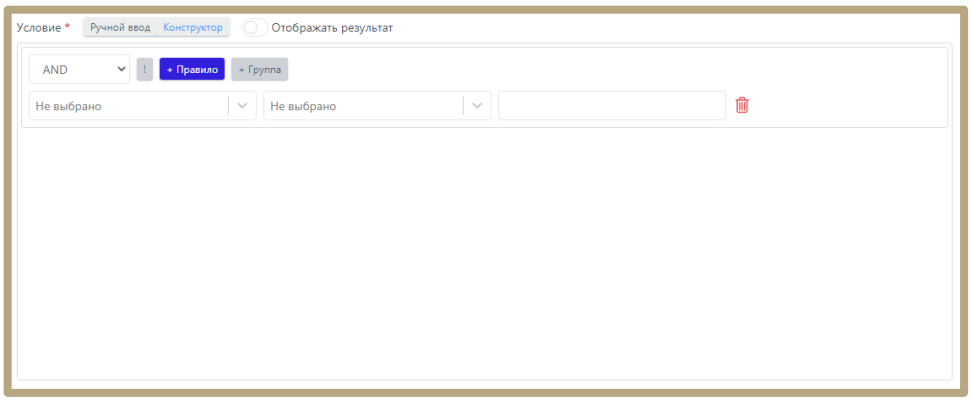
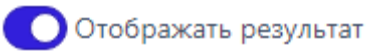


Рисунок 43 – Написание условия с помощью конструктора

Для удобства при написании условия можно использовать кнопку 

. При включении кнопки условие отображается в нижней части конструктора. Это позволяет аналитику детально рассмотреть приоритеты в условии, после чего скорректировать его, если это необходимо.

В конструкторе возможно создавать правила с использованием модели данных Sysmon. Поля событий модели данных Sysmon выбираются в окне, представленном на рисунке 44. Все возможные поля описаны в таблице 54.

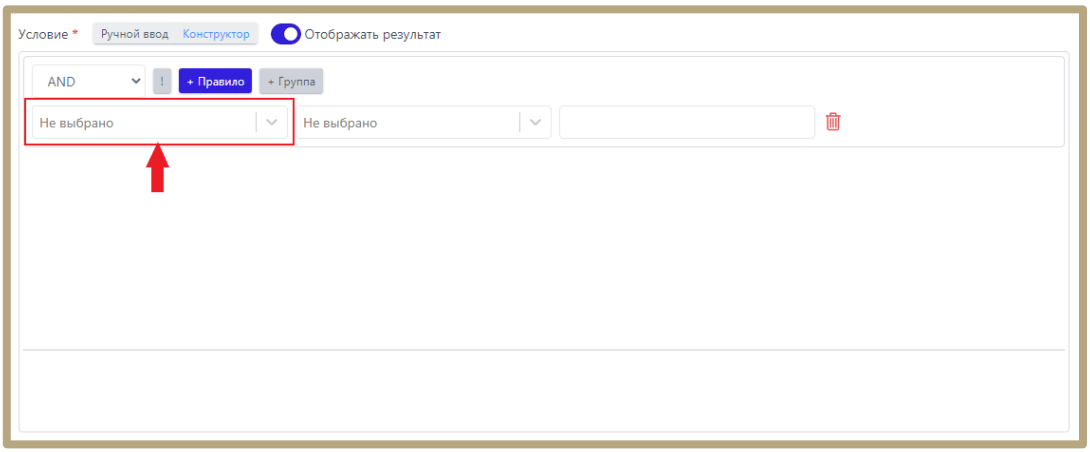


Рисунок 44 – Поле ввода модели данных событий

Операторы выбираются в окне, представленном на рисунке 45. Полный список операторов представлен в разделе **Состав операторов**

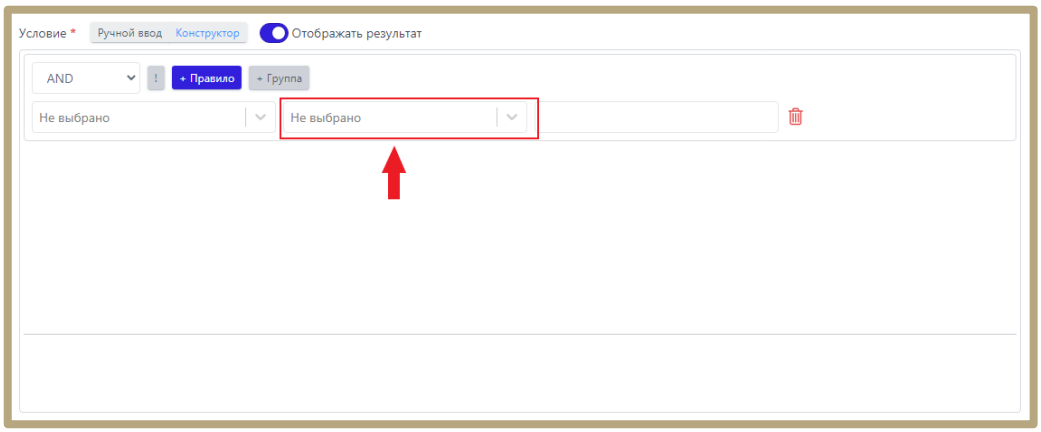


Рисунок 45 – Поле ввода операторов полей событий

Поле для ввода значений позволяет вводить произвольные значения для событий из схемы данных Sysmon. Поле представлено на рисунке 46.

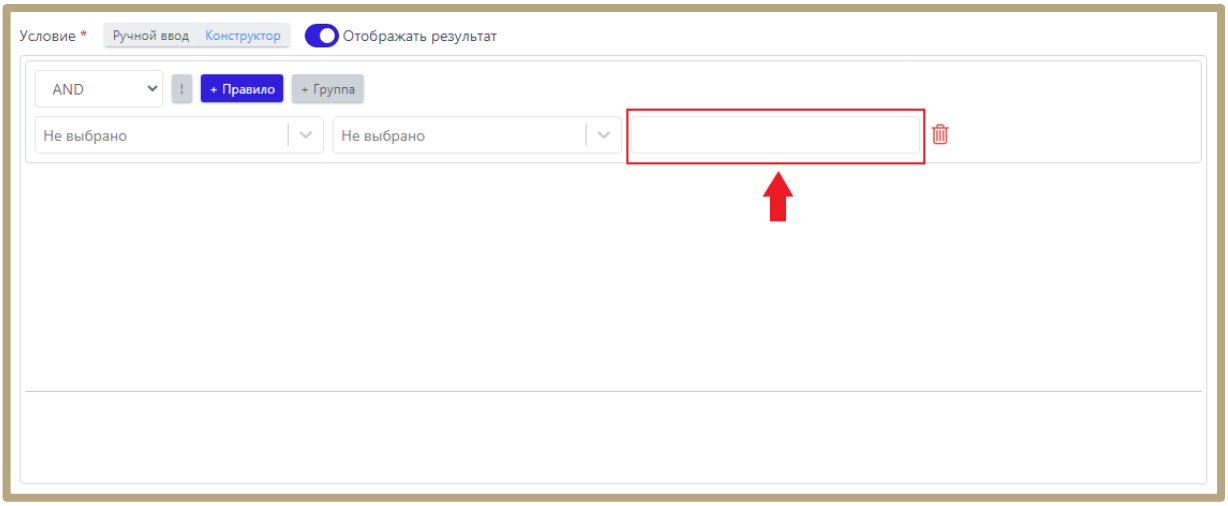


Рисунок 46 – Поле для ввода значений

Поле выбора значения логического оператора представлено на рисунке 47.

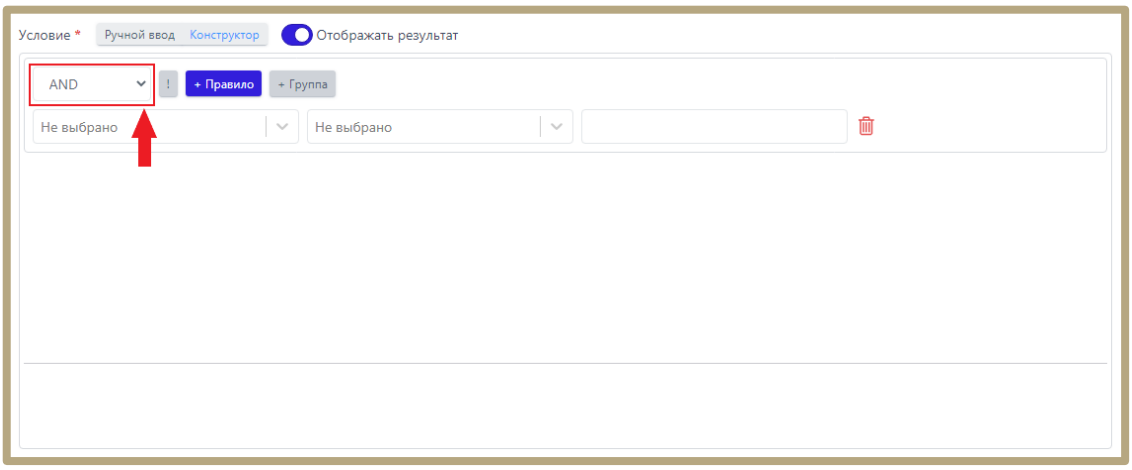


Рисунок 47 – Поле выбора значения логического оператора

В данном поле можно выбрать из двух значений AND (И), OR (ИЛИ).

+ Правило – кнопка для добавления строчки правила.

! – кнопка для добавления отрицания группы.

+ Группа – кнопка для добавления группы правил в условии.

Пример условия, написанного с помощью конструктора, представлен на рисунке 48.

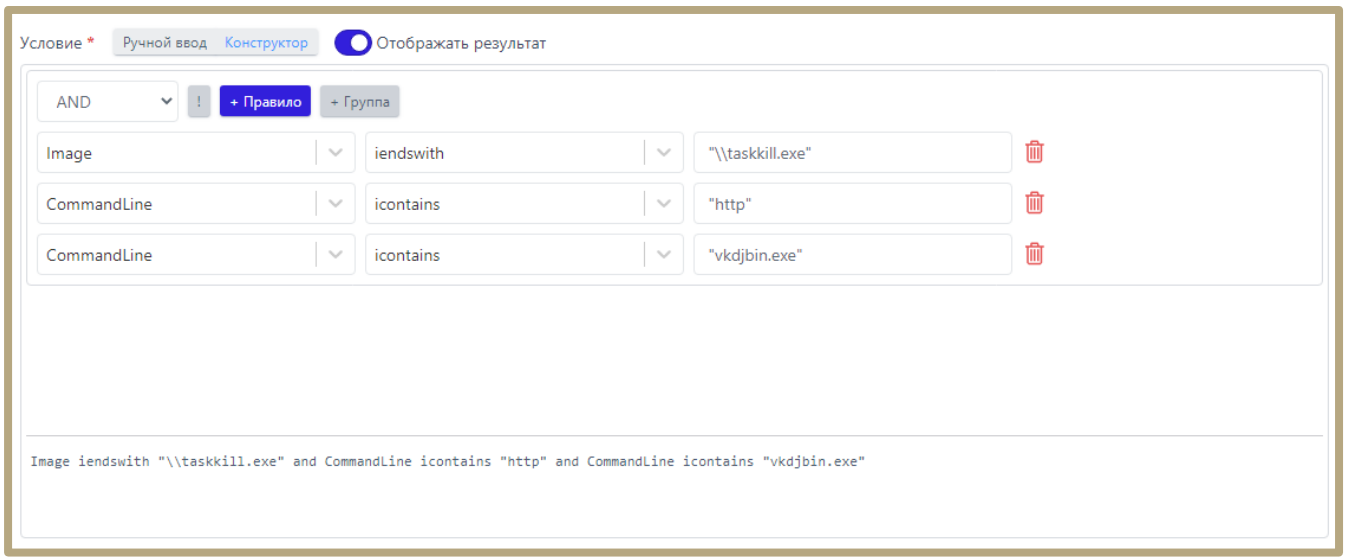


Рисунок 48 – Пример условия, написанного с помощью конструктора

При выборе способа добавления индикатора **Импорт из sigma-правила**, открывается окно, представленное на рисунке 49.

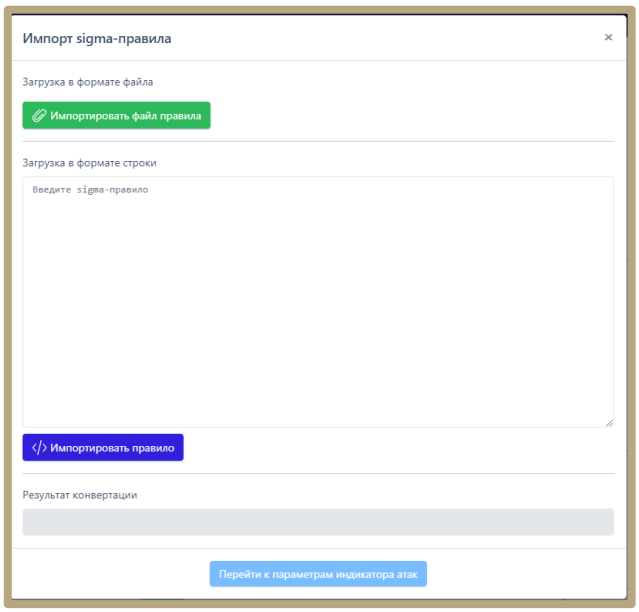


Рисунок 49 – Окно добавления индикатора с помощью импорта из sigma-правила

Sigma-правило, на основании которого будет создан индикатор атак, может быть добавлено в формате файла, либо в формате строки.

Для создания индикатора на основе Sigma-правила следует перейти на сайт https://github.com/SigmaHQ/sigma/blob/master/rules/windows и, выбрав одно из правил, нажать по иконке </> Импортировать правило (рисунок 50).

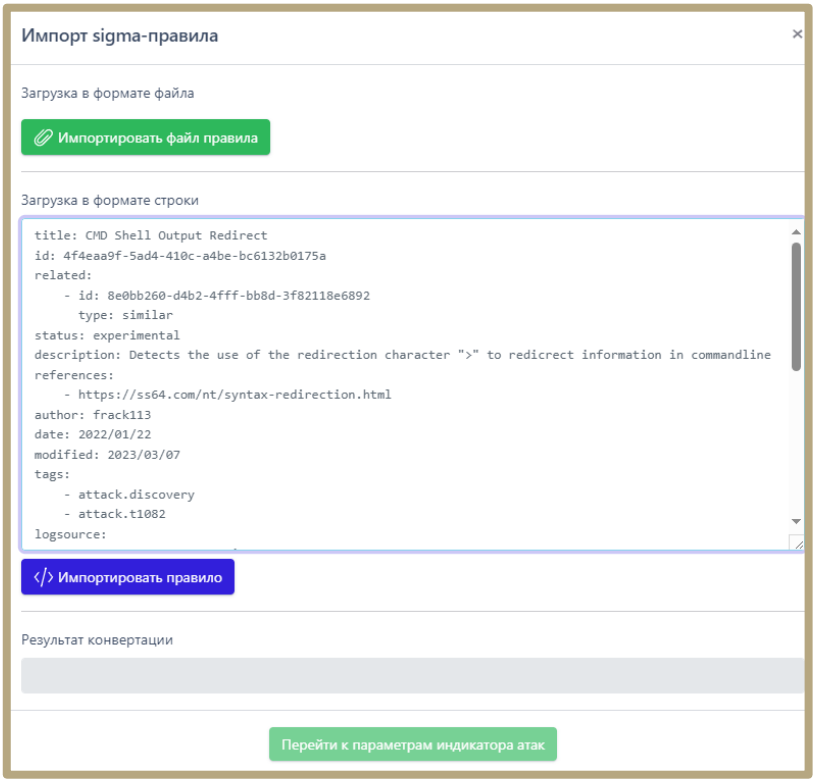


Рисунок 50 – Импорт Sigma-правила с помощью загрузки в формате строки для создания индикатора атаки

При удачной конвертации правила в поле **Результат конвертации** появится запись **Успешная конвертация**.

Далее для редактирования индикатора на основе sigma-правила следует нажать по иконке Перейти к параметрам индикатора атак.

Откроется окно **Добавить индикатор** с информацией из того sigma-правила, на основании которого создан индикатор.

Дальнейшие действия по редактированию и сохранению индикатора атак аналогичны действиям, описанным в этом разделе выше.

Кроме описанной выше процедуры можно воспользоваться импортом yml-файла с правилом, скачав его по ссылке с sigma-правилами и загрузив в формате файла с помощью кнопки Импортировать файл правила.

Проверка условия индикатора атаки

Условия индикатора проверяются с помощью утилиты **Проверка синтаксиса**. Область с информацией по проверке условия отображается в нижней части окна добавления или редактирования индикатора. Проверка условия запускается перед добавлением индикатора или после нажатия кнопки  . В случае написания некорректного условия индикатора атаки в области **Проверка синтаксиса** отобразится информация об ошибке. Если условие не содержит ошибок, то в строке **Проверка синтаксиса** отобразится запись **Корректно**.

Редактирование и удаление индикатора атаки

Для редактирования индикатора необходимо нажать кнопку **Редактировать** в строке выбранного индикатора атаки и в открывшемся окне **Редактировать индикатор** внести необходимые изменения.

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении индикатора. Редактировать индикатор можно только в ручном режиме, при переключении на режим конструктора условие индикатора будет полностью изменено.

Для удаления индикатора атаки необходимо выбрать его с помощью кнопки выбора, установив флажок, после чего нажать кнопку **Удалить выбранные**. Для завершения операции ее необходимо подтвердить в открывшемся окне **Подтверждение действия**.

10.6.2. Индикаторы компрометации

Индикаторы компрометации (IOC) – это артефакты известной вредоносной активности.

Артефакты разделены по типам:

– имя файла;

– хеш-суммы, рассчитанные по алгоритмам SHA-256 (SHA-1 и MD5 будут обнаруживаться, если включена соответствующая настройка в профиле безопасности агента);

– IP-адрес;

– доменное имя;

– URL (на данный момент под URL подразумевается доменное имя и порт);

– сетевая сигнатура.

С каждым индикатором связано действие, которое необходимо предпринять в отношении него – «Детектировать» или «Блокировать». Детектирование подразумевает генерацию события, в котором указывается сработавший индикатор компрометации.

Работа со списком индикаторов компрометации обеспечивается посредством конфигурационного файла, доступного для просмотра и редактирования из графического интерфейса.

В графическом интерфейсе индикаторы компрометации представлены в виде таблицы с наборами.

Таблица наборов индикаторов имеет следующие столбцы:

– **Название набора**;

– **Количество записей** (правил в наборе);

– **Привязано агентов** (количество агентов, которым назначен данный набор правил);

– **Управление**.

Имеется возможность добавления/редактирования как самого набора, так и правил, входящих в набор, а также копирование индикатора из одного набора в другой, сохранение правил индикации (экспорт) с последующим импортом.

Правила в наборе представлены в виде таблицы со следующими столбцами:

– **Имя индикатора**;

– **Тип артефакта**;

– **Артефакт**;

– **Действие**;

– **Комментарий**;

– **Дата создания/Автор**;

– **Последнее изменение/Пользователь**;

– **Управление**.

В таблице наборов имеется набор с индикаторами, установленными по умолчанию.

Пример таблицы одного из наборов индикаторов компрометации представлен на рисунке 51.

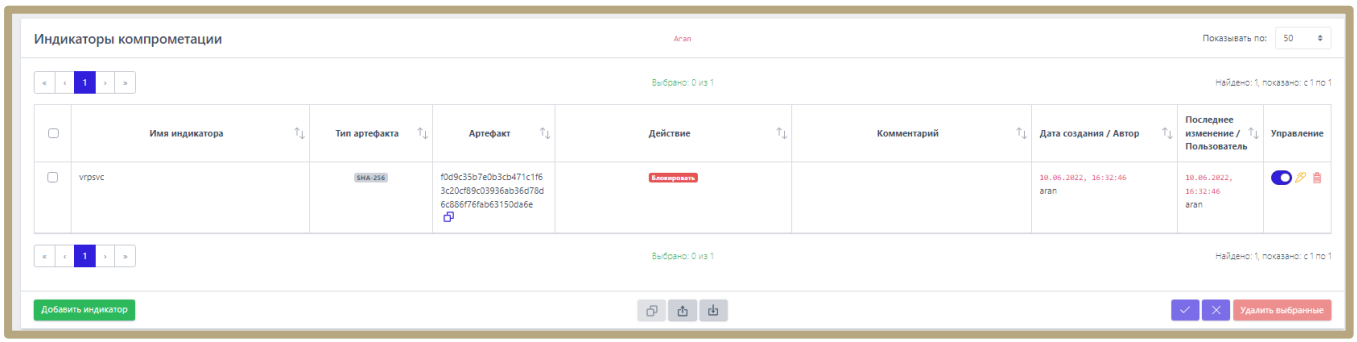


Рисунок 51 – Индикаторы компрометации

Индикаторы компрометации, обрабатываемые Программой, подразделяются на сетевые и файловые. Особенностью работы с файловыми индикаторами является то, что все файлы, находящиеся на конечных точках с установленным на них агентом, проверяются по имени файла или по хешам, если выполнены условия, описанные ниже.

Важно

Индикаторы по хеш-сумме файла работают только для файлов с активным содержимым. К файлам с активным содержимым в текущей реализации относятся исполняемые файлы (определяются по формату или расширению EXE, DLL, SYS, COM, OCX, SCR, CPL), а также так называемые «интересные» файлы с расширениями PDF, PS1, PSM1 и т.д. Соответствующие расширения «интересных» файлов должны быть указаны в профиле безопасности агента.

При обращении к файлу, хеш-сумма которого совпадает с хеш-суммой, указанной в индикаторе компрометации, обращение блокируется, а в модуле администрирования формируется (или дополняется) инцидент, объединяющий в себе все события, соответствующие индикатору. Эти события могут иметь разный тип в зависимости от выполняемой операции: открытие файла, чтение, удаление, а также могут относиться к разным процессам в системе. Блокируются все операции с файлом, изолируя его "по месту", без перемещения в карантин. Запуск исполняемого файла, хеш которого присутствует в перечне индикаторов компрометации, будет блокироваться монитором файловой системы на самом раннем этапе запуска, когда системный объект **процесс** для него еще не сформирован.

Важно

Если в профиле безопасности агента установлен режим «только детектирование», то действие «блокировать» для индикаторов компрометации, применяемых на агенте, будет переопределено на действие «детектировать».

На странице **Наборы индикаторов компрометации** (рис. 52) в разделе **Индикаторы компрометации** содержится информация об объектах (или артефактах), которые являются источником компрометации.

Обнаружение событий, связанных с описанными в наборах компрометации артефактами, вызывает определенное действие, зафиксированное в наборе. Таким действием может быть блокирование или детектирование вызываемого артефактом процесса.

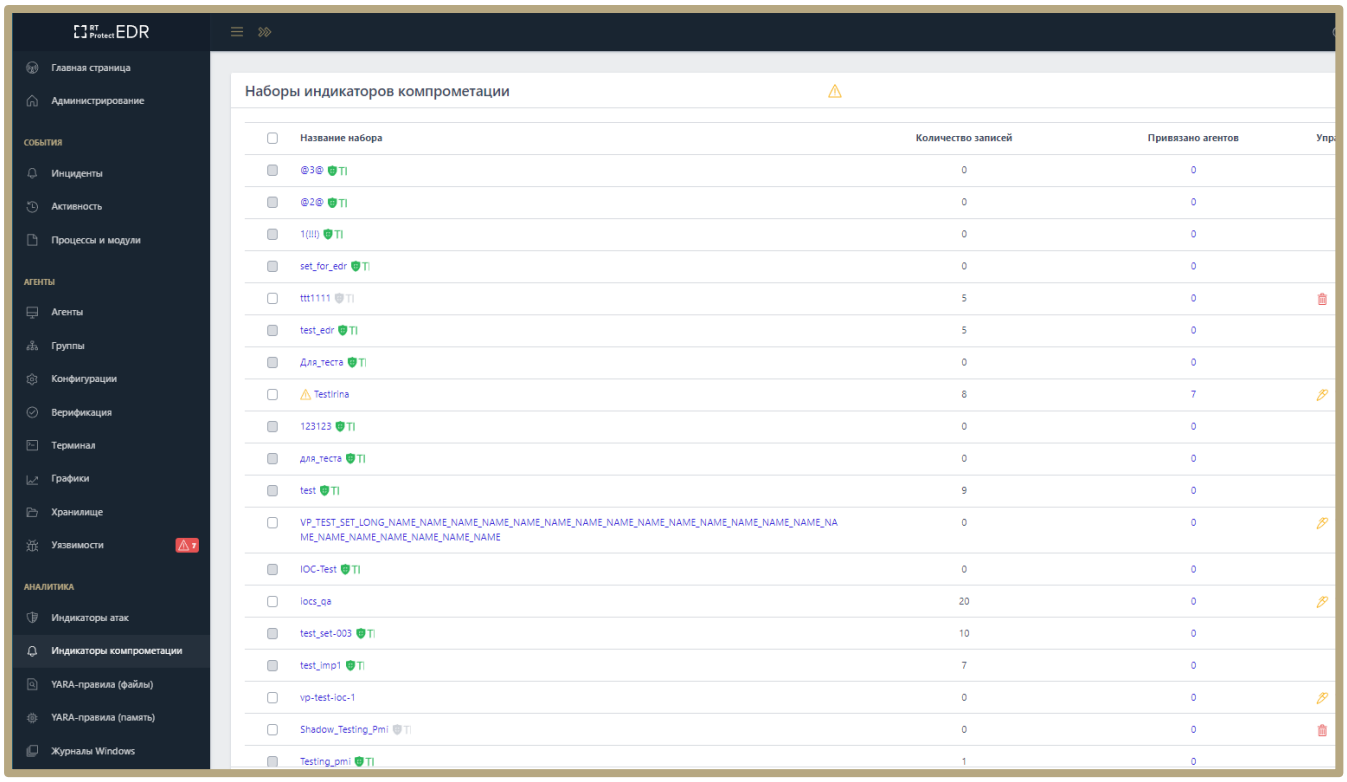


Рисунок 52 – Наборы индикаторов компрометации

Информация на странице представлена в табличном виде. Если присутствует хотя бы один несохраненный набор индикаторов компрометации, то в верхней части таблицы появится значок предупреждения  .

В шапке таблицы представлены следующие поля:

– кнопка выбора (отмечена элементом );

– **Название набора**;

– **Количество записей**;

– **Привязано агентов**;

– **Управление**.

Название набора – в поле отображается название набора индикаторов компрометации, при нажатии ЛКМ на название набора происходит переход на страницу изменения набора.

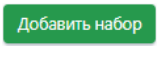
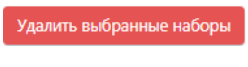
Количество записей – в поле отображается количество индикаторов, сохраненных в наборе.

Привязано агентов – в поле отображается количество привязанных к набору агентов. При нажатии ЛКМ на число агентов происходит переход к странице **Агенты**, на которой в таблице будут показаны привязанные к набору агенты.

Управление – в поле отображаются кнопки операций с набором индикаторов компрометации: **Редактировать** (), **Удалить** () и **Сохранить** ().

Редактировать – при нажатии кнопки  открывается окно **Редактировать набор**. В поле **Имя** отображается название набора, для его изменения необходимо ввести в строке с именем набора новое имя и нажать кнопку  .

Сохранить – кнопка  отображается в поле **Управление** при условии, что набор индикаторов компрометации не сохранен в Программе.

В нижней части страницы находятся кнопки  и  . Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Добавить набор** в строке **Имя** ввести название нового набора.

Если к новому набору требуется добавить индикаторы из наборов, созданных и сохраненных в Программе ранее, то в поле **Базовый набор** необходимо выбрать из выпадающего списка набор, который станет основой для нового набора.

Добавление базового набора является опциональным условием. Если в окне **Добавить набор** не ввести значение имени нового набора, то кнопка **Добавить** не будет активна.

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

Переход на страницу с таблицей **Индикаторы компрометации** (рис. 53) происходит при нажатии ЛКМ на названии набора в таблице **Наборы индикаторов компрометации**.

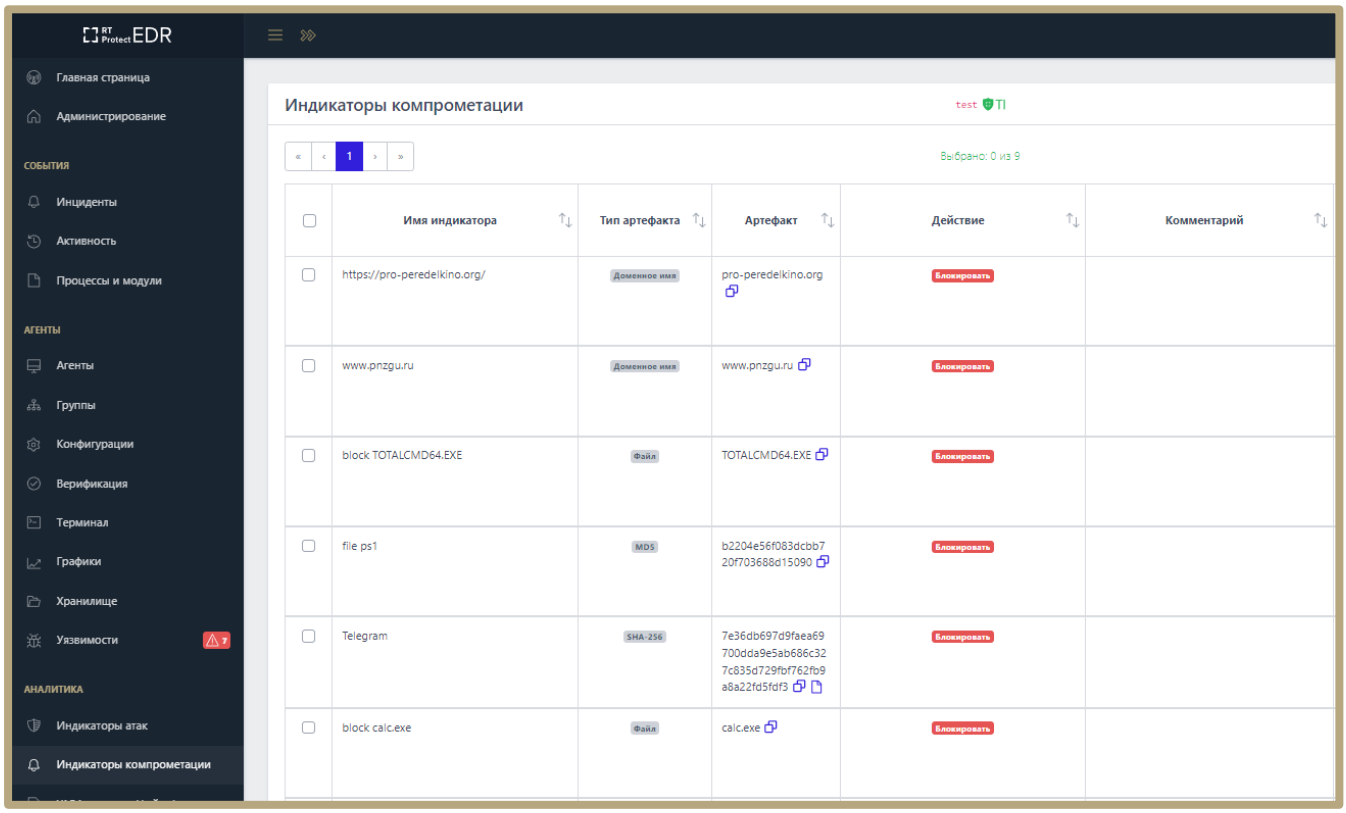


Рисунок 53 – Индикаторы компрометации

В области **Индикаторы компрометации** аналитик может:

– просматривать информацию об индикаторах, входящих в выбранный набор;

– изменять индикаторы компрометации, входящие в выбранный набор;

– экспортировать индикаторы в файлы различных форматов;

– импортировать данные из файла в набор индикаторов;

– копировать индикаторы выбранного набора в другие наборы индикаторов компрометации;

– сохранять набор с добавленными индикаторами компрометации;

– удалять из набора выбранные индикаторы компрометации.

– активировать/деактивировать выбранные индикаторы компрометации.

После добавления или изменения индикаторов слева от названия набора появится значок ⚠ с предупреждающим сообщением **Набор не применен**. Сообщение появляется при наведении курсора мыши на предупреждающий значок.

Шапка таблицы с индикаторами содержит следующие поля:

1) Кнопка выбора (отмечена элементом ▢);

2) **Имя индикатора**;

3) **Тип артефакта**;

4) **Действие**;

5) **Комментарий**;

6) **Дата создания/Автор**;

7) **Последнее изменение/Пользователь**;

8) **Активность**;

9) **Управление**.

Имя индикатора – поле содержит произвольное название индикатора, заданное пользователем.

Тип артефакта – поле содержит тип объекта, являющегося индикатором компрометации. Каждый индикатор компрометации основывается на определенном типе артефакта. Тип артефакта задается при создании или изменении индикатора компрометации. В Программе предусмотрено несколько типов артефактов:

1) **Имя файла** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано имя файла, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

2) **SHA-256** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму sha-256, для объекта, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

3) **SHA-1** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму sha-1, для объекта, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

4) **MD5** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму MD5, для объекта, при обнаружении которого Программа создаст инцидент и выполнит предусмотренное действие;

5) **IP-адрес** – в качестве индикатора компрометации в поле **Артефакт** будет выбран IP-адрес сетевого соединения, при взаимодействии с которым Программа создаст инцидент и выполнит предусмотренное действие;

6) **Доменное имя** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано имя домена, при взаимодействии с которым Программа создаст инцидент и выполнит предусмотренное действие;

Важно

Домен и IP-адрес могут быть написаны в индикаторе вместе с портом (<IP/домен>:<порт>)

---

7) **URL** – в качестве индикатора компрометации будет выбран унифицированный указатель ресурса в сети Интернет, при взаимодействии с которым Программа создаст инцидент;

Важно

Тип артефакта **URL** поддерживается не всеми версиями агента.

---

8) **Сетевая сигнатура** – в качестве индикатора компрометации в поле **Артефакт** будет выбрана сетевая сигнатура, при обнаружении которой система создаст инцидент и выполнит предусмотренное действие (под сетевой сигнатурой подразумеваются сигнатуры в формате Snort).

Артефакт – в поле отображается наименование артефакта. Название артефакта должно соответствовать выбранному типу артефакта, то есть, если указать тип артефакта **Доменное имя**, то название артефакта должно соответствовать правилам написания доменных имен, к примеру, **example.com**. Дополнительно поле содержит элемент , позволяющий скопировать в буфер обмена имя артефакта.

Действие – в поле отображается действие, которое должна осуществить Программа при обнаружении события, связанного с выбранным индикатором компрометации. В качестве ответа на вредоносную или потенциально вредоносную активность в Программе предусмотрены следующие действия:

1) Блокировать – в этом случае активность будет запрещена;

2) Детектировать – в этом случае активность будет разрешена, но Программа уведомит пользователя об обнаружении детектируемого события, создав инцидент.

Комментарий – в поле отображается произвольный комментарий к выбранному индикатору компрометации. Поле **Комментарий** заполняется при необходимости во время редактирования или добавления нового индикатора.

Дата создания/Автор – в поле отображается имя пользователя, создавшего индикатор компрометации, и время его создания.

Последнее изменение/Пользователь – в поле отображается время последнего изменения индикатора и имя пользователя, внесшего изменение.

Активность – в поле отображается кнопка / активировать/деактивировать индикатор компрометации.

Управление – в поле отображаются кнопки **Редактировать** и **Удалить** . Для редактирования индикатора компрометации необходимо нажать кнопку **Редактировать**.

В открывшемся окне **Редактировать индикатор** необходимо изменить одно или несколько полей, требующих изменения или корректировки, и нажать кнопку **Сохранить** (рис. 54).

Поля формы **Редактировать индикатор** идентичны полям шапки таблицы индикаторов, описанным выше.

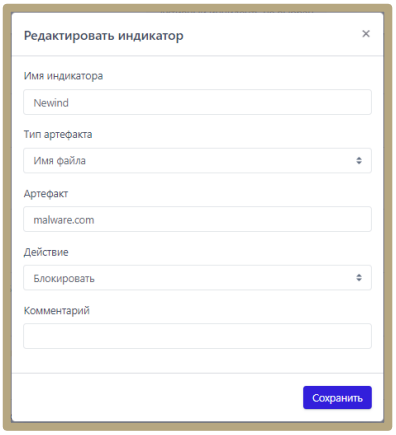


Рисунок 54 – Окно «Редактировать индикатор»

Для удаления индикатора компрометации необходимо нажать кнопку **Удалить** .

В нижней части таблицы находятся кнопки операций с индикаторами:

1) Добавить индикатор;

2) Применить набор – ;

3) Копировать выбранные элементы в другой набор – ;

4) Экспортировать набор в файл – ;

5) Импортировать данные из файла в набор (поддерживаемые форматы: csv, json) – ;

6) Активировать выбранный элемент (группу элементов) – ;

7) Деактивировать выбранный элемент (группу элементов) – .

Для добавления индикатора в области **Индикаторы компрометации** необходимо нажать кнопку Добавить индикатор. Далее в открывшемся окне **Добавить индикатор** необходимо заполнить представленные поля и нажать кнопку Добавить (рис. 55).

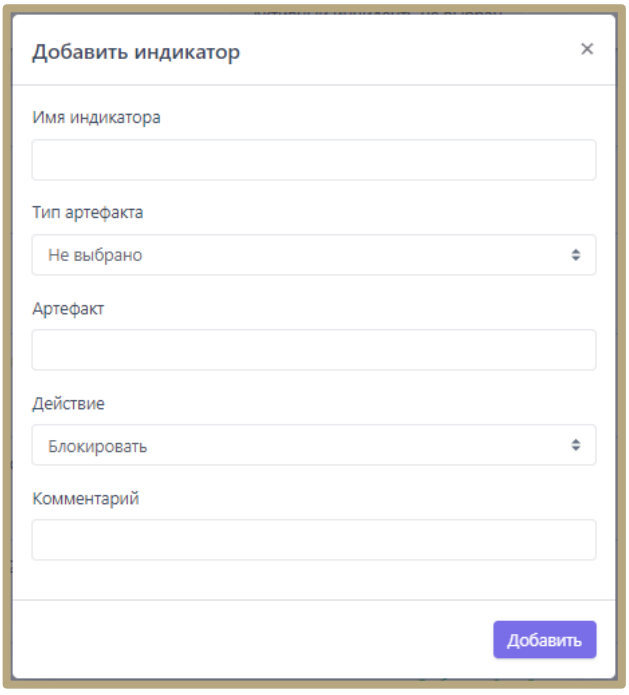
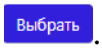


Рисунок 55 – Окно «Добавить индикатор»

Для применения любого изменения в наборах индикаторов необходимо нажать кнопку **Применить набор** ( ). Кнопка не будет отображаться на странице до внесения очередных изменений в набор.

Для копирования индикаторов из одного набора в другой необходимо отметить флажками кнопки выбора для индикатора или индикаторов, которые нужно скопировать в другой набор. После выбора индикаторов следует нажать кнопку **Копировать выбранные элементы в другой набор**  .

В открывшемся окне **Выбор набора** необходимо в поле **Набор** выбрать из выпадающего списка набор индикаторов компрометации. В этот набор будут скопированы выбранные ранее индикаторы. Для завершения операции нужно нажать кнопку  . Для отмены операции необходимо нажать кнопку или кнопку закрытия окна .

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл**  . Далее в открывшемся списке форматов файла необходимо выбрать формат, в котором будут сохранены данные из набора. После выбора формата созданный файл в указанном формате будет сохранен в папку, в которую настроена загрузка файлов в операционной системе.

Для импорта данных из файла с индикаторами необходимо нажать кнопку  (**Импортировать данные из файла в набор, поддерживаемые форматы: csv, json**). После нажатия кнопки открывается окно проводника, в котором необходимо выбрать импортируемый файл, после чего импортировать данные из файла в выбранный набор индикаторов компрометации. После завершения операции импорта индикаторы компрометации из импортируемого файла добавятся в выбранный набор.

Для временной активации/деактивации одного или нескольких индикаторов можно воспользоваться кнопками  , предварительно отметив элемент или группу элементов флагом.

Появится окно подтверждения активации либо деактивации. Для подтверждения действий следует нажать кнопку **Выполнить**. После выполнения операций появятся всплывающие окна, а в таблице индикаторов в столбце **Последнее изменение/Пользователь** будут отображаться дата, время и имя пользователя, производившего действия.

10.6.3. YARA-правила (файлы)

YARA-правила для файлов – это программные элементы, позволяющие определить сигнатуры файлов, которые Программа в случае их обнаружения в защищаемой инфраструктуре отметит как вредоносные.

YARA-правила, как и индикаторы компрометации по хешу, по умолчанию применяются только к исполняемым файлам (PE), к другим файлам могут применяться только после добавления соответствующих расширений в профиле безопасности агента. Матчинг PE-файлов по сохраненным в Программе YARA-правилам возможен только при запуске таких файлов. Под запуском PE-файлов подразумевается исполнение программ, загрузка динамических библиотек (или драйверов) для исполнения их кода. В случае с так называемыми «интересными» файлами с потенциально активным содержимым (файлы с расширениями PDF, PS1, PSM1 и т.д.) анализ по YARA-правилам выполняется при любом открытии документов или скриптов, то есть когда осуществляется доступ к их содержимому. Анализ будет проводиться для таких файлов только в том случае, если соответствующие расширения будут указаны в профиле безопасности агента.

Важно

Файловым монитором агента по умолчанию сканируются только PE-файлы, причем сканирование может настраиваться в соответствии с наличием или отсутствием у файла электронной подписи. Для этого используются настройки профиля безопасности агента.

В Программе предусмотрены YARA-правила в наборе по умолчанию, а также инструментарий для создания новых правил. Таблица с наборами YARA-правил (рис. 56) включает в себя структурные элементы, идентичные элементам таблицы наборов индикаторов компрометации. Подробную информацию об этих элементах и работе с ними можно узнать в пункте 10.6.2.

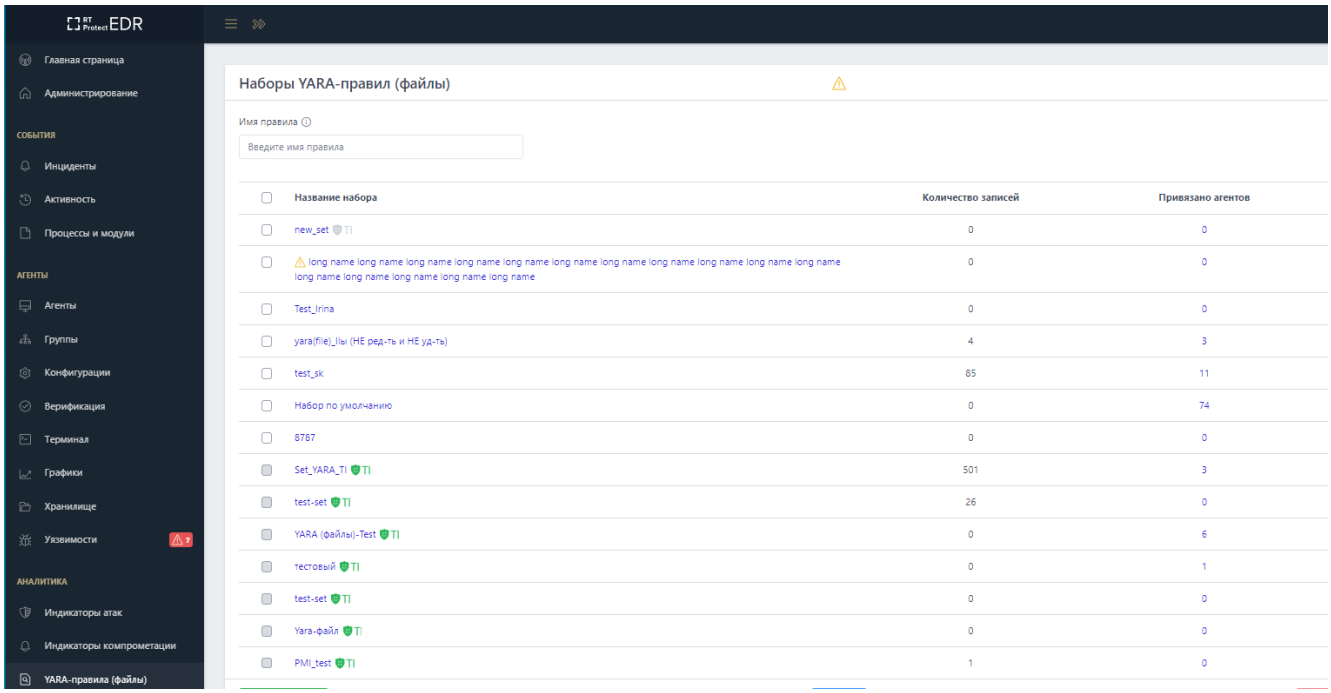


Рисунок 56 – Наборы YARA-правил (файлы)

При нажатии ЛКМ на имени набора открывается страница **YARA-правила** для выбранного набора, которая включает в себя кнопки операций, идентичные описанным в подпункте 10.6.2:

1) Добавить правило (открывает окно, в котором аналитик может добавить одно или несколько правил, при этом необходимо учитывать, что все имена правил должны быть уникальными);

2) Применить набор – (кнопка отображается, если в файле YARA были изменения);

3) Копировать/переместить выбранные элементы в другой набор ( ) – перемещает или копирует выбранный файл или файлы с правилами YARA из одного набора в другой;

4) Экспортировать набор в файл формата JSON– ;

5) Импортировать данные из файла в набор (поддерживаемые форматы: JSON) – ;

6) Активировать YARA-правило – (все правила, указанные в файле, будут активированы);

7) Деактивировать YARA-правило – (все правила, указанные в файле, будут деактивированы);

8) Редактировать ( ) – открывает окно редактирования YARA-правил;

9) Удалить ( ) – удаляет файл с YARA-правилами.

Кроме указанных выше кнопок на странице **YARA-правила** в строке с именем файла присутствует значок просмотра ( ), который позволяет прочесть условие, не заходя в окно редактирования правил.

После нажатия кнопки **Добавить правила** необходимо выбрать, будет ли файл с YARA-правилами создаваться аналитиком или загружаться из ранее сохраненного файла. В случае с созданием нового файла откроется окно **Добавить YARA-правила**, в котором необходимо прописать одно или несколько правил, которые будут обнаруживаться поисковым движком YARA.

Для загрузки YARA-файла или нескольких YARA-файлов на сервер с хоста аналитика необходимо выполнить следующие операции:

1) Нажать кнопку **Добавить правила** и выбрать операцию **Загрузить файлы**;

2) В открывшемся окне **Загрузить файлы YARA** нажать кнопку **Выбрать файлы** и в окне Проводника выбрать один или несколько YARA-файлов для загрузки (файлы с расширениями .yar);

3) Далее нажать кнопку **Загрузить файлы на сервер**.

Важно

YARA-правила работают на агенте только в том случае, если в профиле безопасности выбранного агента установлен режим глубокого сканирования, включающий в себя YARA-правила, то есть выбраны режимы **YARA-правила** или **ML и YARA-правила**. При этом необходимо учитывать, что режим глубокого сканирования дает повышенную нагрузку на файловый монитор, а значит, и на Программу в целом.

В одном файле могут быть сотни, тысячи правил. Обязательным условием для сохранения файла является задание его имени в соответствующей строке. Правила и их имена, сохраняемые в файл, должны быть уникальными, то есть не иметь повтора в рамках одного файла. Для YARA-правил в рамках наборов это утверждение не распространяется – в разных наборах могут содержаться одинаковые YARA-правила.

Важно

Имена YARA-правил учитывают регистр и не должны превышать длину в 128 знаков.

Аналитик может воспользоваться функцией загрузки файла формата .yar при создании нового файла с YARA-правилами в окне **Добавить YARA-правила**. Чтобы загрузить файл с компьютера аналитика,

необходимо нажать кнопку  , после чего выбрать соответствующий файл в открывшемся окне и нажать кнопку **Открыть**.

Аналитик может фильтровать правила и файлы на странице по имени файла с именем правила. При этом поиск по имени правила требует ввода полного имени.

Подробнее об условиях и структуре YARA-правил можно узнать в разделе 7, пункте 8.3 и в официальной документации YARA.

10.6.4. YARA-правила (память)

YARA-правила для памяти – это программные элементы, которые позволяют определить вредоносные сигнатуры внутри памяти процесса путем ее сканирования.

Наборы YARA-правил для памяти формируются также, как и наборы YARA-правил для файлов. Доступны следующие операции с наборами:

1) Добавление набора;
2) Применение всех наборов (сохранение изменений, произведенных в наборах);
3) Удалить выбранные наборы;
4) Редактировать отдельный набор (изменение имени набора);
5) Удалить отдельный набор;
6) Применить отдельный набор.

Для работы внутри отдельного набора необходимо кликнуть по имени набора с YARA-правилами. Откроется страница **YARA-правила (память)** (рис. 57).

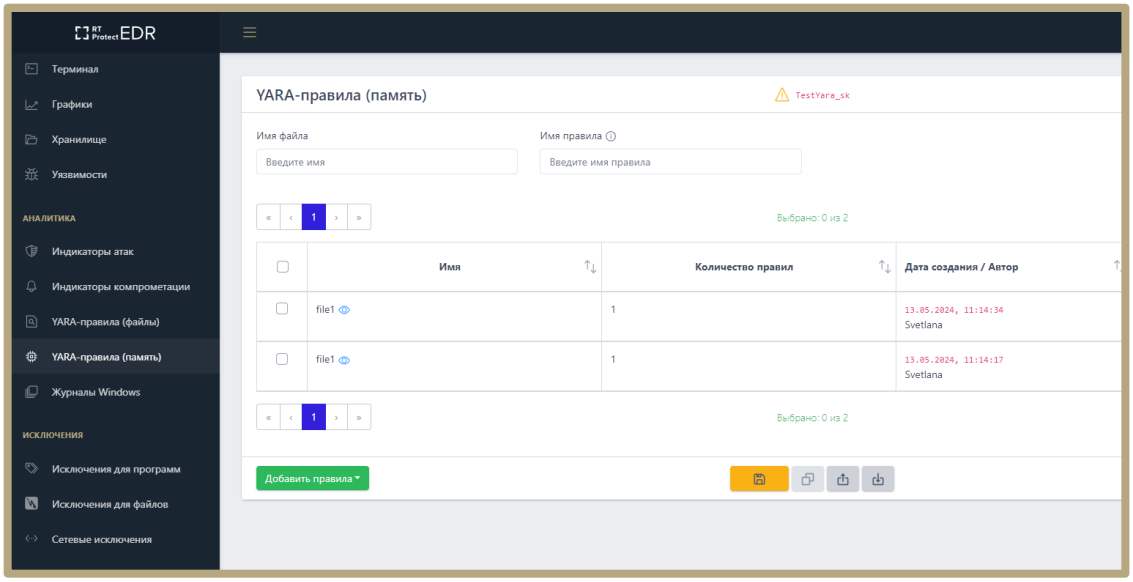


Рисунок 57 – YARA-правила (память)

Операции, которые можно выполнить на странице, представлены в таблице 56.

Таблица 56 – Операции на странице YARA-правила (память)

Операция	Шаги
Добавить YARA-правило или несколько правил в формате одного файла	1. Нажать кнопку **Добавить правила**. 2. Выбрать пункт **Новый файл**. Откроется окно **Добавить YARA-правила**. 3. В открывшемся окне ввести имя файла. 4. Нажать кнопку **Загрузить файл** ( ) и выбрать .yar -файл и нажать кнопку **Открыть**. Текст правила будет загружен в окно **Добавить YARA-правила**. 5. Если правило(а) прописываются вручную, то записать текст одного или нескольких правил в окне **Добавить YARA-правила**. 6. Нажать кнопку **Сохранить**.
Добавить YARA-правило или несколько правил в формате загрузки нескольких файлов	1. Нажать кнопку **Добавить правила**. 2. Выбрать пункт **Загрузить файлы**. Откроется окно **Загрузить файлы YARA**. 3. Нажать кнопку **Выбрать файлы**. В открывшемся окне выбрать один или несколько файлов в формате .yar, после чего нажать кнопку **Открыть**. При выборе нескольких файлов необходимо зажать клавишу Ctrl или Shift. 4. Нажать кнопку **Загрузить файлы на сервер**.
Применить набор (сохранить и применить изменения в YARA-правилах набора)	1. Нажать кнопку **Применить набор** ( ).

Копировать или переместить выбранные элементы в другой набор	1. Отметить флажком ( ) одно или несколько правил. 2. Нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ). Откроется окно **Выбор набора**. 3. В строке **Набор** выбрать набор, в который должны быть скопированы/перемещены правила. Если требуется переместить выбранные элементы с удалением из текущего набора, то следует установить флажок **Переместить и удалить выбранные элементы из текущего набора**. 4. Нажать кнопку **Выбрать**.
Экспортировать набор с правилами в файл	1. Нажать кнопку **Экспортировать набор в файл** ( ). Файл сохранится в папку автосохранения (чаще всего **Загрузки**)
Импортировать данные из файла в набор	1. Нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: JSON**. 2. В открывшемся окне выбрать файл для импорта и нажать кнопку **Открыть**.
Деактивировать один или несколько элементов (файлов с YARA-правилами)	1. Выбрать один или несколько элементов, установив флажок ( ); 2. Нажать кнопку **Деактивировать выбранные элементы** ( ). Откроется окно **Подтверждение действия**. 3. Нажать кнопку **Подтвердить**.
Активировать один или несколько элементов (файлов с YARA-правилами)	1. Выбрать один или несколько деактивированных элементов, установив на них флажок ( ); 2. Нажать кнопку **Активировать выбранные элементы** ( ). Откроется окно **Подтверждение действия**. 3. Нажать кнопку **Подтвердить**.
Удалить один или несколько выбранных элементов (файлы с YARA-правилами)	1. Выбрать один или несколько, установив на них флажок ( ); 2. Нажать кнопку **Удалить выбранные**. Откроется окно **Подтверждение действия**. 3. Нажать кнопку **Подтвердить**.
Деактивировать файл с YARA-правилами	1. В строке с выбранным файлом нажать кнопку **Деактивировать YARA-правила (память)** ( ). Откроется окно **Подтверждение действия**. 2. Нажать кнопку **Подтвердить**.
Редактировать файл с YARA-правилами	1. В строке с выбранным файлом нажать кнопку **Редактировать** ( ). Откроется окно **Редактировать YARA-правила**.

	2. Выполнить необходимые изменения YARA-правил и нажать кнопку **Сохранить**.
Удалить файл с YARA-правилами	1. В строке с выбранным файлом нажать кнопку **Удалить** ( ).Откроется окно **Подтверждение действия**. 2. Нажать кнопку **Подтвердить**.

Файлы и правила на странице можно фильтровать с помощью двух фильтров:

1) Имя файла;

2) Имя правила.

Важно

При поиске по имени правила необходимо вводить полное имя правила.

10.6.5. Журналы Windows

Во многих случаях для определения аномальной активности в защищаемой инфраструктуре аналитику могут понадобиться события, которые относятся к подсистеме журналирования Windows. В Программе предусмотрена возможность добавлять и отслеживать провайдеры событий подсистемы ETW.

После установки на хосте агент регистрирует ETW-провайдер RT Protect EDR. В этом журнале аналитик может просмотреть сообщения с ошибками, предупреждениями, информацией и т.д. Для просмотра журнала на агенте необходимо перейти в **Панель управления/Администрирование/Просмотр событий/Журналы приложений и служб/RT Protect EDR**.

Для просмотра журнала на сервере управления необходимо выполнить фильтрацию по DSL-запросу **winlog.provider_name:*RT*** на странице **Активность**.

Провайдеры добавляются в наборы. Чтобы создать или изменить набор с правилами обнаружения событий подсистемы журналирования аналитику необходимо перейти в раздел **Журналы Windows**.

На странице **Наборы журналов Windows** содержатся наборы с правилами детектирования подсистемы трассировки событий для Windows (ETW). События, генерируемые подсистемой ETW, собираются агентом и доставляются на сервер Программы.

На странице **Наборы журналов Windows** пользователю доступны те же операции, что и на странице **Наборы индикаторов компрометации** (см. пункт 10.6.2):

1) Добавление новых наборов;
2) Редактирование имен наборов;
3) Удаление выбранных наборов;
4) Применение изменений.

Таблица с наборами журналов Windows (рис. 58) содержит структурные элементы, идентичные структурным элементам таблицы **Наборы индикаторов компрометации**. С подробной информацией об этих элементах и работе с ними можно ознакомиться в подпункте 10.6.2.

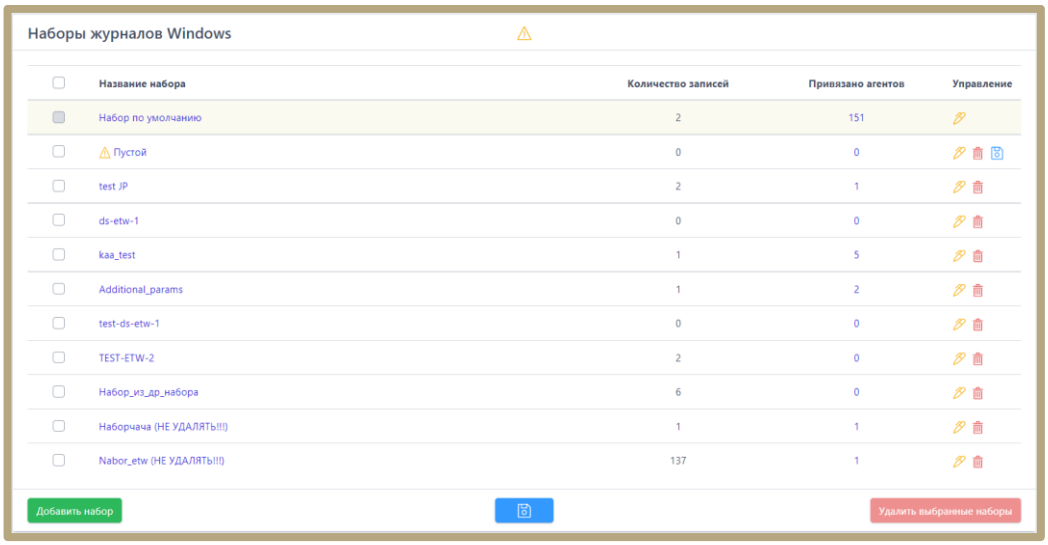


Рисунок 58 – Наборы журналов Windows

Для перехода к странице **Журналы Windows** необходимо нажать ЛКМ на имени набора.

На странице **Журналы Windows** в табличном виде отображается информация о конкретном наборе правил для ETW-событий. (рис. 59).

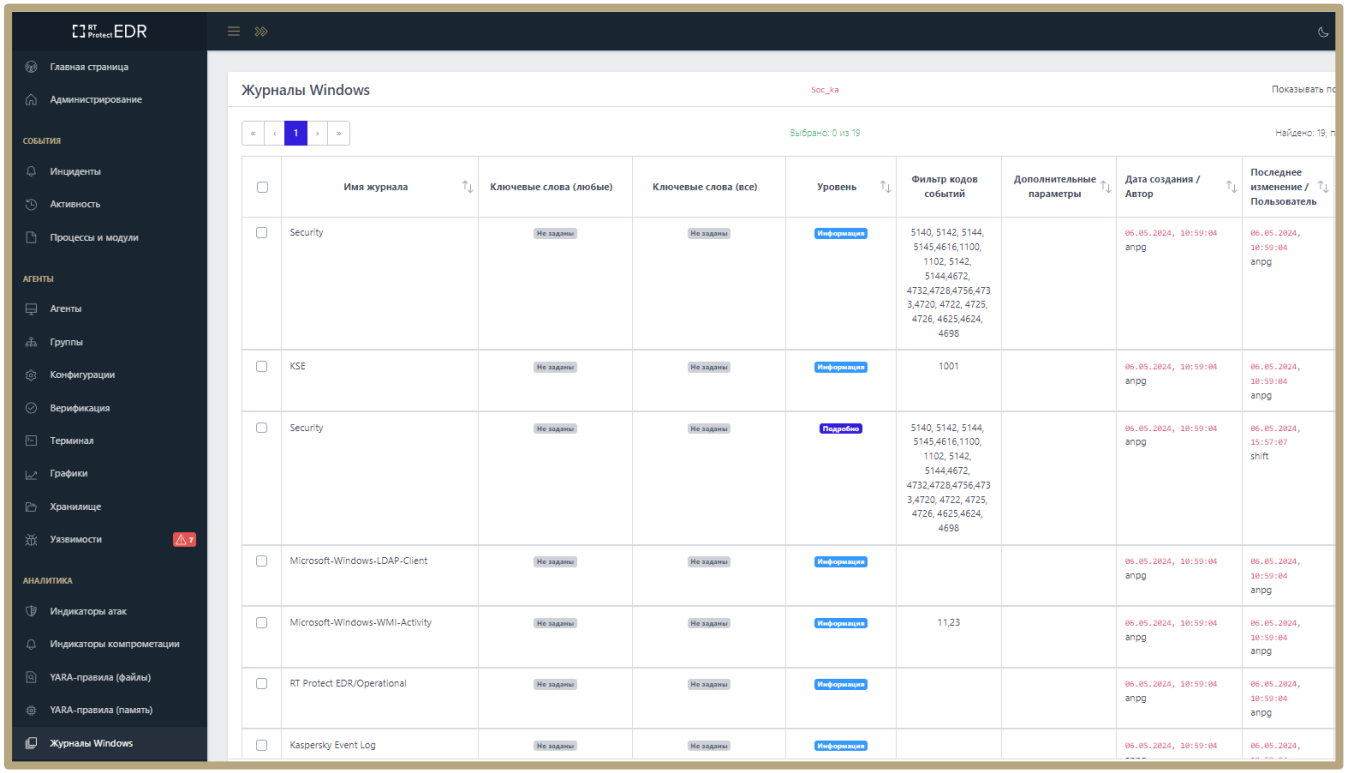


Рисунок 59 – Журналы Windows

Пользователь Программы, используя инструментарий, описанный ранее в пункте 10.6.2, может выполнить на странице следующие операции:

– добавить новое правило или несколько правил;

– редактировать или удалить существующее правило/правила;

– выполнить экспорт/импорт файла с набором;

– копировать элементы одного набора или весь набор в другой набор;

– активировать/деактивировать правило в наборе.

В таблице **Журналы Windows** отображаются следующие поля:

1) Поля кнопки выбора ( );

2) **Имя журнала**;

3) **Ключевые слова (любые)**;

4) **Ключевые слова (все)**;

5) **Уровень**;

6) **Фильтр кодов событий**;

7) **Дополнительные параметры**;

8) **Дата создания/Автор**;

9) **Последнее изменение/Пользователь**;

10) **Управление**.

Имя провайдера – в поле отображается имя провайдера событий подсистемы ETW.

Ключевые слова (любые) – в поле отображается информация о любых ключевых словах, на основе которых будут обнаруживаться события выбранного ETW-провайдера. В Программе доступна настройка детектирования событий по ключевым словам для определенных провайдеров ETW, поэтому для многих правил в поле будет отображаться надпись Не заданы.

Ключевые слова (все) – в поле отображается информация о всех ключевых словах, на основе которых будут обнаруживаться события выбранного ETW-провайдера.

В Программе доступна настройка детектирования событий по ключевым словам для определенных провайдеров ETW, поэтому для многих правил в поле будет отображаться надпись Не заданы.

Уровень – в поле отображается уровень обнаруживаемого события журнала, заданный пользователем Программы. Доступны следующие уровни событий: **Подробно**, **Информация**, **Предупреждение**, **Ошибка** и **Критическая ошибка**.

Фильтр кодов событий – в поле прописываются коды событий, согласно которым будут фильтроваться события выбранного провайдера. Правила записи кодов событий отображается при наведении курсора на значок ⓘ в окне добавления журнала (рис 60).

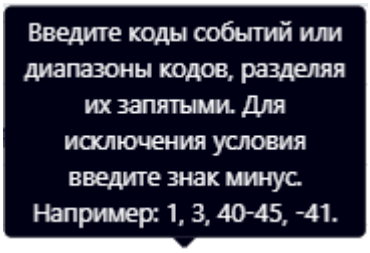


Рисунок 60 – Правила записи кодов событий

Дополнительные параметры – в поле отображается информация о дополнительных параметрах детектирования ETW-событий. Доступны для выбора следующие параметры:

1) SID пользователя;

2) ID терминальной сессии;

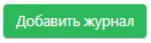
3) Стек вызовов;

4) Исключить события с нулевым значением KEYWORD;

5) Порядковый номер процесса;

6) Ключ события;

7) Исключить события от приватных процессов.

Чтобы добавить нового провайдера событий подсистемы ETW, в соответствии с настройками которого будут обнаруживаться события на агенте, необходимо в нижней части страницы нажать кнопку 

. Пользователю доступно два режима добавления журнала Windows:

– по GUID;

– по имени канала.

Для режима **GUID** обязательными к заполнению являются поля **Имя провайдера** и **GUID провайдера**. Для режима **Имя канала** обязательным для заполнения является поле **Имя канала**.

Для копирования или перемещения журнала из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ().

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

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

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

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

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

10.7 Добавление файлов или программ в список исключений

Исключения – это программные элементы, которые позволяют переопределить логику определенного события, например, сделать так, чтобы файл, который изначально система определила вредоносным воспринимался ей далее безопасным. Кроме того, исключения позволяют ограничить работу программы с помощью помещения её в «черный» список.

Исключения необходимы в случае появления ложных срабатываний. Ложные срабатывания можно разделить на два типа:

1) Статические – срабатывания, основанные на анализе содержимого исполняемых файлов (или файлов с потенциально активным содержимым, например, PDF и др.);

2) Поведенческие – такие срабатывания возникают в результате анализа действий процессов.

Чтобы добавить программу или файл в список исключений (если произошло ложное срабатывание), аналитик может воспользоваться функционалом разделов **Исключения для файлов** и **Исключения для программ**.

Чтобы добавить исключение, нужно выбрать набор с правилами и добавить файл или программу в исключения по имени или хешу, а в случае с программой можно дополнительно добавить ее по командной строке.

10.7.1. Механизм работы файловых исключений

Механизм файловых исключений предназначен для переопределения логики обработки файлов с потенциально активным содержимым (далее просто «файлы») со стороны агента EDR, которая реализуется перед запуском этих файлов. Среди файлов с активным содержимым можно выделить отдельную группу – исполняемые файлы, т.е. файлы программ (динамических библиотек, драйверов). Под термином «запуск» подразумевается исполнение программ (исполняемых файлов), загрузка динамических библиотек (или драйверов) для исполнения их кода, любое открытие PDF-документов или скриптов (если применены

соответствующие настройки в профиле безопасности агента), подразумевающее доступ к их содержимому, что трактуется тоже как попытка запуска.

В отсутствии файлового исключения для заданного файла агент при попытке запуска этого файла перед его запуском синхронно (т.е. в режиме реального времени) производит следующие действия:

1) Проверка файла по набору индикаторов компрометации (на основе имени файла или хеша от его содержимого), назначенному агенту;

2) Для исполняемых файлов выполняется статический анализ содержимого файла с использованием модели машинного обучения;

3) Сканирование содержимого файла по набору YARA-правил, назначенному агенту.

Важно

Кроме синхронной проверки механизм файлового сканирования предполагает также проверку в отложенном режиме, когда проверка происходит при создании или модификации файла.

Если по результатам проверок, перечисленных выше, запуск файла не блокируется, то для исполняемых файлов в потоке событий появляется событие о запуске программы или загрузке динамической библиотеки (драйвера), содержащее в числе прочего хеш исполняемого файла (sha-256 и, опционально, sha-1 и md5, что определяется настройками профиля безопасности агента). Когда данное событие доставляется на сервер EDR, он производит обращение к TI-платформе для проверки этого хеша (sha-256). Вердикт платформы предусматривает несколько вариантов дальнейшего развития событий согласно уровню опасности: «безопасный», «подозрительный» и «опасный». Получив вердикт в ответ на свой запрос, сервер EDR связывает его с исходным событием и, если вердикт не «безопасный», то регистрирует инцидент ИБ. При получении «опасного» вердикта сервер EDR дополнительно отправляет команду на принудительное завершение соответствующей программы на агенте (если проверка была инициирована событием запуска программы). «Подозрительный» вердикт не подразумевает дополнительных действий со стороны сервера EDR, кроме как регистрацию инцидента ИБ.

При наличии файлового исключения для заданного файла (идентифицируется по имени или хешу от содержимого) описанная выше логика изменяется согласно действию, которое предписывается исключением.

Если указано действие **Разрешить**, то все проверки, описанные выше, пропускаются (в том числе для исполняемых файлов пропускается взаимодействие с TI-платформой). В данном случае исключение работает в классическом понимании – исключает потенциально ложные срабатывания по содержимому файла (неправильный или нерелевантный индикатор компрометации, неточное YARA-правило, ошибочная оценка модели машинного обучения и т.д.). Если же указано действие **Блокировать**, то запуск файла безальтернативно блокируется.

При этом все описанные выше проверки опять же не выполняются. Однако такая блокировка не генерирует инцидент ИБ – в потоке событий лишь появляется событие о срабатывании исключения для файла с соответствующим предпринятым действием.

Совет

Такой режим работы с исключениями для файлов может использоваться для реализации политики предотвращения запуска нежелательного ПО, которое в то же время не относится к вредоносному в общем смысле, и, соответственно, попытки запуска которого не должны расцениваться как инцидент ИБ.

Ниже приведены практические примеры использования файловых исключений для решения задач по обеспечению ИБ и соблюдения регламентов по использованию ПО в компаниях.

1. Ложное срабатывание для загружаемой библиотеки msi.dll на платформе Windows.

В реальном контуре зафиксирован поток инцидентов ИБ, вызванных «подозрительным» вердиктом TI-платформы для библиотеки msi.dll (sha256 b98aab78e5ef705e67a1f2ad79d1c66cf7360e0be5a843846e5ec402cbd07c21) платформы Windows (рис. 61).

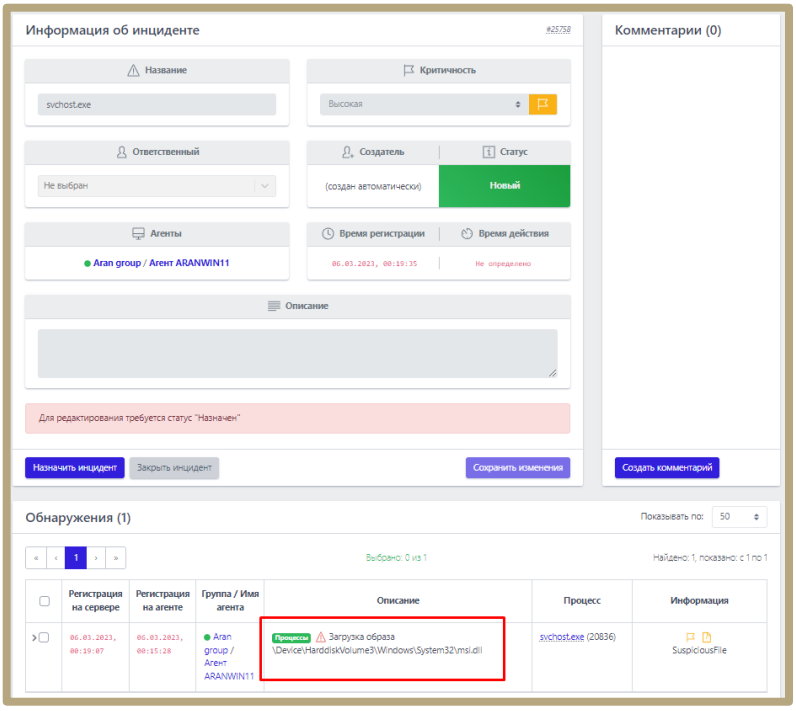


Рисунок 61 – Инцидент с загрузкой образа msi.dll

Данный вердикт обусловлен ошибочным индикатором компрометации в ленте, предоставляемой провайдером MalwareBazar (рис. 62).

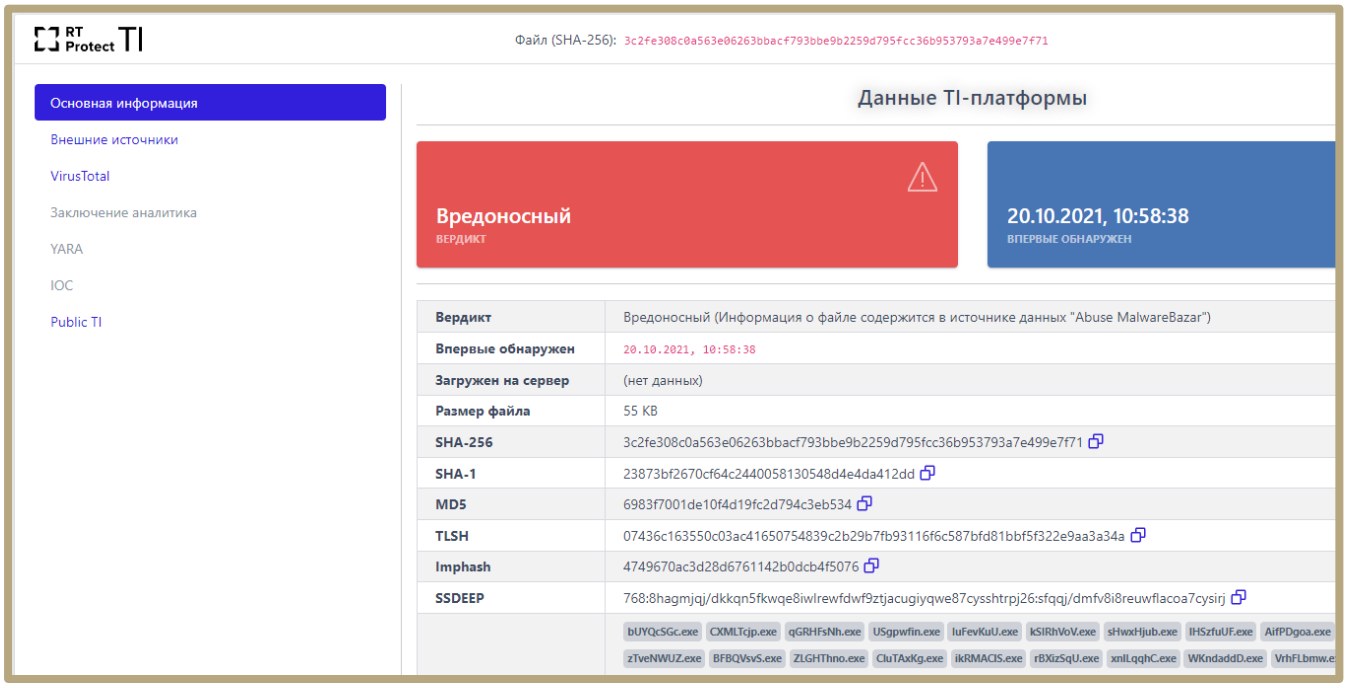


Рисунок 62 – Вердикт TI-платформы

Для решения проблемы создано файловое исключение со статусом **Разрешить** для указанного выше хеша (рис. 63).

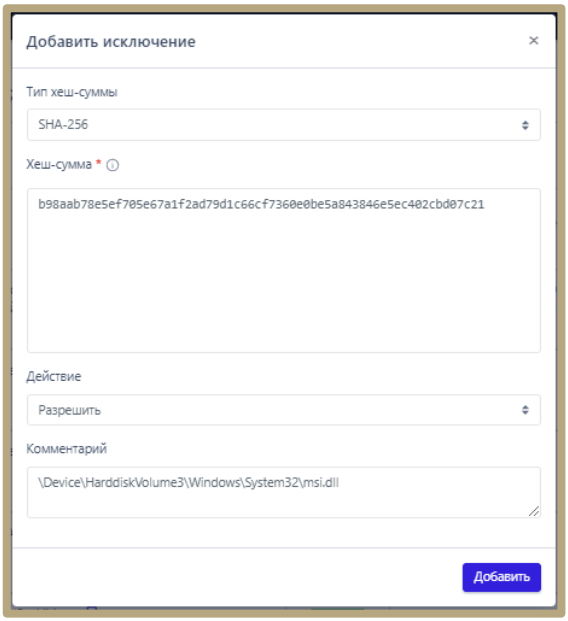


Рисунок 63 – Добавление файлового исключения

2. Запрет использования медиа-приложения MediaGet в компании.

Администратором безопасности в потоке событий обнаружено использование приложения MediaGet (ПО для Windows) в компании, в то время, как такое использование нежелательно (рис. 64).

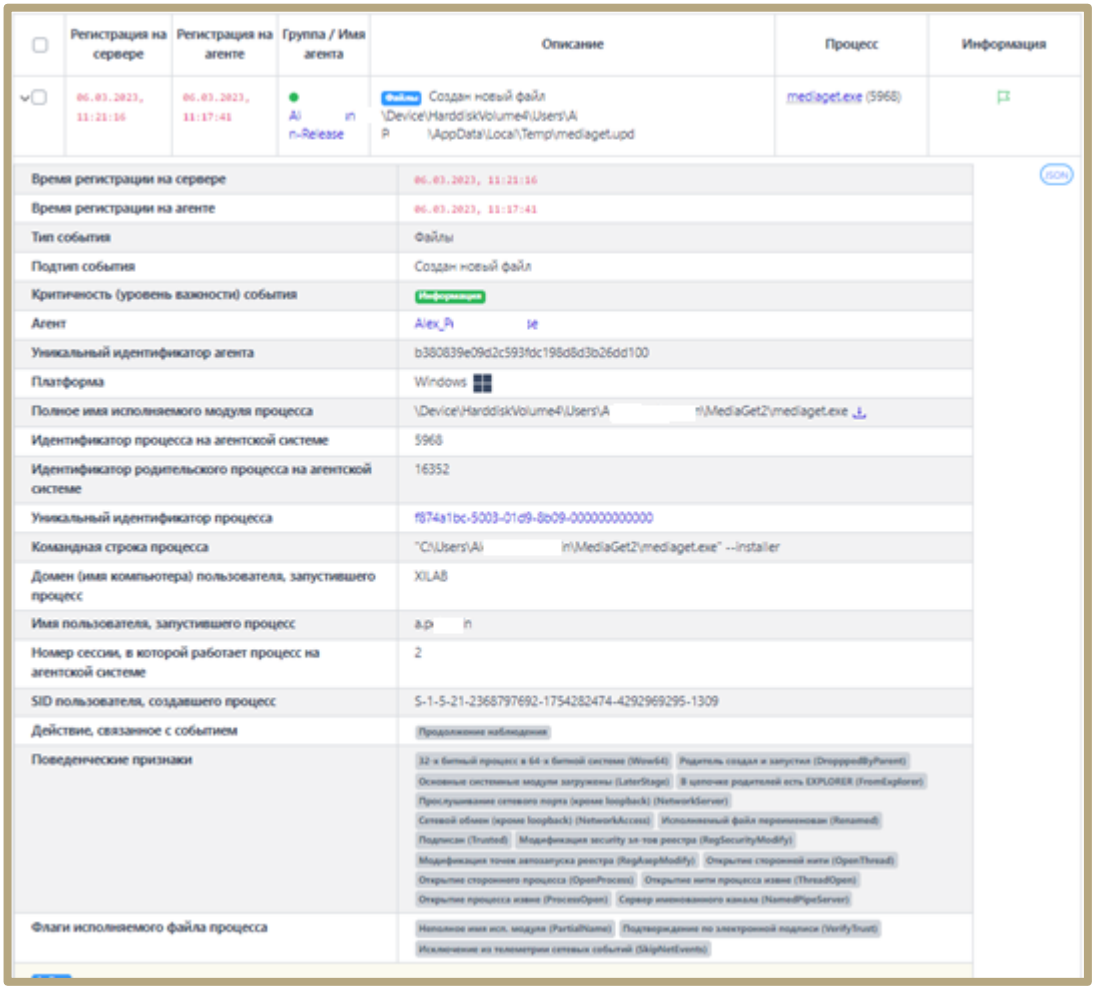


Рисунок 64 – Событие старта процесса mediaget.exe

Администратор может заблокировать использование конкретной версии программы MediaGet путем добавления в файловые исключения хеша ее исполняемого файла с действием **Блокировать** (рис. 65).

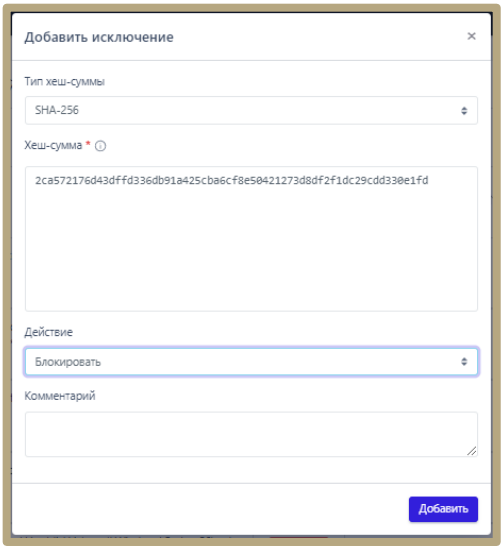


Рисунок 65 – Добавление блокирующего исключения

Кроме того, администратор может заблокировать любой запуск программы по имени ее исполняемого файла – mediaget.exe (рис. 66).

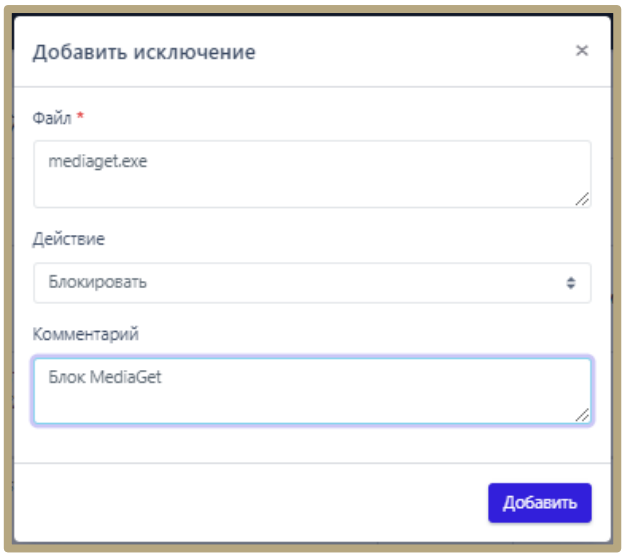


Рисунок 66 – Исключение по имени файла

В том или ином случае последующий запуск ПО MediaGet после создания исключения будет невозможен, а в числе событий при попытке такого запуска будет присутствовать событие о срабатывании соответствующего исключения (рис. 67 и рис. 68).

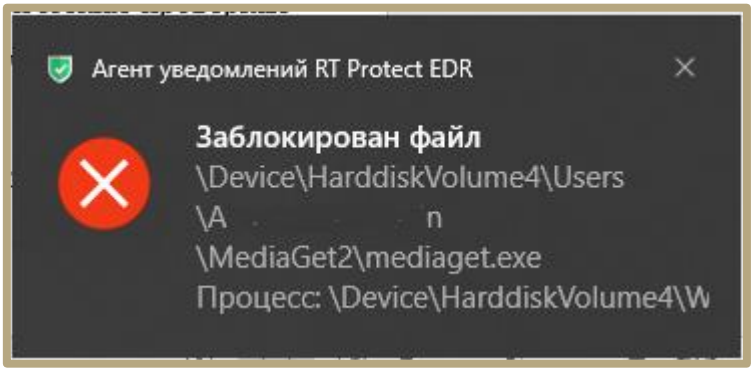


Рисунок 67 – Сообщение о невозможности запуска файла на агенте

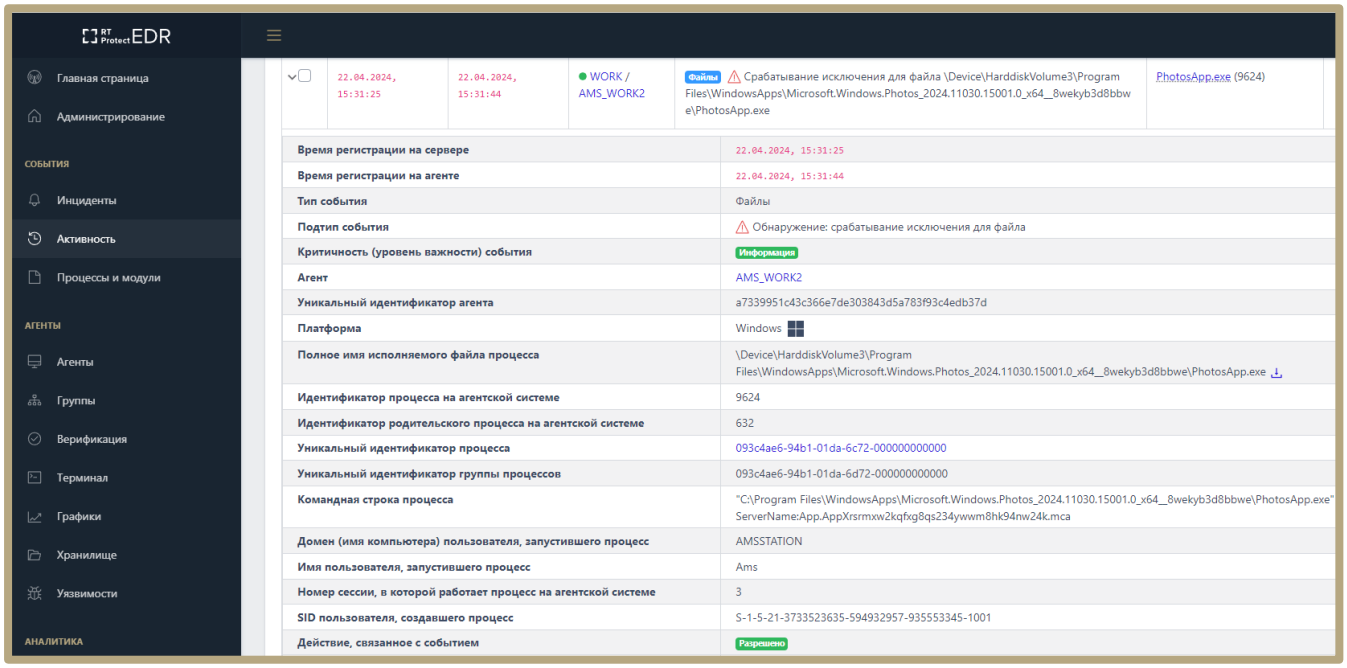


Рисунок 68 – Срабатывание исключения для файла

10.7.2. Добавление исключений для файла

Исключения для файлов должны основываться на статических проверках содержимого файлов. В системе RT Protect EDR к статическим проверкам содержимого файлов относятся:

– проверки на основе IOC-ов (имя файла, хеш от содержимого файла);

– анализ с помощью модели машинного обучения;

– сигнатурный поиск.

Элементы на странице **Исключения для файлов** (рис. 69):

1) Название набора;

2) Отображение количества выбранных элементов;

3) Кнопка выбора элементов таблицы ( );

4) Элементы навигации и фильтрации;

5) Поле **Комментарий**;

6) Поле **Дата создания/Автор**;

7) Поле **Последнее изменение/Пользователь**;

8) Элементы активации/деактивации правила в наборе (/ ,);

9) Элементы поля **Управление** ( );

10) Кнопки применения конфигурации правил, копирования, экспорта и импорта ( ).

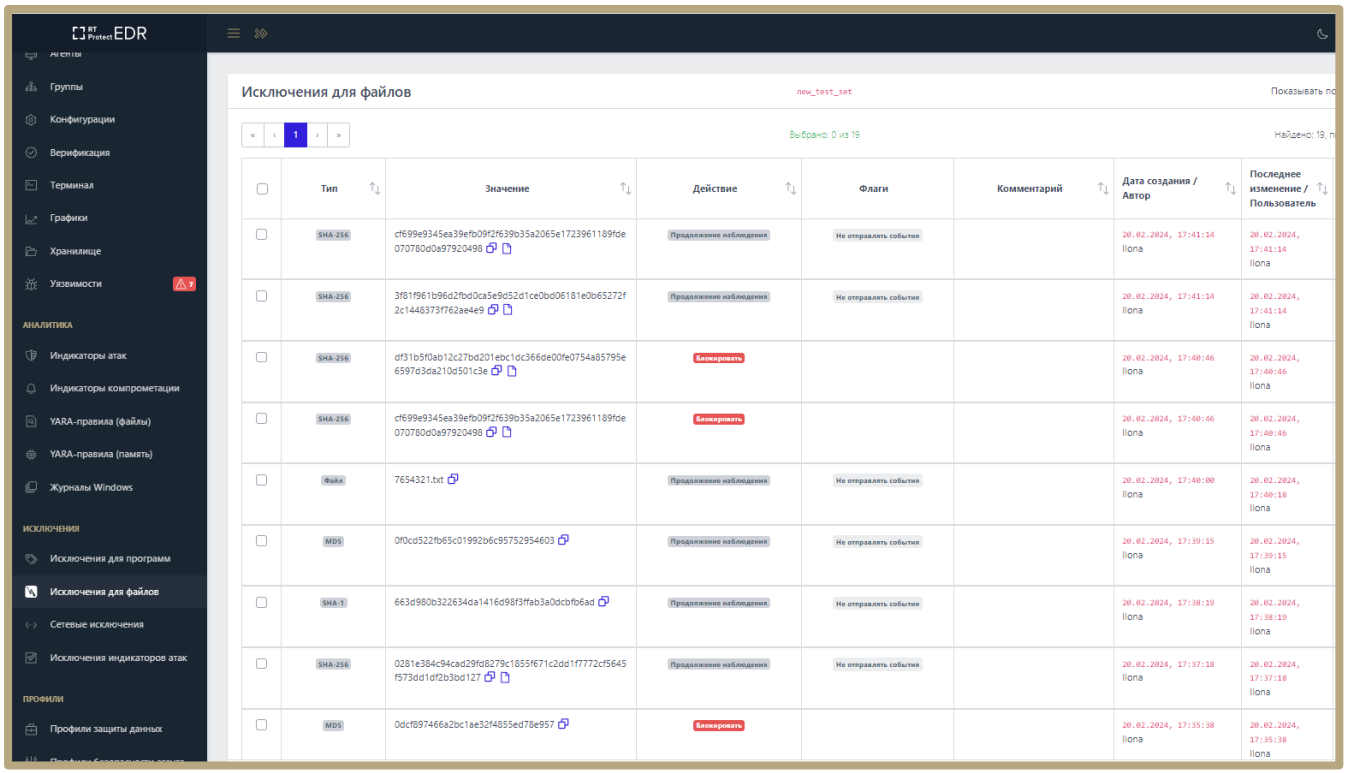


Рисунок 69 – Исключения для файлов

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение** и выбрать тип добавляемого исключения: **Файл** или **Хеш** (рис. 70).

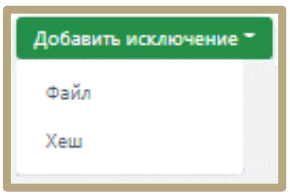


Рисунок 70 – Добавить исключение для файла (выбор типа)

Далее в открывшемся окне **Добавить исключение** необходимо заполнить поля с параметрами исключения. В зависимости от выбора типа исключения окно **Добавить исключение** будет содержать поля с различными параметрами.

Для типа **Файл** необходимо определить следующие параметры (рис. 71):

– **Файл**;

– **Действие**;

– установить значение опции **Не отправлять события**;

– **Комментарий**.

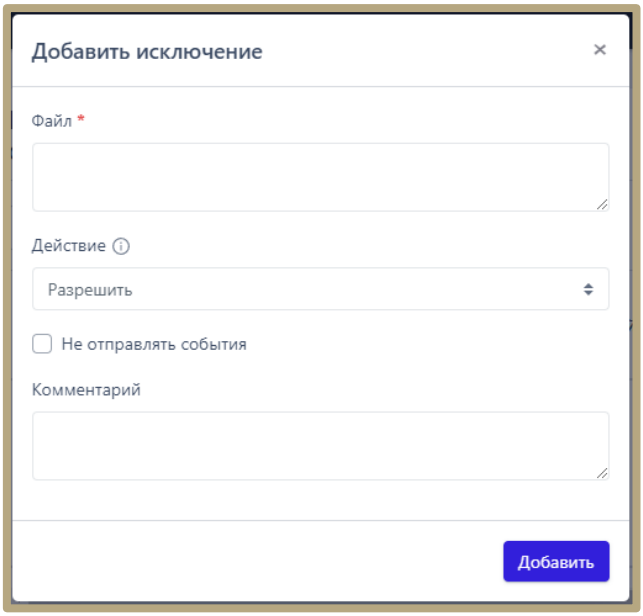


Рисунок 71 – Добавление исключения (файл)

Для типа **Хеш** необходимо определить следующие параметры (рис. 72):

– **Тип хеш-суммы**;

– **Хеш-сумма**;

– **Действие**;

– установить значение опции **Не отправлять события**;

– **Комментарий**.

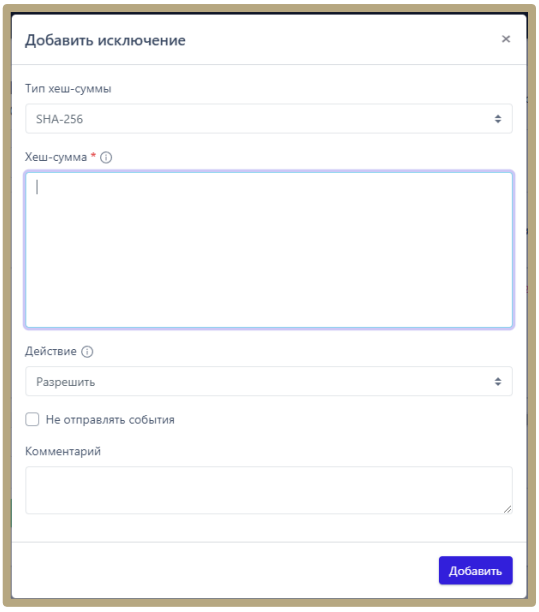


Рисунок 72 – Добавление исключения (хеш)

По умолчанию в Программе подсчитываются хеш-суммы по алгоритму SHA-256. Для подсчета хеш-сумм по алгоритмам SHA-1 и MD5 необходимо установить соответствующие флажки в профиле безопасности агента.

Файл – в поле прописывается имя файла, которое необходимо добавить в исключения. Имя файла после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Значение**. Поле является обязательным для заполнения, на что указывает значок *. Имя файла может задаваться с помощью регулярного выражения (файловые регулярные выражения Windows, допускающие использование символов ? для пропуска любого символа и * для пропуска последовательности символов любой длины, в т.ч. нулевой). Имя файла является менее точным способом подавления, его необходимо использовать в том случае, если имеется много экземпляров одной программы, на которой проявляется ложное срабатывание (рис. 73).

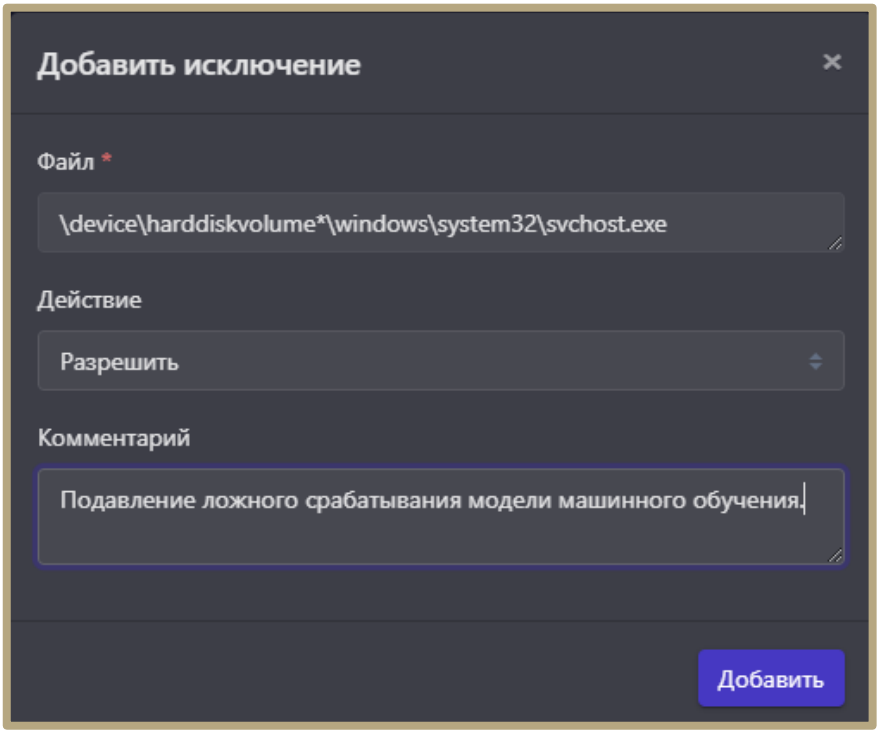


Рисунок 73 – Добавление исключения по файлу

Путь до файла должен быть указан в формате ссылки на устройство (как это выглядит на рисунке 73). Необходимо указывать максимально полное имя. Например, для исключения, представленного на рисунке 73, строка **svchost.exe* (или *svchost.exe*) является менее удачным вариантом, так как для любого файла с таким именем будут подавляться статические проверки, чем могут воспользоваться злоумышленники. Иерархия пути здесь обеспечивает некоторую защиту от этого. Квантификатор * все еще оставляет злоумышленнику возможность в любой вложенной директории повторить часть пути *\windows\system32\svchost.exe* и для такого файла будут отключены статические проверки (пример такого пути c:\temp\windows\system32\svchost.exe). В связи с этим, если требуется исключение для файлов, расположение которых предполагается только на системном томе, необходимо в качестве ссылки на системный том использовать переменные окружения: **%systemdisk%**, **%systemdrive%**.

Совет

Учитывая сказанное, для примера выше наиболее удачным вариантом указания пути до файла является: *%systemdisk%\windows\system32\svchost.exe*. Также необходимо отметить, что при обработке путей исключения регистр символов не учитывается.

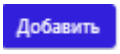
Действие – в поле устанавливается действие Программы в случае обнаружения файла с указанным именем или хеш-суммой. Предусмотрены следующие действия: **Блокировать, Разрешить**, **Продолжение наблюдения**. Выбранное действие после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Действие.** В случае с блокированием будет остановлен запуск файла с активным содержимым, в остальных случаях запуск будет разрешен, только для действия **Продолжение наблюдения** на сервер события отправляться не будут.

Опция **Не отправлять события** позволяет существенно изменить нагрузку по отправляемым событиям, связанным с тем или иным файлом, при этом необходимо учитывать, что сочетания включенной опции и действия **Блокировать**, а также выключенной опции и действия **Продолжение наблюдения** считаются недопустимыми, все остальные сочетания допустимы.

Комментарий – в поле прописывается произвольный комментарий. Для добавления нового файла-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром. Комментарий после добавления исключения будет отображаться в таблице И**сключения для файлов** в поле **Комментарий**.

Тип хеш-суммы – в поле устанавливается тип хеш-суммы файла. В Программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256**, **SHA-1** и **MD5**. Тип хеш-суммы после добавления исключения отображается в таблице **Исключения для файлов** в поле **Тип**.

Хеш-сумма – в поле прописываются значения хеш-сумм для файлов, которые необходимо добавить в исключения. После добавления исключения значение хеш-суммы отображается в таблице **Исключения для файлов** в поле **Значение**. Поле является обязательным для заполнения, на что указывает знак *. Метод добавления исключения по хеш-сумме является более безопасным, чем метод добавления исключения по имени файла, так как основан на содержимом файла.

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

.

В поле **Значение** таблицы с исключениями для файлов отображается значок  , который позволяет скопировать значение исключения в буфер обмена.

Для внесения изменений в исключение для файла необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключения для файлов** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

Удалить исключение можно, выбрав в таблице с исключениями необходимое правило и нажав кнопку .

В зависимости от типа исключения, которое можно увидеть в поле **Тип** таблицы **Исключения для файлов**, окно **Редактировать исключение** (рис. 74 и рис. 75) будет содержать разный набор полей, соответствующий окну **Добавить исключение** (см. рис. 71 и рис. 72).

Рисунок 74 – Редактировать исключение (тип имя файла)

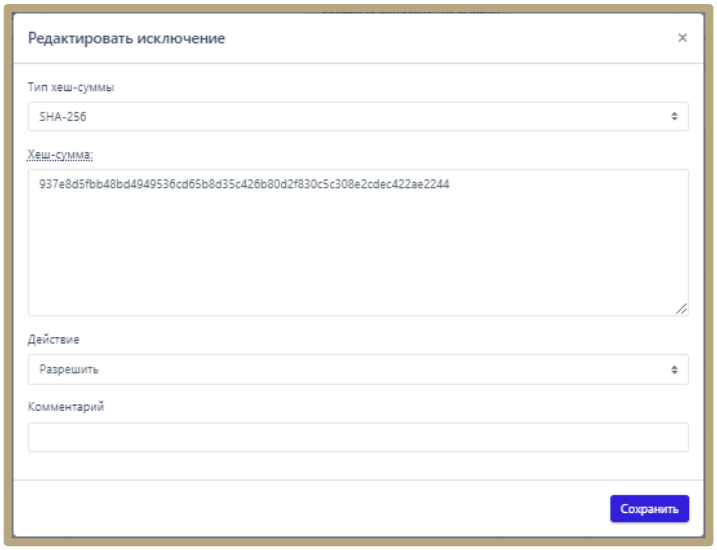


Рисунок 75 – Редактировать исключение (тип хеш-сумма)

Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений необходимо нажать кнопку **Закрыть окно** – ✕. После добавления файла в список исключений и сохранения набора с добавленным исключением необходимо применить этот набор для соответствующего агента или агентов. Для этого следует перейти на страницу **Настройка агента**, выбрать нужного агента из списка и в области **Конфигурация** применить измененный набор исключений для файлов (рис. 76).

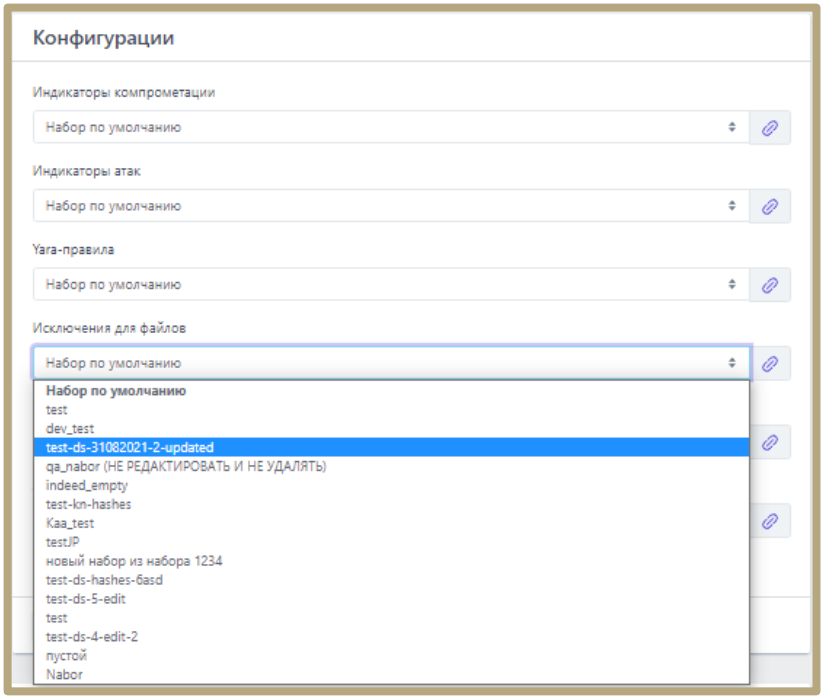


Рисунок 76 – Изменение конфигурации правил на агенте

Правило с добавленным исключением будет применяться для выбранного агента после применения конфигурации, для этого аналитику необходимо нажать кнопку Применить конфигурацию.

Примечание

Если требуется применить конфигурацию с исключением сразу на несколько агентов, то для этого следует перейти на страницу **Агенты**, отметить флажком агентов, для которых нужно применить исключение, и с помощью кнопки **Применить конфигурацию** ( ) назначить сохраненную ранее конфигурацию с исключением.

10.7.3. Исключения для программ

Исключения для программ – это программные элементы, которые позволяют управлять поведением процессов, управлять телеметрией и задействуют механизм идентификации программ. Это позволяет определить особенности исполнения программы.

Совет

При создании исключения необходимо руководствоваться общим принципом: чем точнее условия, описанные в исключении, тем лучше правило.

Чтобы аналитику добавить исключение для программы, ему необходимо перейти на страницу **Наборы исключений для программ** (рис. 77).

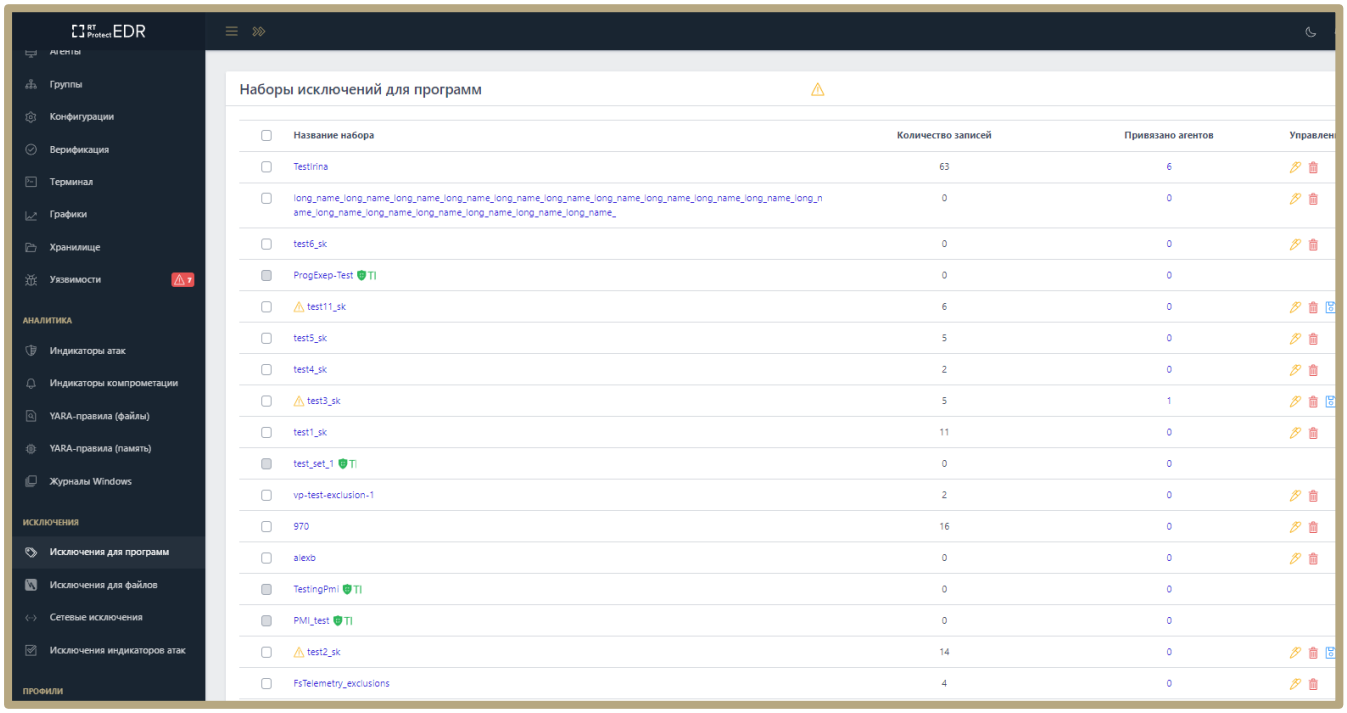


Рисунок 77 – Наборы исключений для программ

Для перехода к странице следует выбрать на панели управления раздел Исключения для программ. Здесь содержатся наборы с правилами, в каждый из них можно сохранить список исполняемых файлов, запуск которых должен соответствовать тем или иным настройкам безопасности. Для этого в Программе предусмотрена система флагов, устанавливающих параметры безопасности для

исполняемых файлов. Исключающие флаги определяют, какие проверки необходимо выключить для указанного исполняемого файла и порождаемого им процесса.

В список исключений для программ можно вносить исполняемые файлы без настройки для них каких-либо определенных условий, задаваемых флагами. Наличие этой возможности позволяет аналитику настроить EDR для уменьшения количества ложных срабатываний, а в случае необходимости, заблокировать ту или иную программу в целях обеспечения безопасности.

На странице **Наборы исключений для программ** пользователю доступны следующие операции:

– добавление новых наборов исключений;

– редактирование имен наборов исключений;

– удаление выбранных наборов исключений.

Для добавления программы в список исключений аналитику необходимо нажать ЛКМ на имени набора в поле **Название набора**, после чего откроется страница **Исключения для программ**. Информация о правилах с исключениями представлена в табличном виде (рис. 78).

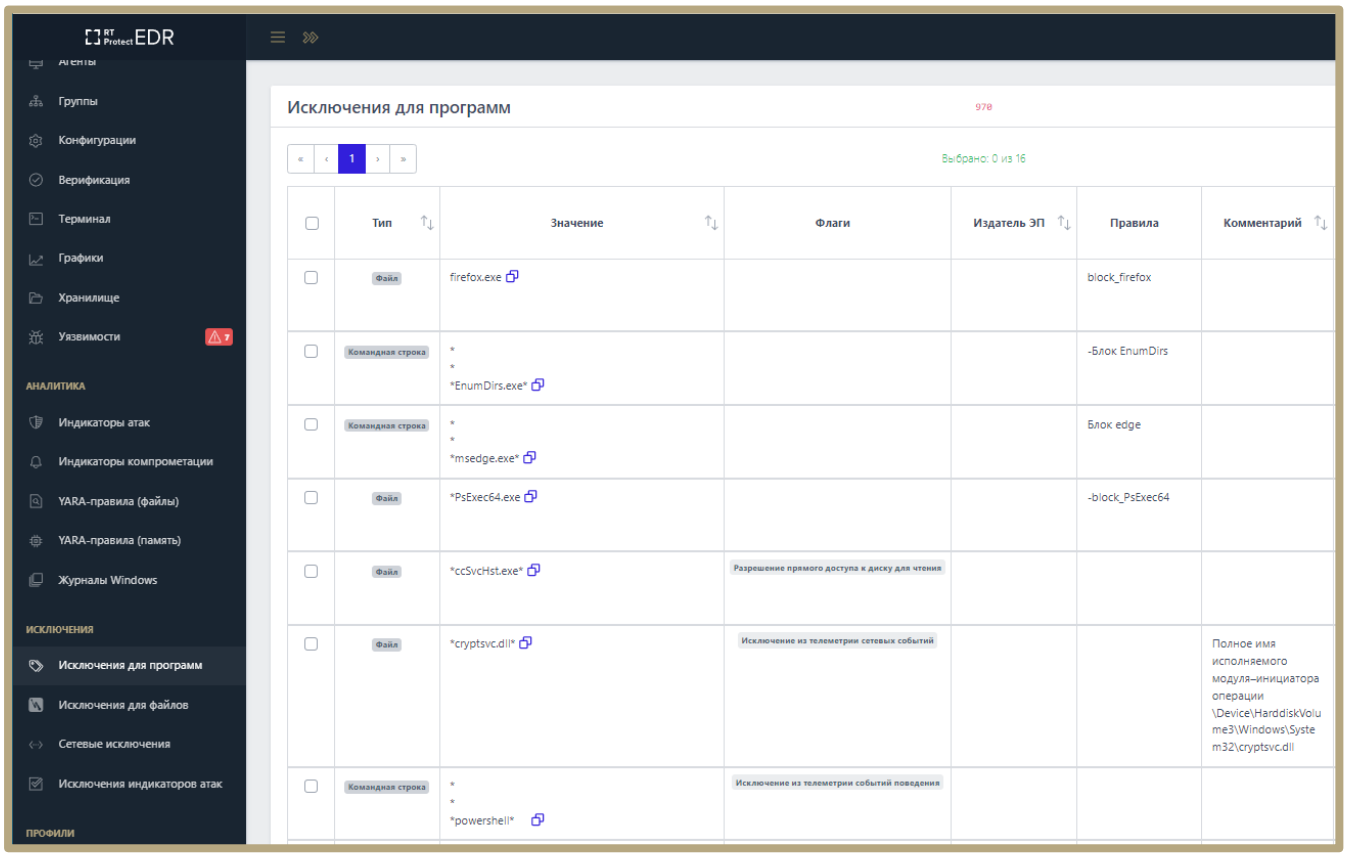


Рисунок 78 – Исключения для программ

Аналитику доступны те же операции, что и в разделе **Исключения для файлов** (см. пункт 10.7.2):

— добавление новых исключений;

— редактирование исключений;

— активация/ деактивация правила;

— копирование набора исключений;

— экспорт/импорт файлов с набором исключений;

— удаление исключений из набора.

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

Далее в открывшемся окне **Добавить исключение** необходимо установить параметры, в соответствии с которыми будет функционировать программа, внесенная в список исключений.

В зависимости от выбора типа исключения (**Файл**, **Хеш** или **Командная строка**) окно **Добавить исключение** будет содержать поля с различными параметрами.

Для типа исключений **Файл** необходимо определить следующие параметры:

— **Файл**;

— **Флаги**;

— **Издатель ЭП**;

— **Правила**;

— **Комментарий**.

Для типа исключений **Хеш** необходимо определить следующие параметры:

— **Тип хеш-суммы**;

— **Хеш-сумма**;

— **Флаги**;

— **Издатель ЭП**;

— **Правила**;

— **Комментарий**.

Для типа исключений **Командная строка** необходимо определить следующие параметры:

– **Командная строка прародителя**;

– **Командная строка родителя**;

– **Командная строка процесса**;

– **Флаги**;

– **Издатель ЭП**;

– **Правила**;

– **Комментарий**.

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

Важно

Правила указания имени файла при создании исключений для программ такие же, как и при создании исключения для файла. Т.е. регистр символов не учитывается, поддерживаются переменные окружения: **%systemdisk%**, **%systemdrive%**, допускается использовать символы ? и *, а также указывать имя файла программы без пути.

Тип хеш-суммы – в поле устанавливается тип хеш-суммы исполняемого файла. В программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256**, **SHA-1** и **MD5**. Тип хеш-суммы после добавления исключения отображается в таблице **Исключения для программ** в поле **Тип**.

Хеш-сумма – в поле прописываются значения хеш-сумм для исполняемых файлов, которые необходимо добавить в исключения. После добавления исключения значение хеш-суммы отображается в таблице **Исключения для программ** в поле **Значение.** Хеш-значение является наиболее точным способом идентификации программ при создании исключений для программ.

Командная строка (прародителя, родителя и процесса) – в поле прописывается значение командной строки в соответствии с правилами записи, справка о правилах записи командной строки появляется при наведении курсора мыши на значок ⓘ (рис. 79).

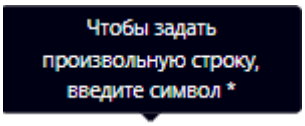


Рисунок 79 – Правила записи командной строки в исключениях для программ

После добавления исключения значение командной строки отображается в таблице **Исключения для программ** в поле **Значение**. При создании правила на основе командной строки все 3 поля для ввода командных строк («Командная строка прародителя», «Командная строка родителя», «Командная строка процесса») являются обязательными. Т.е. если мы хотим сделать правило для некоторой программы по командной строке её запуска, также необходимо указать командные строки запуска ее родительского процесса, а также прародительского. В случае, если значение каких-либо из указанных командных строк не важны, в качестве их значений следует использовать символ * (см. рис. 79).

Примечание

При использовании идентификации исключения на основе имени файла или командной строки необходимо стараться вводить как можно более полные значения путей и командных строк.

Путь *\device\harddiskvolume*\windows\system32\svchost.exe* является более безопасным, нежели **\svchost.exe* (или просто *svchost.exe*).

То же касается и командных строк: "*c:\Windows\System32\DISM.exe /Apply-Ffu /ImageFile:flash.ffu /ApplyDrive:\\.\PhysicalDrive0*" – более безопасно, чем "*c:\Windows\System32\DISM.exe *\\.\PhysicalDrive0*". И тем более, безопаснее варианта: "**DISM.exe *\\.\PhysicalDrive0*". Пути для командных строк следует брать из соответствующего события, поскольку некоторые пути могут начинаться с префикса \??\. Могут быть и другие отличия. В правилах необходимо указывать именно так, как этот путь видит агент. Для командных строк переменные окружения не поддерживаются. Регистр символов, также, как и для путей, не учитывается.

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

В Программе предусмотрены следующие типы флагов:

1) Управляющие поведением процессов (каждый флаг определяет право совершения процессом соответствующего потенциально опасного действия):

— разрешение внедрения кода в сторонние программы;

— разрешение записи памяти сторонних программ;

— разрешить чтения памяти сторонних программа и управления ими;

— право взаимодействия с критическими системными программами;

— разрешение прямого доступа к диску для чтения;

— разрешение прямого доступа к диску для записи;

2) Вспомогательные для механизма идентификации программ:

— компонент имеет 32-х битную и 64-х битную версию (позволяет одним правилом указать, что исключение относится и к версии программы, расположенной в директории System32, и к версии из директории SysWOW64);

— подтверждение по электронной подписи (позволяет указать, что действие разрешается для программы, исполняемый файл которой подписан любой валидной электронной подписью; для указания конкретного издателя необходимо использовать поле «Издатель ЭП» (при этом устанавливать флаг не обязательно, его наличие подразумевается автоматически));

— антивирусный компонент;

3) Управляющие потоком телеметрии (позволяют для указанного процесса исключать из потока события указанного типа или разрешают отправку всех событий процессов, даже при включенной опции их подавления в профиле безопасности агента):

— исключение из телеметрии сетевых событий;

— исключение из телеметрии файловых событий;

— исключение из телеметрии событий реестра Windows;

— исключение из телеметрии событий поведения;

— исключение всей телеметрии;

— запрет принудительного подавления событий;

4) Управляющие потоком аналитической активности (позволяют для указанного процесса исключить из потока события указанного типа, связанные со сработками аналитических правил):

— исключение анализа файловой активности;

— исключение анализа входящей сетевой активности;

— исключение анализа исходящей сетевой активности;

— исключение матчинга индикаторов атак.

Совет

Чтобы не создавалось событие сработки исключения для того или иного индикатора атак, необходимо указать имя этого индикатора в строке **Правила**, поставив перед ним знак минус.

В случае с файловой активностью для заданной программы будут исключены проверки по индикаторам компрометации и YARA-правилам/ML, если режим сканирования по YARA-правилам и ML включен для соответствующего профиля. В этом же случае будут исключены проверки хешей на TI-платформе. Для сетевой активности запрет аналитики для заданной программы отменяет проверку по индикаторам компрометации (IP, URL, домены, сетевые сигнатуры), соответственно, на TI-платформе проверка по IP-адресам, доменам и URL также будет отключена. Исключение матчинга индикаторов атак для заданной программы позволяет отменить для нее проверки по всем индикаторам атак, назначенным в конфигурации правил агента(ов).

Все установленные для добавляемого исключения флаги будут отображаться в таблице **Исключения для программ** в поле **Флаги**.

Издатель ЭП – в поле прописывается имя издателя электронной подписи для исполняемого файла. После добавления исключения имя издателя отобразится в таблице **Исключения для программ** в поле **Издатель ЭП**. Добавление издателя электронной подписи к любому из доступных способов идентификации значительно повышает его безопасность.

Правила – в поле прописывается название правила индикации, работу которого требуется подавить с помощью исключения (например, «CmdLineTampering»). Правила «MaliciousFile», «SuspiciousFile», «MaliciousDomain», «SuspiciousDomain», «MaliciousIP», «SuspiciousIP», «MLStaticDetection» относятся к срабатываниям на основе анализа содержимого файлов и подавляться должны с помощью файловых исключений. Сюда же относятся обнаружения на основе YARA-сигнатур, но имена таких правил указываются в

метаданных YARA-сигнатуры, т.е. они не фиксированы. YARA-сигнатуры фигурируют в рамках единственного события файлового монитора – **Обнаружение: Файл классифицирован как вредоносный (YARA-правила)**.

Комментарий – в поле прописывается произвольный комментарий. Для добавления новой программы-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром. Комментарий после добавления исключения будет отображаться в таблице **Исключения для программ** в поле **Комментарий**.

Чтобы завершить добавление исключения для программы необходимо после ввода всей необходимой информации в окне **Добавить исключение** нажать кнопку **Добавить**.

Для внесения изменений в исключение для программы аналитику следует нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключения для программ** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

В зависимости от типа исключения, которое можно увидеть в поле **Тип** в таблице **Исключения для программ**, окно **Редактировать исключение** (рис. 80, 81, 82) будет содержать разный набор полей, соответствующий набору полей окна **Добавить исключение**.

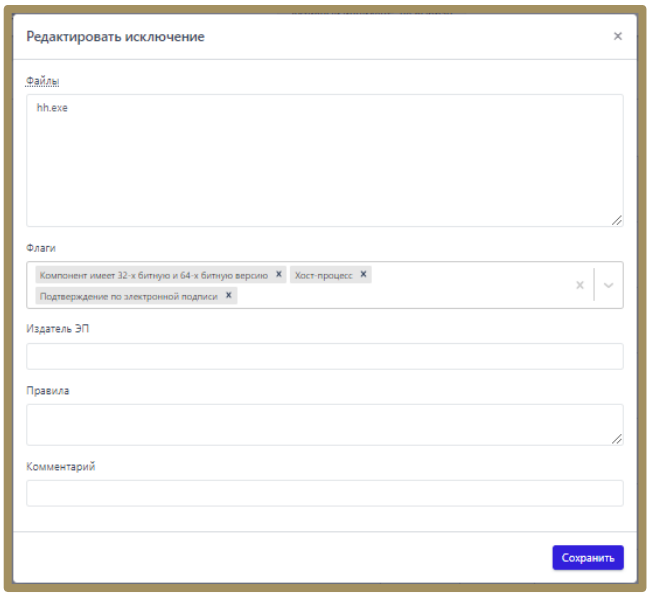


Рисунок 80 – Редактировать исключение для программы (файл)

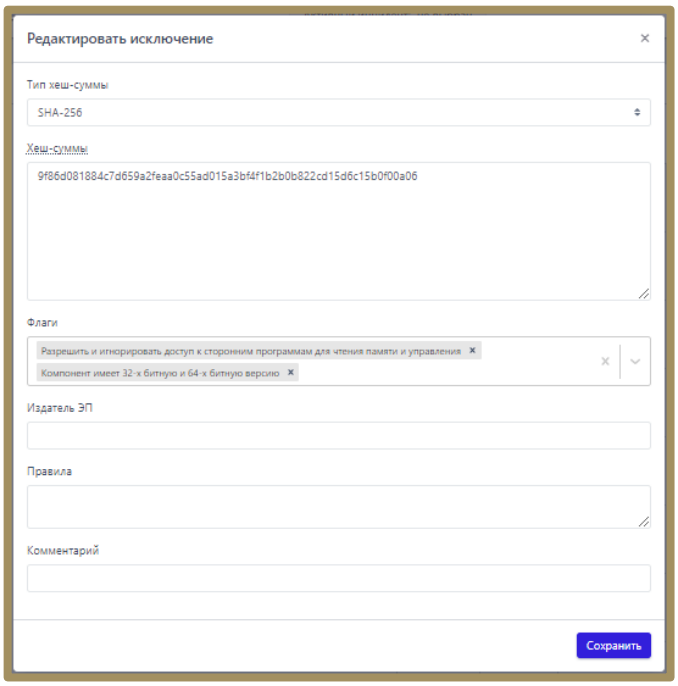


Рисунок 81 – Редактировать исключение для программы (хеш)

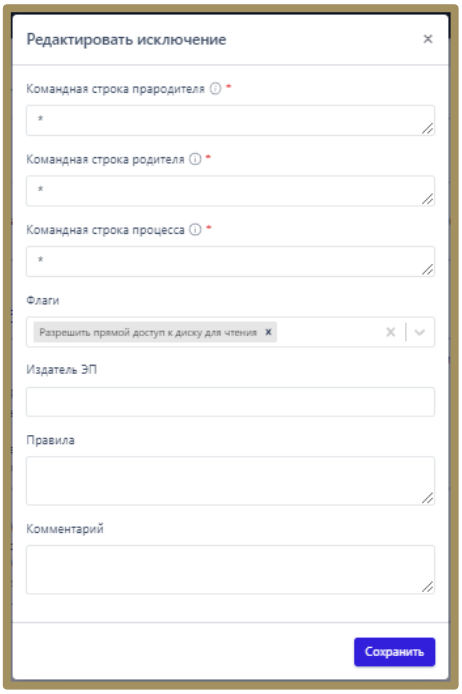


Рисунок 82 – Редактировать исключение для программы (командная строка)

Для завершения редактирования необходимо нажать кнопку Сохранить после внесения изменений в редактируемый элемент. Для отмены изменений следует нажать кнопку закрытия окна ✕.

После добавления программы в список исключений и сохранения набора с добавленным исключением необходимо применить этот набор для соответствующего агента или агентов. Для этого следует

перейти на страницу **Настройка агента**, выбрать нужного агента из списка и в области **Конфигурации** применить измененный набор исключений для программ (рис. 83).

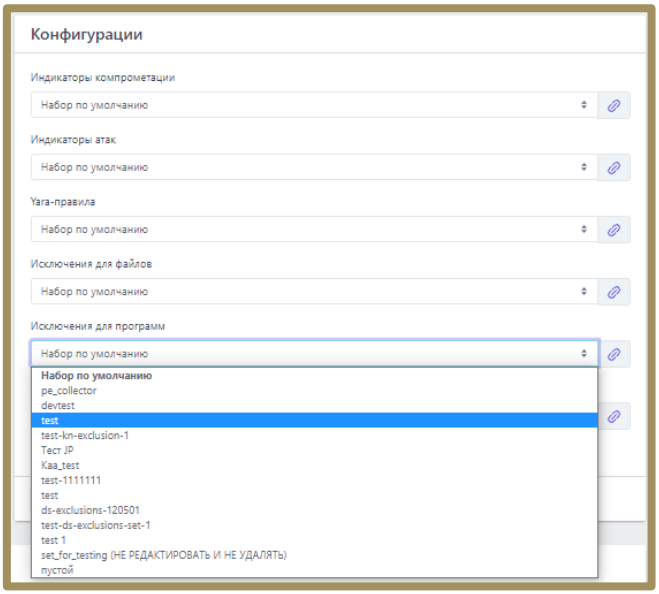


Рисунок 83 – Изменение конфигурации правил на агенте

Правило с добавленным исключением будет применяться для выбранного агента после применения конфигурации, для этого аналитику необходимо нажать кнопку Применить конфигурацию. Если требуется применить конфигурацию с исключением сразу на несколько агентов, то для этого следует перейти на страницу **Список агентов**, отметить флажком агентов, для которых нужно применить исключение, и с помощью кнопки **Применить конфигурацию** ( ) назначить сохраненную ранее конфигурацию с исключением.

Следует также рассмотреть сценарий, когда с помощью управляющих флагов (**Разрешить внедрение кода в сторонние программы**, **Разрешить запись памяти сторонних программ**, **Разрешить доступ к сторонним программам для чтения памяти и управления**, **Право взаимодействия с критическими системными программами**, **Разрешить прямой доступ к диску для чтения**, **Разрешить прямой доступ к диску для записи**) необходимо разрешить определенное действие для хост-процессов.

К таким процессам в системе RT Protect EDR относятся:

– svchost.exe;

– rundll32.exe;

– dllhost.exe;

– taskhostw.exe;

– taskhost.exe.

Если действие, которое требуется разрешить, совершается самим этим процессом (инициатором соответствующего вызова является исполняемый модуль этого процесса), то все сказанное ранее про составление правила исключения остается справедливым. Если же действие совершается от имени определенной DLL, запускаемой с помощью хост-процесса, то в качестве правила идентификации должны использоваться либо имя, либо хеш этой DLL (инициатора операции).

10.7.4. Добавление исключений для файла с помощью мастера исключений

Добавлять исключения для файлов, обнаруживаемых на агентах, в Программе можно в автоматизированном режиме с помощью мастера исключений. Создание исключений для файла предусмотрено для следующих типов обнаружений (соответствуют названию правила, на основе которого событие попало в инцидент):

1) SuspiciousFile;
2) MaliciousFile;
3) MLStaticDetection;
4) Срабатывание YARA-правила;
5) Срабатывание индикатора компрометации для файла.

Тем самым, создавая исключение, аналитик разрешает работу файла, несмотря на то, что статический анализ этого файла показывает потенциальную опасность для защищаемой инфраструктуры, это дает возможность аналитику быстро подавлять ложноположительные срабатывания.

Мастер исключений доступен на странице **Инцидент** в поле **Информация** события, включенного в инцидент, или на странице **Активность** также в поле **Информация**.

Чтобы добавить обнаруженный файл в исключения, необходимо нажать кнопку **Ложное срабатывание** ( ), после чего откроется окно **Мастер создания исключений**. Здесь аналитику необходимо предпринять несколько шагов:

1) Выбрать тип создаваемого исключения (хеш или файл);

2) Выбрать набор с исключениями (по умолчанию выбирается действующий набор с исключениями того агента, на котором возник инцидент);

3) Выбрать действие (по умолчанию выбирается действие **Разрешить**);

4) Написать комментарий (если это необходимо);

5) Нажать кнопку **Добавить**.

После завершения операции произойдет автоматический переход на страницу **Исключения для файлов** в тот набор, в котором было добавлено исключение.

В некоторых случаях аналитику вместо разрешающего исключения может понадобиться создать запрещающее исключение. От индикатора компрометации оно будет отличаться тем, что по такому событию инцидент создаваться не будет. Для создания блокирующего исключения необходимо вместо действия **Разрешить** выбрать в мастере исключений действие **Блокировать**.

10.7.5. Добавление исключений для программ в режиме мастера исключений

Подобно добавлению файлов в режиме мастера исключений программные исключения также можно добавлять с помощью мастера со страницы **Активность**. Использование мастера исключений для программ возможно для событий-обнаружений, у которых заполнено поле **rul**, кроме событий-обнаружений следующих типов:

– события-обнаружения файлового монитора с подтипами **Срабатывание индикатора компрометации для файла**, **Файл классифицирован как вредоносный (ML на агенте)** и **Файл классифицирован как вредоносный (YARA-правила)**;

– события-обнаружения сетевого монитора с подтипом **Срабатывание индикатора компрометации**;

– события-обнаружения, у которых поле **rul** равно **SuspiciousFile**, **MaliciousFile**, **SuspiciousDomain**, **MaliciousDomain**, **SuspiciousIp**, **MaliciousIp**.

При обнаружении соответствующих событий на странице **Активность** в поле **Информация** появляется кнопка **Исключить как ложное срабатывание** ( ). При нажатии кнопки открывается окно **Мастер создания исключения для программ** со следующими полями:

1) Тип создаваемого исключения;

2) Командная строка прародителя;

3) Командная строка родителя;

4) Командная строка процесса;

5) Издатель ЭП;

6) Правило (rul);

7) Комментарий;

8) Набор.

На этом этапе можно поменять тип создаваемого исключения с командной строки на файл. Обязательным для выбора является назначение набора с исключениями, при этом необходимо учитывать, что во внешние наборы сохранить исключение нельзя. При выборе типа исключения **Файл** набор полей изменится на следующие:

1) Тип создаваемого подключения;

2) Файл (содержит полное имя файла);

3) Правило;

4) Комментарий (заполняется автоматически командной строкой процесса);

5) Набор.

После выбора типа создаваемого подключения и набора необходимо нажать кнопку **Далее**. Откроется окно **Добавить исключение**. На этом этапе можно установить флаги, согласно которым будут исполняться файлы, добавленные в список исключений для программ, а также изменить информацию в остальных полях (**Правила**, **Коммментарий** и т.д.). Для завершения операции необходимо нажать кнопку **Добавить**.

10.8 Добавление сетевых исключений

10.8.1. Общая информация

Сетевые исключения — это элементы Программы, позволяющие управлять списками глобальных и локальных IP-адресов и доменов с помощью переопределения логики событий, то есть разрешая или блокируя доступ к IP-адресам или доменам.

Важно

Блокирование сетевого соединения происходит на транспортном уровне.

Аналитик может задавать артефакты «черного» и «белого списков», где в «черный» список будут входить запрещенные IP-адреса, URL-адреса или домены, а в «белый» список разрешенные, доступ к которым разрешается даже при наличии индикаторов компрометации или данных TI-платформы с вердиктом «Вредоносный». То есть использование сетевых исключений как элементов «белого списка» позволяет подавлять сетевые срабатывания TI-платформы или индикаторов и снижать количество анализируемой системой информации, так как при сетевом взаимодействии с элементами «белого списка» агент не анализирует данные потока (не производит матчинг сетевых сигнатур).

Блокирующие сетевые исключения («черный» список) позволяют ограничивать доступ к сетевым ресурсам без создания инцидентов.

На странице **Наборы сетевых исключений** представлены имена наборов исключений, в которых указываются IP-адреса, URL-адреса и доменные имена в качестве идентификаторов при создании исключений. Предусмотрены следующие действия при создании сетевых исключений для взаимодействия с перечисленными выше артефактами: **Блокировать, Разрешить (всегда)**, **Продолжение наблюдения**, **Разрешить (кроме изоляции)**.

Важно

Тип артефакта **URL** поддерживается не всеми версиями агента.

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

– **Блокировать** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем блокируется, при этом (в отличие от действия **Блокировать** в индикаторах), не создается событий с критичностью **Средняя** или выше, которые необходимы для создания инцидента, создается событие с критичностью **Низкая**;

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

— **Продолжение наблюдения** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем разрешается, при этом связанные с артефактом события создаваться и отправляться на сервер не будут);

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

10.8.2. Добавление сетевых исключений с помощью мастера исключений

Сетевые исключения могут быть добавлены со страниц **Активность** или **Инцидент** с помощью мастера исключений. Принцип его работы не отличается от создания файловых исключений: при нажатии кнопки  открывается окно **Мастер создания сетевых исключений** с предзаполненными полями, в котором аналитик может изменить набор, куда будет сохранено исключение. После нажатия кнопки **Далее** открывается второе окно **Добавить исключение**, в котором необходимо выбрать одно из доступных для сетевых исключений действий в сочетании с опцией отправки событий. Опция позволяет оптимизировать отправку событий, связанных со статическими проверками домена, URL-адреса или IP-адреса (проверка по индикаторам компрометации). Некоторые сочетания действий и опции являются невозможными:

— действие **Блокировать** и включенная опция **Не отправлять события**;

— действие **Продолжать наблюдение** и отключенная опция **Не отправлять события**.

Создать сетевое исключение возможно для следующих типов событий:

— события-обнаружения сетевого монитора с подтипом **Срабатывание индикатора компрометации**;

— события-обнаружения сетевого монитора с подтипом **Исходящее подключение** и **Входящее подключение**, у которых в поле rul указано **SuspiciousIp** или **MaliciousIp**;

— события-обнаружения сетевого монитора с подтипом **Исходящее подключение**, **Входящее подключение**, **SSL HELLO**, **DNS-запрос**, у которых в поле **rul** указано **SuspiciousDomain** или **MaliciousDomain**.

10.8.3. Наборы сетевых исключений

Страница **Наборы сетевых исключений** включает в себя следующие структурные элементы (рис. 84):

— таблица с наборами сетевых исключений;

— кнопка **Добавить набор**;

— кнопка **Применить набор**;

— кнопка **Удалить выбранные наборы**.

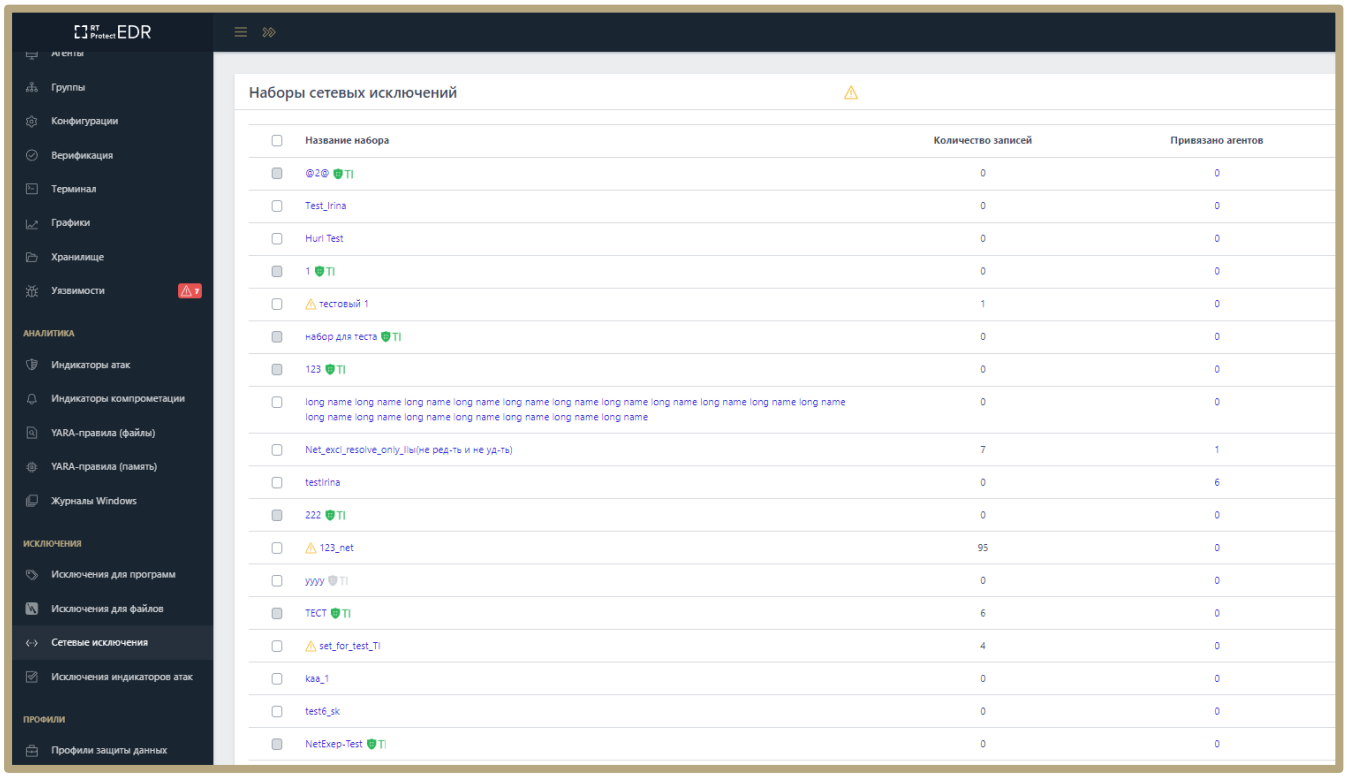


Рисунок 84 – Страница «Наборы сетевых исключений»

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. На этом этапе можно добавить к новому набору исключения для файлов из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Для завершения операции необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Сетевые исключения** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

10.8.4. Страница «Сетевые исключения»

На странице **Сетевые исключения** можно выполнять следующие операции:

— просматривать сетевые исключения в выбранном наборе;

— добавлять новое исключение по IP-адресу;

— добавлять новое исключение по доменному имени;

— применять изменения в наборе исключений;

— копировать/перемещать выбранные исключения из одного набора в другой;

— экспортировать набор с исключениями в файл;

— импортировать исключения из файла в набор;

— активировать/деактивировать исключения в наборе;

— редактировать исключение;

— удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения. При добавлении исключения необходимо обратить внимание на флаг **Не отправлять события**, который позволяет включить или отключить функцию отправки событий, связанных с доменом, URL или IP-адресом. При этом в комбинациях, предусмотренных для артефактов и флага **Не отправлять события** есть недопустимые комбинации: действие **Блокировать** и включенная опция **Не отправлять события**, действие **Продолжение наблюдения** и отключенная опция **Не отправлять события**.

Важно

Домен и IP-адрес могут быть написаны в исключении вместе с портом (<IP/домен>:<порт>)

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

В поле **Значение** таблицы с сетевыми исключениями отображается элемент , который позволяет скопировать IP-адрес, URL-адрес или доменное имя в буфер обмена.

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

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ).

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

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

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

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

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

При добавлении/редактировании исключения, если в обязательном для заполнения поле было введено не валидное значение, появляется надпись о некорректно введенном значении (IP-адреса или доменного имени) и исключение не будет создано. Данное утверждение представлено на рисунке 85.

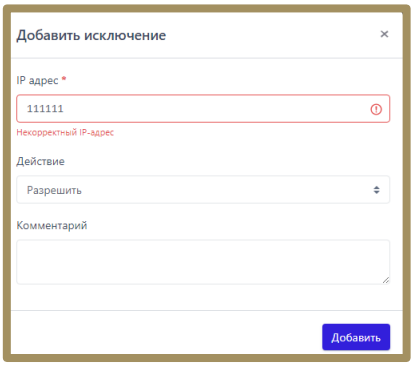


Рисунок 85 – Ввод некорректных параметров при добавлении исключения

10.9 Добавление исключений индикаторов атак

10.9.1. Общая информация

Исключения индикаторов атак – это программные элементы, позволяющие переопределить логику индикаторов атак, то есть исключить блокирующее или детектирующее действие при совпадении с условием исключения.

Исключение работает по имени и типу индикатора, к условию которого добавляется условие исключения, поэтому важно указывать правильные имя и тип индикатора атак. То есть, иными словами, имя и тип исключения индикаторов атак должны соответствовать имени и типу исключаемого индикатора.

В Программе предусмотрена возможность исключать группу индикаторов атак подстановкой символа *, например, soc_indicator* будет применяться для всех правил, в имени которых содержится часть soc_indicator. Кроме подстановочного знака * (любые символы или их отсутствие) в работе с исключениями для индикаторов атак может использоваться знак **?** (один любой символ).

Исключения можно создавать только для индикаторов атак, созданных в режиме **Обычный**.

10.9.2. Наборы исключений индикаторов атак

Страница **Наборы исключений индикаторов атак** включает в себя следующие структурные элементы (рис. 84):

— таблица с наборами исключений для индикаторов атак;

— кнопка **Добавить набор**;

— кнопка **Применить набор**;

— кнопка **Удалить выбранные наборы**.

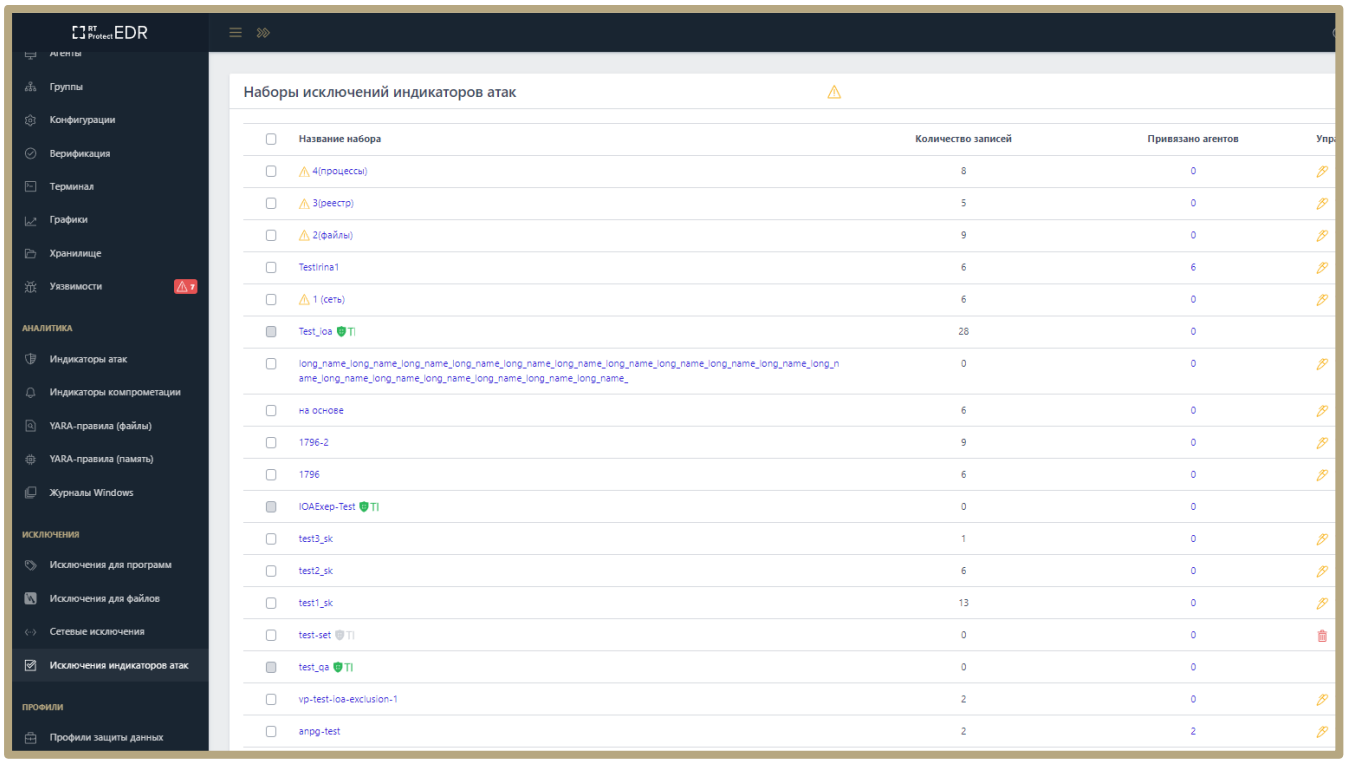


Рисунок 86 – Страница «Наборы исключений индикаторов атак»

Чтобы добавить новый набор с исключениями для индикаторов атак, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. На этом этапе можно добавить к новому набору исключения из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор.** Чтобы завершить операцию, необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

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

10.9.3. Страница «Исключения индикаторов атак»

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

— просматривать исключения индикаторов атак в выбранном наборе;

— добавлять новое исключение индикатора атак;

— применять изменения в наборе исключений;

— копировать/перемещать выбранные исключения из одного набора в другой;

— экспортировать набор с исключениями в файл;

— импортировать исключения из файла в набор;

— активировать/деактивировать исключения в наборе;

— редактировать исключение;

— удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения. Добавить условие исключения индикатора атак можно как вручную, так и с помощью конструктора. Также, как и для индикаторов атак, в исключениях для них доступна функция проверки синтаксиса.

Важно

При заполнении поля ***Тип индикатора атаки*** можно выбрать параметр **Универсальный тип индикатора**. При выборе данного параметра исключение будет действовать для всех типов индикаторов атак.

В списке исключений индикаторов атак в наборе тип исключения, созданного для универсального типа индикатора, будет отображаться как **Универсальный**.

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

.

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

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ). Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

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

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

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

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

10.10 Особенности работы Программы с антивирусными средствами сторонних производителей

10.10.1. Срабатывание антивирусных средств при работе с веб-приложением RT Protect EDR

Срабатывание антивирусных средств при работе с веб-приложением EDR возникает в том случае, если в данных, получаемых фронтендом от сервера (в основном они приходят в формате JSON) содержится какая-то информация, которую антивирусное средство распознает как потенциально опасную. Это может быть хеш, имя файла, командная строка и т.д. (ниже такие информационные фрагменты называются артефактами).

Список экранов приложения, где высока вероятность срабатывания антивирусных средств:

— **Инциденты**, **Инцидент** (incidents, incident): внутри инцидентов могут содержаться артефакты;

— (!) любой экран (edr/*): в оповещении о новом инциденте содержится информация об инциденте (всплывающие нотификации в правом верхнем углу);

— **Активность** (events): внутри событий могут содержаться артефакты;

— **Оповещения** (user-messages): внутри оповещений содержится информация об инцидентах;

— **Процессы и модули** (modules): внутри событий могут содержаться артефакты;

— **Процесс** (process): в информации о процессе могут содержаться артефакты;

— **Журнал** (users-actions): в событиях журнала могут содержаться артефакты (внутри инцидентов и тд);

— отчет TI-платформы (ti): в отчете могут содержаться артефакты.

Список экранов приложения, где вероятность срабатывания ниже:

— **Уязвимости** (vuln): в информации об уязвимостях могут содержаться артефакты;

— **Хранилище** (storage): файлы могут определяться как вредоносные;

— **Агенты**, **Агент** (agents): из-за виджета сканера уязвимостей на экране **Агент**;

— **Терминал** (terminal): внутри команд могут содержаться артефакты;

— **Главная страница** (dashboard): в некоторых местах могут быть артефакты (например, топ-10 модулей);

— экраны наборов и элементов (config-set, config-item): внутри элементов наборов могут содержаться артефакты.

Список экранов приложения, где вероятность срабатывания можно считать нулевой:

— **Администрирование** (administration);

— **Профиль пользователя** (user-profile);

— **Группы** (groups);

— **Верификация** (verification);

— **Графики** (charts);

— **Дистрибутивы** (distributions);

— **Лицензия** (license);

— экраны профилей (profile);

— экраны множеств профилей и наборов (profiles, config-sets);

— экран сброса пароля (reset-password).

Важно

Таким образом, для полного исключения ложных срабатываний антивирусных средств при работе с веб-приложением EDR целесообразно добавить в исключения соответствующий домен/адрес полностью: <host/IP>/*.

10.10.2. Особенности выполнения действия блокирования для антивирусных решений.

В некоторых случаях к заблокированному модулю процесса может обращаться антивирусное средство. Для того, чтобы это было возможно, в Программе предусмотрено внутреннее исключение, которое создает событие для подобного обращения. То есть, если событие блокирования возникает в контексте антивирусного процесса (такие процессы отмечаются в системе флагом AVEngine), то блокирующее действие переопределяется на **Продолжать наблюдение** и критичность события сбрасывается на уровень **Информация**, при этом в причине события указывается **Исключение для программ**. Такая логика характерна для всех аналитических правил, кроме файловых исключений.

10.11 Операции со списком агентов

На странице **Агенты** пользователь Программы может выполнить следующие действия:

— скачать список агентов в формате CSV;

— фильтровать агентов с помощью фильтров, представленных на странице;

— добавить агентов в существующую или вновь создаваемую группу;

— применить конфигурацию с аналитическими наборами или профилями на выбранных агентах;

— изолировать выбранных агентов или отменить изоляцию ранее изолированных агентов;

— отключить или включить автоматическое обновление выбранных агентов;

— включить или отключить защиту выбранных агентов (защитные функции драйвера будут включены/отключены);

— зафиксировать состав ПО выбранных агентов в качестве золотого образа;

— включить или отключить парольную защиту от удаления агентов;

— отключить отслеживание состава ПО выбранных агентов;

— выполнить команду для выбранных агентов;

— исключить выбранных агентов из определенной группы;

— удалить агентов из модуля администрирования (после удаления агент попадает на повторную верификацию);

— объединять агентов для дальнейшего изучения информации по ним по определенным признакам с помощью DSL-запросов.

Совет

Последнее может быть полезным аналитику, так как позволяет формировать выборки, исходя из сложного условия по активности, происходящей на агентах, например, DSL-запрос «sha256:x» покажет список агентов, на которых произошли события с указанным хешем x (поле sha256 события).

Также в качестве примера можно привести следующие выборки (рис. 87).

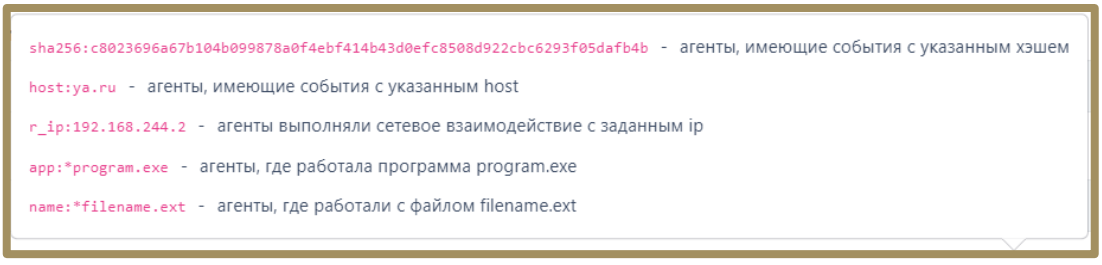


Рисунок 87 – Запросы DSL на странице «Агенты»

В результате отправки запроса формируется список агентов, на которых присутствует активность, соответствующая запросу. Это позволяет обнаруживать аномальную активность на агентах, определять, каких агентов затронули те или иные события или действия, выполнять команды для определенной группы агентов, для которой задан фильтр с помощью DSL-запроса.

Введенный DSL-запрос создает выборку над базой событий, из которой делается агрегация агентов, подлежащих отображению. При этом в поле **События** выборки по запросу пользователь может увидеть, сколько событий, соответствующих запросу, произошло на агенте. Нажимая на ссылку с количеством событий в поле **Совпадения по DSL**, пользователь сразу перейдет на страницу **Активность** с соответствующей фильтрацией по имени агента, DSL-запросом, а также трехмесячным периодом регистрации событий. Подробная информация о DSL-запросах приведена в подразделе 10.19.

Чтобы добавить выбранных агентов в группу, необходимо отметить флажками нужных агентов и с помощью кнопки **Добавить в группу** выполнить одну из предложенных операций: добавить агентов в выбранную группу или добавить их во вновь создаваемую группу. Команда особенно полезна, когда требуется объединить большое количество агентов по определенному признаку в группу, чтобы в дальнейшем применять групповые команды. То есть сначала с помощью настройки фильтров, например, отфильтровав всех агентов по домену, необходимо сформировать группы, к которым будут применяться команды, а потом уже применять различные команды для этих групп.

Чтобы применить конфигурацию с набором для определенных агентов, необходимо выбрать их, отметив флажками, после чего нажать кнопку **Применить конфигурацию** (). Откроется окно **Выбор набора**, в котором нужно выбрать соответствующие наборы правил, исключений или профили, после чего нажать кнопку **Сохранить**. Выбранные наборы появятся в таблице с агентами в поле **Конфигурации**.

Чтобы изолировать агентов, необходимо отметить их флажками, после чего нажать кнопку **Изолировать выбранных агентов** (), далее ввести произвольный комментарий в окне **Переход к изоляции агентов** и нажать кнопку **Отправить**. Изоляция агентов может эффективно работать в связке с DSL-запросом, например, когда известна информация о компрометации одного агента, то с помощью запроса можно определить, на каких еще агентах в сети был замечен артефакт компрометации и тут же изолировать скомпрометированные машины.

Для отмены изоляции необходимо отметить флажками выбранных агентов, после чего нажать кнопку **Отменить изоляцию выбранных агентов** () и подтвердить операцию в открывшемся окне, нажав кнопку **Выполнить**.

Чтобы отключить автоматическое обновление для выбранных агентов, необходимо отметить их флажками и нажать кнопку **Отключить автоматическое обновление выбранных агентов** (), после

чего подтвердить выбранную операцию, нажав кнопку **Выполнить**. Для включения автоматического обновления необходимо отметить агентов флажками, после чего нажать кнопку **Включить автоматическое обновление выбранных агентов** () и подтвердить операцию, нажав кнопку **Выполнить**.

Чтобы включить защиту на агенте, необходимо отметить его флажком и нажать кнопку **Включить защиту выбранных агентов** (), после чего подтвердить операцию в открывшемся окне. При отключенной защите агент не блокирует действия, которые EDR считает опасными или потенциально опасными.

Чтобы отключить защиту на агенте, необходимо отметить его флажком и нажать кнопку **Отключить защиту выбранных агентов** (), после чего подтвердить операцию в открывшемся окне.

Важно

Отключение защиты на агентах приводит к выгрузке драйвера, поэтому события любых источников, кроме событий журналов Windows и производных от них, перестанут поступать на сервер для таких агентов.

Чтобы зафиксировать списки ПО на выбранных агентах (создать золотой образ), необходимо отметить агентов флажками и нажать кнопку **Зафиксировать состав ПО выбранных агентов в качестве золотого образа** (), после чего подтвердить операцию в открывшемся окне.

Примечание

Любое изменение состава ПО на таких агентах будет отмечено специальным значком (), который означает, что на агенте появились новые программы, не зафиксированные в составе ПО золотого образа. Просмотреть, что именно изменилось, можно после перехода на страницу **Агент** выбранного агента. Агенты с созданным золотым образом, состав ПО которых не менялся, будут отмечены значком  .

Чтобы отменить отслеживание состава ПО на агентах, необходимо отметить их флажками и нажать кнопку **Отключить отслеживание состава ПО выбранных агентов золотому образу** (), после чего подтвердить операцию в открывшемся окне. Информация об изменениях состава ПО для таких агентов перестанет отображаться на сервере управления.

Чтобы включить защиту от удаления для выбранных агентов, необходимо отметить их флажками и нажать кнопку **Включить защиту от удаления для выбранных агентов** (), после чего откроется окно **Включение защиты от удаления агентов**. Далее необходимо задать пароль и нажать кнопку **Отправить**. Удаление агента с компьютера, на котором он установлен, после завершения операции будет возможно только после ввода пароля. Чтобы увидеть и при необходимости скопировать пароль (токен удаления) необходимо перейти на страницу удаляемого агента. Токен будет показан аналитику при наведении курсора на значок  . Пароль для удаления будет установлен для выбранных агентов вне зависимости от того, устанавливался ли на одном или нескольких агентах пароль ранее, в таком случае пароль будет просто перезаписан.

Чтобы отключить защиту от удаления для выбранных агентов, необходимо отметить их флажками и нажать кнопку **Отключить защиту от удаления для выбранных агентов** (), после чего подтвердить операцию в открывшемся окне. Требование о вводе пароля при удалении агента будет снято.

Аналитик может выполнить команды терминала на нескольких агентах одновременно, например, чтобы распространить какой-либо скрипт в пределах агентской сети или ее части с помощью команды **put**. Для выполнения команды необходимо отметить флажками агентов, после чего нажать кнопку **Выполнить команду на выбранных агентах** (). В открывшемся окне ввести соответствующую команду и нажать кнопку **Отправить**, после чего подтвердить операцию.

Чтобы исключить агента из группы, необходимо отметить флажками агентов, состоящих в группе, после чего нажать кнопку **Исключить из группы**. Далее следует подтвердить операцию в открывшемся окне.

В таблице аналитик может выбрать произвольное количество агентов для проведения операций с ними, в том числе всех агентов на странице или всех агентов выборки. Чтобы выбрать всех агентов на странице, аналитику необходимо поставить флаг для кнопки выбора в первом столбце таблицы ().

Совет

Если требуется отметить всех агентов, показанных на всех страницах, то необходимо перевести переключатель **Выбрать все элементы** во включенное положение (). При этом переход на другую страницу переводит переключатель в выключенное положение.

Для удаления агентов необходимо отметить их флажками и нажать кнопку **Удалить выбранные**, после чего подтвердить операцию в открывшемся окне. Удаленные агенты не удаляются из системы полностью, а попадают на повторную верификацию.

Аналитик может фильтровать информацию на странице **Агенты** по следующим полям фильтрации (рис. 88):

1) Показывать по;
2) Активность;
3) Имя агента;
4) Группа;
5) Агент;
6) Имя агента;
7) Сетевой адрес;
8) Операционная система;
9) Имя компьютера;
10) Домен;
11) Автоматическое обновление;
12) Изоляция;
13) Защита агента;
14) Платформа;
15) Запрос на языке DSL;
16) Поля для фильтрации.

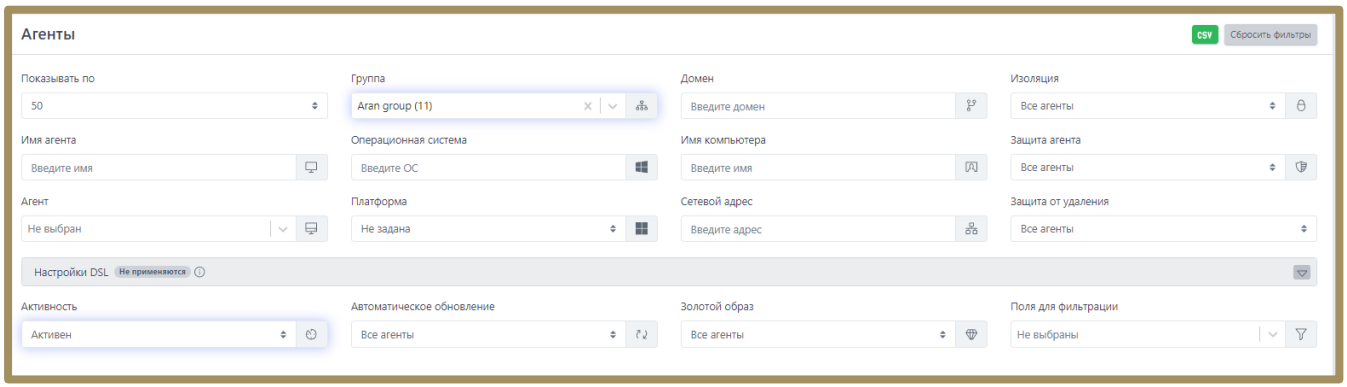


Рисунок 88 – Поля фильтрации в области «Агенты»

Показывать по – фильтр устанавливает количество событий, которые отображаются на странице в таблице. Возможно выбрать отображение по 10, 20, 50 или 100 событий.

Активность – при выборе одного из значений фильтра (**Все агенты**/**Активен**/**Не активен**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению.

Имя агента – фильтрует агентов по имени, которое было присвоено им при регистрации в Программе.

Группа – фильтрует агентов по названию группы, к которой они принадлежат.

Сетевой адрес – фильтрует агентов по вводимому в поле фильтра сетевому адресу.

Операционная система – фильтрует агентов по установленной на них операционной системе.

Имя компьютера – фильтрует агентов по именам компьютеров, на которых установлены зарегистрированные в Программе агенты.

Домен – фильтрует агентов по имени домена, к которому принадлежат компьютеры, на которых установлены зарегистрированные в Программе агенты.

Автоматическое обновление – фильтрует агентов по признаку включенного или выключенного автоматического обновления.

Изоляция – при выборе одного из значений фильтра (**Все агенты**/**Изолирован**/**Не изолирован**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению

Защита агента – фильтрует агентов в соответствии с тем, включена на них защита или нет.

Платформа – фильтрует агентов в соответствии с выбранной операционной системой: Windows, Linux или MacOS.

Поля для фильтрации – при выборе значений в фильтре **Поля для фильтрации** на страницу дополнительно могут быть добавлены следующие фильтры: **Опция /NO_DRIVER**, **Проблемный**, **Часовой пояс**,

Конфигурация, **Исключения для файлов**, **Исключения для программ**, **Индикаторы компрометации**, **Журналы Windows**, **YARA-правила**, **Индикаторы атак**, **Профили защиты данных**, **Профили безопасности агента** (см. рис. 89).

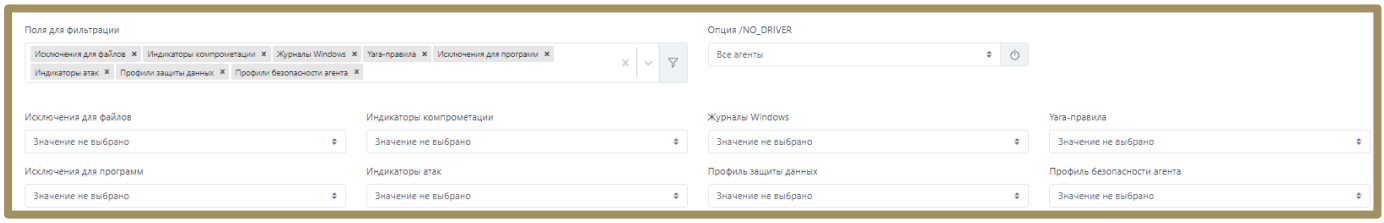


Рисунок 89 – Дополнительные поля фильтрации в области «Агенты»

Опция /NO_DRIVER – позволяет фильтровать агентов в соответствии с тем, включен ли драйвер на агенте или нет (для агента с установленной опцией NO_DRIVER отсутствует возможность переводить машину с агентом в изоляцию, а также отсутствует защита, то есть правила индикации атак, срабатывание индикаторов компрометации не приводят к завершениям процессов, запрету тех или иных действий потенциально опасных программ и т.д.). Защиту агента при выключенном драйвере также, как и изоляцию, невозможно включить.

Проблемный – фильтрует агентов по наличию на них проблем (например, некорректное время на агенте) или их отсутствию.

Часовой пояс – фильтрует агентов по определенному часовому поясу в различных форматах часовых поясов: EST, GMT, UTC и др.

Конфигурация – при выборе одного из значений фильтра (**Все агенты**/**Заданы не все настройки**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению. В случае, если выбрано значение **Заданы не все настройки**, то в таблице отображаются агенты с ненастроенными наборами и профилями.

Исключения для файлов – фильтрует агентов по названию выбранного в поле фильтра набора исключений для файлов. В таблице будут представлены только агенты, привязанные к этому набору.

Исключения для программ – фильтрует агентов по названию выбранного в поле фильтра набора исключения для программ. В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация об исключениях для программ содержится в пункте 10.7.3.

Индикаторы компрометации – фильтрует агентов по названию выбранного в поле фильтра набора индикаторов компрометации. В таблице будут представлены только агенты, привязанные к этому набору.

Журналы Windows – фильтрует агентов по названию выбранного в поле фильтра набора журналов Windows. В таблице будут представлены только агенты, привязанные к этому набору.

YARA-правила – фильтрует агентов по названию выбранного в поле фильтра набора файловых сигнатур. В таблице будут представлены только агенты, привязанные к этому набору.

Индикаторы атак – фильтрует агентов по названию выбранного в поле фильтра набора индикаторов атак. В таблице будут представлены только агенты, привязанные к этому набору.

Профили защиты данных – фильтрует агентов по названию выбранного в поле фильтра профиля защиты данных. В таблице будут представлены только агенты, привязанные к этому профилю.

Профили безопасности агента – фильтрует агентов по названию выбранного в поле фильтра профиля безопасности агента. В таблице будут представлены только агенты, привязанные к этому профилю.

Запрос на языке DSL представляет собой отдельную область на странице **Агенты**, в которой помимо строки запроса существуют дополнительные строки **Период регистрации**, **Источник события**, **Подтип события**.

10.12 Операции на странице «Агент»

На странице **Агент** аналитик может управлять выбранным агентом и просматривать подробную информацию о его состоянии. Большинство операций, которые аналитик может выполнить для отдельного агента, совпадает с групповыми операциями. Для перехода к странице **Агент** необходимо кликнуть по имени агента в любом разделе Программы, содержащем имена агентов.

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

— просмотреть информацию о выбранном агенте (версия, часовой пояс, имя и т.д);

— просмотреть количество событий и инцидентов на агенте за последнее время и за все время с момента его верификации;

— снять или установить параметр автоматического обновления агента при обновлении дистрибутива агента;

— удалить агента из модуля администрирования;

— изолировать агента;

— включить/выключить защиту на агенте;

— отправить агенту команду через терминал;

— зафиксировать состав ПО агента и отслеживать изменения в составе ПО;

— включить или выключить защиту от удаления агента;

— задать или изменить пароль для удаления агента;

— просмотреть информацию о количестве событий, приходящих с агента в секунду (EPS) на текущий момент и среднее EPS за последнюю неделю;

— просмотреть информацию о системе, в которой установлен агент;

— просмотреть информацию об установленном ПО на машине с агентом;

— просмотреть информацию об установленных драйверах;

— выявить уязвимости установленного ПО;

— назначить или изменить конфигурационные наборы с индикаторами, профилями или исключениями для агента;

— изменить группу, в которую входит агент;

— просмотреть графики, показывающие статистическую информацию по активности системы за последние 15 минут;

— создать отчет об агенте в формате pdf;

— узнать информацию о пяти последних пользователях, вошедших локально или дистанционно на компьютер с установленным агентом (кроме того, показывается и время входа);

— создать текстовое описание агента;

— просмотреть последние 500 событий в журнале агента (провайдера подсистемы ETW).

Важно

Для агентов, у которых установлена опция с выключением драйвера, будет отсутствовать возможность переводить агента в изоляцию и включать защиту.

10.12.1. Изоляция агента

Управление изоляцией агента с помощью интерфейса в модуле администрирования

Изоляция означает отключение сетевого взаимодействия компьютера, на котором установлен агент, от локальной сети и сети Интернет с целью ограничения дальнейшего распространения вредоносных файлов, имеющихся на данном компьютере. Ограничение не распространяется на взаимодействие агента с административным модулем управления.

Изоляцию можно настроить на страницах **Агент** или **Агенты**, при этом на странице **Агенты** можно отправить на изоляцию сразу несколько агентов, предварительно отметив их флажками. На странице **Агенты** изоляция настраивается и снимается с помощью кнопок  и  .

На странице **Агент** изоляция настраивается в области **Управление** с помощью кнопки **Включить изоляцию** (рис. 90).

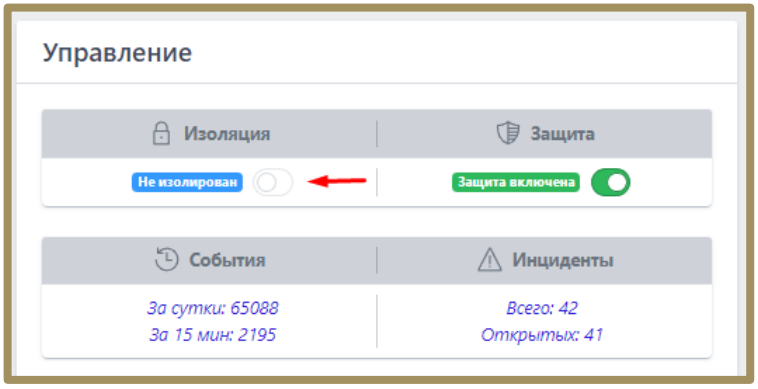


Рисунок 90 – Изоляция агента

После нажатия кнопки появится окно, в котором необходимо ввести комментарий и выполнить операцию **Отправить** (рис. 91).

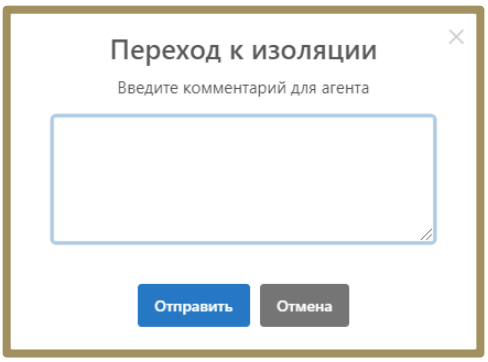


Рисунок 91 – Окно ввода комментария для изолированного агента

Изоляция агента происходит в течение 10 секунд, после чего статус агента в области **Управление** поменяется на Изолирован. На машине агента в этот момент в области уведомлений пользователю придет сообщение о том, что сеть агента изолирована.

Для возврата в штатный режим необходимо нажать кнопку **Отменить изоляцию**. Далее в открывшемся окне **Подтверждение действия** необходимо нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об отправке команды на отмену изоляции. Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна.

Отмена изоляции агента происходит в течение 10 секунд, во время которых статус агента в области **Управление** поменяется на Отмена изоляции, после чего агенту будет возвращен статус Не изолирован, а на машине агента в области уведомлений появится сообщение, что изоляция сети отменена.

Описание механизма реализации функции сетевой изоляции со стороны агента.

Режим сетевой изоляции включается при получении агентом соответствующей команды от сервера управления EDR. С логической точки зрения сетевая изоляция подразумевает невозможность сетевого обмена с агентом (установку новых входящих/исходящих соединений и прием/передачу данных по установленным соединениям), кроме как со стороны сервера управления EDR с целью предотвращения утечки данных, распространения угрозы, связи с серверами управления злоумышленника, а также предотвращения других подобных проявлений при возникновении признаков потенциальной вредоносной активности на агенте.

С технической точки зрения сетевая изоляция распространяется на сетевые слои, начиная с транспортного и выше (согласно модели OSI), при этом также распространяется на ICMP-трафик (ping и др.) и реализуется драйвером агента за счет следующих мер:

1) Блокировка новых исходящих TCP-подключений (исходящий TCP-пакет SYN не отправляется с агентской машины);

2) Блокировка новых входящих TCP-подключений одним из 3-х методов (определяется настройками сетевого модуля агента):

— входящие TCP-пакеты SYN не доставляются до стека TCP/IP агента;

— в ответ на входящие TCP-пакеты SYN агент безальтернативно отправляет TCP-пакет RST;

— соединение устанавливается до момента первой попытки сетевого обмена, при возникновении которой соединение разрывается;

3) Принудительный разрыв соединения при возникновении попыток сетевого обмена (отправка/прием данных) в рамках уже установленных TCP-соединений соответствующая попытка блокируется (пакет не доставляется);

4) Блокировка входящих и исходящих UDP-пакетов (пакеты не доставляются).

Как следует из логики, описанной выше, если на момент включения режима сетевой изоляции TCP-соединение уже было установлено, но обмен данными по нему не происходил во время действия режима сетевой изоляции, то это соединение останется существовать, и после выхода из режима сетевой изоляции данные по нему снова могут беспрепятственно передаваться.

Кроме того, есть ряд исключений в части сетевого обмена, на которые не распространяется сетевая изоляция.

К ним относятся протоколы:

— NETBIOS;

— DHCP (в т.ч. IPv6-версия);

— LLMNR (определяются по TCP/UDP-порту).

Важно

Взаимодействие по указанным выше протоколам не прекращается даже в режиме сетевой изоляции агента, поскольку это критично для функционирования сетевого стека ОС (в частности, Windows).

10.12.2. Возврат к нормальному режиму работы после установки агента в режиме «no_driver»

Для возврата агента, который был установлен с опцией «no_driver», к нормальному режиму работы требуется выполнить следующие действия:

1) В модуле администрирования перейти в раздел **Терминал**;
2) Выбрать агента, которому требуется изменить параметр;
3) Выполнить команду:

– enable;

4) Перейти на страницу агента и убедиться, что опция **Защита агента** включена.

Указанную выше команду можно выполнить для группы агентов на странице **Агенты** с помощью операции **Выполнить команду на выбранных агентах** ().

10.12.3. Отслеживание изменений состава ПО

Во многих случаях изменение состава ПО на компьютерах защищаемой инфраструктуры может сигнализировать о том, что на рассматриваемую систему выполняется установка нежелательных или вредоносных программ. В RT Protect EDR аналитик может создать золотой образ ПО на выбранном агенте, после чего отслеживать изменения состава ПО и установленных драйверов этого агента. Для этого аналитик может воспользоваться кнопкой  (управление золотым образом) на странице **Агент**.

По умолчанию для любого агента в защищаемой инфраструктуре золотой образ имеет статус **Не отслеживается**. Чтобы у аналитика была возможность отслеживать изменения золотого образа, ему необходимо нажать кнопку  и выбрать операцию **Зафиксировать и включить отслеживание**, после чего подтвердить выбранное действие.

После создания золотого образа в списках, представленных в разделах **Обновления системы**, **Установленное ПО** и **Установленные драйверы**, аналитику будут показаны все установленные программы и

драйверы, а также обновления операционной системы, не соответствующие золотому образу. Значок и зачеркнутое наименование элемента означает, что программа была удалена с компьютера с установленным агентом, но при этом присутствует в золотом образе. Значок означает, что программа была установлена на компьютер с агентом, но при этом в золотом образе она отсутствует.

10.12.4. Настройка конфигураций

Для корректной работы конфигурации с исключениями, правилами, или профилями для того или иного агента необходимо назначить для него соответствующую конфигурацию и применить ее после назначения. Аналитические конфигурации могут содержать несколько наборов, например, наборы, получаемые с TI-платформы, и наборы, создаваемые в Программе.

На странице **Агенты** можно назначить конфигурационные наборы или профили для нескольких агентов с помощью кнопки **Применить конфигурацию** ( ), предварительно отметив агентов флажками. После нажатия кнопки необходимо выбрать набор(ы) или профиль, после чего в открывшемся окне выбрать название набора(ов) или профиля, которые будут назначены агентам.

На странице **Агент** назначить конфигурационные наборы и профили для агента можно в области **Конфигурации** (рис. 92).

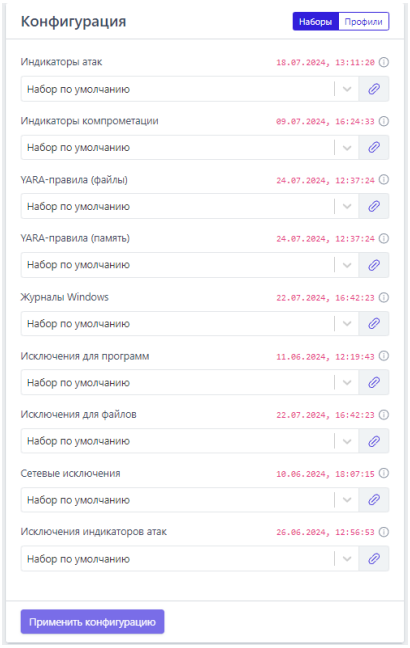


Рисунок 92 – Настройка конфигурации для агента

Конфигурации разделены по двум вкладкам: **Наборы** и **Профили**. Переключаясь между вкладками, можно настроить все необходимые конфигурации правил, исключений и профилей агента. Пустой конфигурация быть не может, в этом случае кнопка **Применить конфигурацию** становится неактивной.

10.12.5. Защита на агенте

Еще одной важной операцией, которая доступна аналитику на страницах **Агент** и **Агенты**, является включение или отключение защиты (рис. 93).

Рисунок 93 – Защита на агенте

Отключение защиты на агенте означает, что будут отключены защитные функции драйвера: не будут работать индикаторы компрометации, индикаторы атак, другие аналитические возможности. При этом агент отправляет статистику и может принимать конфигурационные наборы, а также обрабатывать команды терминала, кроме команд get и stop.

Чтобы отключить защиту необходимо перевести ползунок в области **Защита агента** на странице **Агент** или с помощью кнопки  на странице **Агенты**.

10.12.6. Обновление агента

Обновление агента по умолчанию осуществляется в EDR автоматически. Для управления функцией обновления предусмотрена кнопка на странице **Агент** (рис. 94).

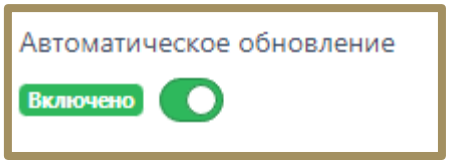


Рисунок 94 – Кнопка обновления агента

Операцию включения/отключения автоматического обновления необходимо подтверждать.

10.12.7. Защита от удаления агента

Режим защиты от удаления агента управляется на странице **Агент** модуля управления EDR. В Программе предусмотрена возможность включения/выключения режима и возможность установки/изменения пароля для удаления агента с конечной точки. После установки пароля удалить агента с помощью стороннего ПО становится невозможно, агент удаляется только с помощью утилиты uninstall.exe из состава дистрибутива агента, при этом какая-либо информация о пароле на машине с установленным агентом отсутствует, ее можно увидеть только на сервере управления EDR.

Защита от удаления агента на странице **Агент** включается ползунком в области **Управление**. Операция требует подтверждения в отдельном окне. Защита от удаления устанавливает на агенте парольную защиту, которая позволит удалить агента только после ввода пароля. Пароль задается аналитиком при включении защиты в отдельном окне, которое появляется после перевода ползунка в состояние **Защита включена**. Длина пароля не должна быть меньше шести знаков. После установки пароля для защиты от удаления агента в строке с ползунком появятся дополнительные значки управления токеном (паролем). Чтобы просмотреть значение токена, необходимо навести курсор мыши на значок  . Скопировать токен для удаления агента можно, нажав значок  . Изменить значение пароля можно, нажав значок  .

При удалении агента, защищенного от удаления паролем, Программа откроет окно, в котором необходимо будет ввести токен, только после этого агент будет удален с компьютера. Это позволит избежать несанкционированного удаления агента с компьютера пользователем этой машины или злоумышленником.

10.12.8. Создание отчета об агенте в формате pdf

Чтобы создать отчет о функционировании агента, аналитику необходимо нажать кнопку **Скачать отчет в PDF** () в области **Агент**. Отчет сохранится в папку **Загрузки**. Отчет может быть представлен в полном или кратком виде.

Отчет содержит различную информацию, связанную с активностью и статистикой работы агента: группа, ОС, версия агента, количество событий на агенте за сутки и за 15 минут, общее количество инцидентов, количество открытых инцидентов, число уязвимых программ на компьютере с установленным агентом и т.д.

10.12.9. Просмотр событий журнала агента

На странице **Агент** аналитику доступен просмотр события службы трассировки Windows для выбранного агента. Аналитик может просмотреть последние 500 событий, для этого ему необходимо раскрыть их список с помощью кнопки  . Список можно фильтровать в соответствии с запросом, введенным в строку **Поиск**.

10.13 Группы

Группировка агентов по определенным признакам, например, по домену, позволит выполнять групповые операции с агентами, для чего нужно будет просто отфильтровать их на странице **Агенты** по определенной группе.

В разделе **Группы** на странице **Группы агентов** можно выполнить следующие операции:

– просмотреть список групп агентов;

– создать новую группу агентов;

– редактировать название группы;

– удалить выбранные группы агентов.

Чтобы создать группу агентов на странице **Группы агентов**, необходимо ввести название в поле **Название группы**, после чего нажать кнопку **Создать группу**.

Для редактирования имени группы можно воспользоваться кнопкой **Редактировать группу** (). Откроется окно, в котором можно изменить название, после чего нажать кнопку **Сохранить изменения**.

Чтобы удалить группу или группы из модуля администрирования, необходимо отметить флажками соответствующие кнопки выбора и нажать кнопку **Удалить выбранные**. После подтверждения операции выбранные группы будут удалены.

При клике по имени группы произойдет переход на страницу **Агенты** с соответствующим предустановленным фильтром по имени группы, то есть в списке будут отображаться все агенты этой группы. На странице **Агенты** аналитик также сможет добавить агентов в группу или исключить агентов из нее (подробнее см. пункт 10.11).

10.14 Конфигурации

Раздел **Конфигурации** содержит настройки наборов и профилей для агентов Windows и Linux, которые агенты получают в момент верификации. Можно настраивать несколько наборов в одной конфигурации. Конфигурации профилей подразумевают действие только одного профиля.

Чтобы назначить выбранные конфигурации, необходимо нажать кнопку **Сохранить**.

Если аналитик настроит не все конфигурации, в верхней части страницы появится значок  , сигнализирующий о том, что заданы не все настройки для наборов и профилей.

10.15 Уязвимости

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

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

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

Примечание

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

Для специалиста, работающего с уязвимостями, важны такие понятия, как инциденты модуля уязвимости и критичность агента. Под инцидентами подразумеваются сущности, возникающие в случае совпадения двух событий: на агенте присутствует программа, в которой есть «трендовая» уязвимость, а также критичность агента имеет значение «Критичная». Трендовые уязвимости определяются аналитиками на TI-платформе, а критичность агента устанавливается аналитиками RT Protect EDR. Критичным может быть агент, установленный на важном хосте: контроллер домена, сервер с важной базой данных и т.д. Трендовая

уязвимость в Программе помечается соответствующим значком (). Обычно под трендовыми подразумеваются такие уязвимости, которые активно используются злоумышленниками в данный момент времени и поэтому требуют особого внимания к себе со стороны сотрудников информационной безопасности.

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

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

1) Инцидент (содержит название инцидента и CVE-идентификатор уязвимости);

2) Агент (показывает имя критичного агента, на котором содержится программа с трендовой уязвимостью);

3) Статус инцидента (активен, завершен автоматически или завершен вручную);

4) Программное обеспечение (название программы, в которой обнаружена трендовая уязвимость);

5) Время обнаружения;

6) Действия (содержит кнопку **Закрыть инцидент**).

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

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

1) Имя;

2) Издатель;

3) Версия;

4) Агенты;

5) Уязвимости.

Программы в таблице можно фильтровать с помощью следующих фильтров:

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

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

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

Примечание

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

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

10.15.1. Формирование отчетности на странице с уязвимостями

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

.

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

10.15.2. Распространенность программы с уязвимостью в защищаемой инфраструктуре

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

10.15.3. 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 исполняется программа).

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

Базовые метрики, отображаемые на странице **Сведения об уязвимости** и их возможные значения представлены в таблице 57.

Таблица 57 –Базовые метрики уязвимостей

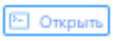
Стандарт	Метрики	Описание	Значения метрики
CVSS 3.x	Вектор атаки (AV)	Показывает удаленность потенциального атакующего от уязвимого объекта	Сетевой (N)
			Смежная сеть (A)
			Локальный (L) (атакующему требуется локальная сессия)
			Физический (P) (атакующему требуется физический доступ к уязвимой системе)
	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)
			Не оказывает (N)

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

Для уточнения значения метрик дополнительно можно использовать временные и контекстные метрики, которые позволяют учитывать отличные от базовых факторов. Для подобной работы можно использовать калькулятор БДУ ФСТЭК, ссылка на который содержится на странице с уязвимостью (кнопка в строке **Вектор атаки**).

10.16 Работа с терминалом

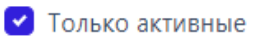
10.16.1. Общая информация

Терминал является консолью управления, предназначенной для задания команд определенному агенту. Оболочка командной строки доступна аналитику со страницы **Терминал** или со страницы агента. Переход к командной строке происходит при нажатии кнопки 

в области **Консоль управления**.

Примечание

Формат команд аналогичен формату команд средства автоматизации PowerShell для агентов, установленных в ОС Windows, и командного процессора BASH для агентов, установленных в ОС Linux.

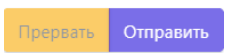
В области **Выбор Агента** необходимо выбрать из всплывающего списка агента, для которого будут вводиться команды в терминале. Чтобы оставить в списке только активных в данный момент агентов, следует установить флажок 

. Если флажок не устанавливать, то для выбора будут доступны все агенты, но отправлять команды в терминале можно будет только активным, для неактивных агентов доступен только просмотр истории команд терминала.

После выбора активного агента появится окно **Терминал**, разделённое на две части:

1) Область просмотра истории работы с терминалом;

2) Область ввода команд.

Если в списке выбрать неактивного в данный момент агента, то область ввода команд будет выделена для такого агента заливкой серого цвета, обозначающей, что ввод команд невозможен, кнопки 

также будут неактивны, как и область ввода **Таймаут (сек)**. По умолчанию таймаут составляет 300 секунд.

Для некоторых пользователей доступ к терминалу может быть запрещен, в этом случае страница **Терминал** будет отсутствовать для такого пользователя, а также станут неактивными кнопки **Выполнить команду на выбранных агентах** на странице **Агенты** и **Открыть** на странице **Агент**.

10.16.2. Отправка команд управления на странице «Терминал»

Для управления агентом с помощью командной строки аналитику следует прописать в области ввода **Введите команду (Enter – отправить, Ctrl-C – прервать, макс. длина 32768 символов)** необходимую команду и нажать клавишу **Enter** или кнопку Отправить. В области просмотра истории терминала отображаются ранее введённые команды и показывается текущий статус выполнения команды. Предусмотрены следующие статусы: Отправлена / Получена / Выполнена (код 0)

Для просмотра основных доступных команд и описаний к ним необходимо ввести в окне терминала команду **help** (рис. 95**)**.

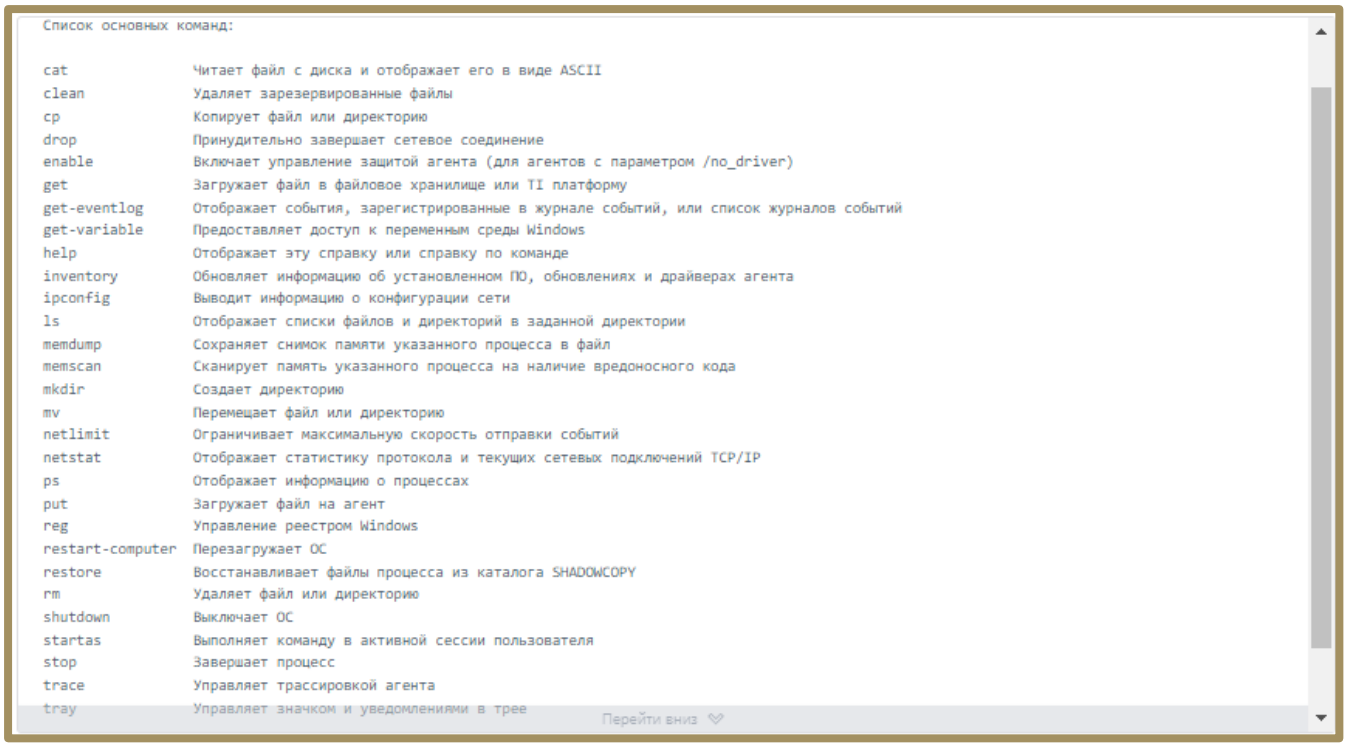


Рисунок 95 – Список основных команд терминала

Если требуется справка о команде из представленного списка, необходимо ввести команду с одним из аргументов: /h, /help, -h, --help, /?. Примеры команд:

restore /?

restore --help

Снизу от области просмотра истории терминала находится кнопка перехода к результату последнего ввода команды Перейти вниз.

В нижней части области **Терминал** содержится кнопка Прервать, ее действие дублируется с помощью нажатия сочетания клавиш Ctrl+C во время выполнения команды в терминале. С помощью кнопки или сочетания клавиш можно прервать выполнение команды. Статус команды поменяется на Прервана (Ctrl-C), а через единицу времени, указанную в поле **Таймаут (сек)** статус поменяется на Прервана (таймаут).

Для установки времени ожидания ответа от агента при отправке команд в поле **Таймаут (сек)** необходимо указать нужный интервал времени в секундах. По умолчанию время ожидания составляет 300 секунд.

Для изменения агента в области **Выбор Агента** нужно нажать кнопку ✕ в строке с названием текущего агента, после чего из выпадающего списка выбрать нового агента.

10.16.3. Описание команд терминала, реализованных в службе агента

Перечень команд, реализованных в службе агента:

– clean;

– drop;

– get;

– put;

– inventory;

– restore;

– startas;

– stop;

– tray;

– off;

– enable;

– команды перезапуска службы агента;

– trace;

– memdump;

– memscan;

– netlimit.

Команда **clean** – удаляет зарезервированные файлы. Команда выполняется согласно синтаксису **clean** [<Максимальный возраст файлов>]. Максимальный возраст файлов (допустимые суффиксы: d – дни, h – часы, m – минуты). По умолчанию используется значение из профиля защиты данных агента (10 дней).

Примеры написания команды **clean**:

clean 10h – удаляет зарезервированные файлы старше десяти часов;

clean 2d – удаляет зарезервированные файлы старше двух дней.

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

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

— id – fluuid или flow сетевого соединения;

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

Примеры написания команды **drop**:

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

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

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

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

-f –путь до файла;

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

Пример написания команды:

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

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

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

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

Пример написания команды:

memdump 2260

memdump -id 2260

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

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

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

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

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

Пример написания команды:

memscan 1080

memscan -id 1080

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

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

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

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

-u – это ссылка для загрузки;

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

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

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

Примеры написания команды:

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

put https://192.168.113.7/api/storage/user/object/894a2551-1e14-4e38-9f44-432428017c06/first_aid_kit.exe;

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

put https://192.168.113.7/api/storage/user/object/894a2551-1e14-4e38-9f44-432428017c06/first_aid_kit.exe -w C:\Tools -n file_ver_1.exe.

Команда **restore** – восстанавливает зарезервированные файлы. Команда выполняется согласно синтаксису restore [-id] <UUID-процесса> [-c], где:

-id – это UUID процесса;

-c – аргумент для удаления созданных файлов.

Пример написания команды:

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

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

-cmd – это командная строка для запуска;

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

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

Пример написания команды:

startas calc.

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

-id – это UUID процесса;

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

-w – кто завершил процесс: admin – администратор, ti – ti-платформа (по умолчанию admin);

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

Примеры написания команды:

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4};

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti;

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w admin -t error.

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

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

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

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

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

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

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

Пример написания команды:

tray (выводит информацию о текущем состоянии значка трея);

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

Команда управления параметром **off** – для изменения параметра off необходимо в терминале агента ввести след. команду:

New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpnt\Parameters -Name off -PropertyType DWord -Force -Value <Новое значение параметра off>.

Пример написания команды:

New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpnt\Parameters -Name off -PropertyType DWord -Force -Value 0x1F.

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

Пример: enable.

Команда перезапуска службы агента – для перезапуска службы агента необходимо выполнить последовательно следующие команды в терминале агента:

```
New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpsvc -Name AllowStop -PropertyType DWord -Force -Value 1
& sc.exe control vrpsvc 128
restart-service vrpsvc
```

Совет

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

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

-start – запускает трассировку;

-stop – останавливает трассировку;

-svc – управление трассировкой службы;

-drv – управление трассировкой драйвера;

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

[уровень логирования] – 0x5 (verbose), 0x4 (Informational), 0x3 (Warning), 0x2 (Error), 0x1 (Critical), (используется в команде -start);

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

Маски логируемых подсистем и наименования этих подсистем приведены в таблице 58.

Таблица 58 – Маски логируемых подсистем

Подсистемы	Маски
Маски логируемых подсистем для службы агента	

TRACE_SERVICE_ENGINE	0x00000001
TRACE_EVENTS	0x00000002
TRACE_METADATA_ENGINE	0x00000004
TRACE_AGENT_UPDATE	0x00000008
TRACE_FILE_SCANNER	0x00000010
TRACE_NETWORK_CONTAINMENT	0x00000020
TRACE_SESSION_MONITOR	0x00000040
TRACE_ETW_CONSUMER	0x00000080
TRACE_ETW_DOTNET_LOAD_IMAGE_MONITOR	0x00000100
TRACE_ETW_RPC_MONITOR	0x00000200
TRACE_ETW_KERBEROS_ATTACK_MONITOR	0x00000400
TRACE_ETW_SYSTEMTIME_CHANGED_MONITOR	0x00000800
TRACE_ETW_WMI_ACTIVITY_MONITOR	0x00001000
TRACE_ETW_MONITORS	0x00002000
TRACE_TERMINAL	0x00004000
TRACE_WMI_MONITOR	0x00008000
TRACE_SYSTRAY	0x00010000
TRACE_MS_GROUP_POLICY	0x00020000
TRACE_YARA	0x00040000
TRACE_ML	0x00080000
Маски логируемых подсистем для драйвера агента	
TRACE_REGISTRY_MONITOR	0x00000001
TRACE_REGISTRY_MATCHER	0x00000002
TRACE_REGISTRY_CONFIG_PARSER	0x00000004
TRACE_RESERVED1	0x00000008
TRACE_FS_MONITOR	0x00000010
TRACE_FS_MONITOR_SIGN	0x00000020
TRACE_FS_MONITOR_RULES	0x00000040
TRACE_FS_MONITOR_HASHES	0x00000080
TRACE_FS_MONITOR_SCAN	0x00000100
TRACE_FS_MONITOR_DEF_SCAN	0x00000200
TRACE_RESERVED2	0x00000400

TRACE_RESERVED3	0x00000800
TRACE_ARW	0x00001000
TRACE_ARW_BLOCK_OPERATION	0x00002000
TRACE_ARW_RESERVED1	0x00004000
TRACE_ARW_RESERVED2	0x00008000
TRACE_PATH_CLASSIFY	0x00010000

Примеры написания команды:

1) Трассировка всех подсистем службы с уровнем логирования Verbose:

trace -start –svc

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

trace -start -svc 0x8040 0x3

3) Остановка трассировки службы:

trace -stop -svc

4) Трассировка всех подсистем драйвера с уровнем логирования Verbose:

trace -start -drv

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

trace -start -drv 0x7 0x2

6) Остановка трассировки драйвера:

trace -stop –drv

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

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

Пример написания команды:

1) Вывод текущего ограничения максимальной скорости отправки:

netlimit

2) Установка ограничения максимальной скорости отправки 5 Кбит\с:

```
netlimit 5
```

3) Снятие ограничения на максимальную скорость:

```
netlimit 0
```

10.16.4. Информация в области «Выбор Агента»

В области **Выбор агента** аналитик может выбрать агента, которому необходимо отправить команду. Для большего удобства в строке выбора можно оставить только активных агентов, поставив флажок **Только активные**. В области **Выбор агента** пользователю доступна следующая информация об агенте:

1) Имя компьютера;
2) Версия ОС;
3) Время загрузки системы;
4) Процессор;
5) Оперативная память;
6) Сетевые адреса.

Имя компьютера – в поле отображается имя компьютера, на котором установлен агент.

Версия ОС – в поле отображается название ОС, установленной на компьютере, на котором работает агент.

Время загрузки системы – в поле отображается информация о дате и времени последней загрузки операционной системы, под управлением которой действует агент.

Процессор – в поле отображается наименование и тактовая частота процессора компьютера, на котором установлен агент.

Оперативная память – в поле отображается объем оперативной памяти компьютера, на котором установлен агент. Объем указан в мегабайтах.

Сетевые адреса – в поле отображаются IP-адреса, назначенные для всех сетевых интерфейсов компьютера, на котором установлен агент.

В нижней части области **Выбор Агента** отображается состояние агента – Активен / Не активен.

10.17 Просмотр графиков

На странице **Графики** аналитик 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.

Графики поддерживают выбор и фиксацию временного интервала, после чего можно перейти к событиям, произошедшим на этом временном интервале, для этого необходимо зажать ЛКМ и выбрать интервал, после чего нажать кнопку **Перейти к событиям на выбранном интервале** (), для перехода на страницу **Активность**, где будет предустановлен выбранный период регистрации событий.

10.18 Просмотр файла в разделе Хранилище

Любой исполняемый файл может быть загружен в файловое хранилище со страниц **Активность**, **Инцидент** и **Процесс** с помощью кнопки (**Загрузить файл в файловое хранилище**). После скачивания в хранилище файл будет доступен аналитику для просмотра и дальнейшего скачивания на компьютер, с которого осуществляется доступ к модулю администрирования (кнопка во вкладке **Файлы с агентов**). Аналитик также может загружать файлы в хранилище со своего компьютера, перейдя на вкладку **Загрузка файлов** или использовать ссылку на скачивание ( ) для того, чтобы вставить ее в команду агента. Идентичная ссылка представлена и на вкладке **Файлы с агентов**.

Файл на странице **Хранилище** можно проанализировать с помощью программы просмотра файлов.

Для просмотра загруженного файла необходимо кликнуть по соответствующей ему кнопке **Просмотреть файл** ( ), после чего откроется окно **Просмотр файла** (рис. 96).

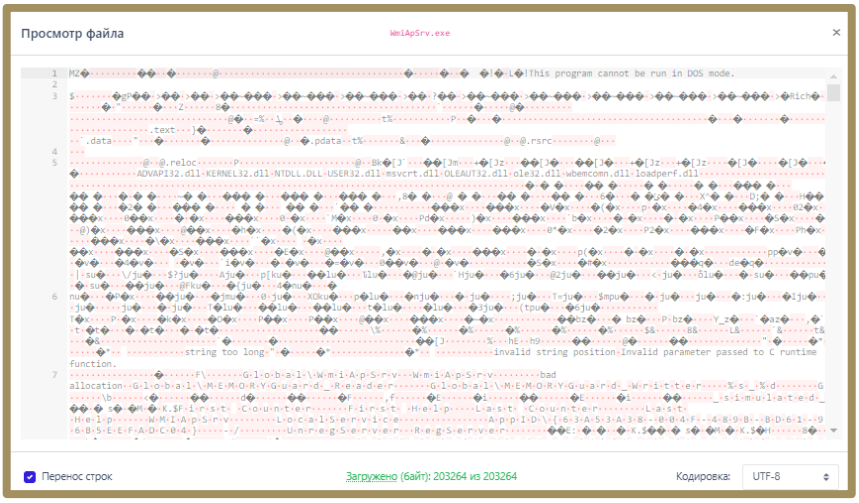


Рисунок 96 – Окно «Просмотр файла»

Файл можно просмотреть в различных кодировках или в бинарном представлении. Если размер файла превысит 1 мегабайт, то файл будет загружен только частично. В таких случаях для загрузки оставшейся части файла необходимо нажать кнопку (**Загрузить ещё 1 Мб содержимого файла**). После просмотра файла его можно удалить, воспользовавшись кнопкой **Удалить файл** ( ).

Файлы, которые были загружены с хостов аналитиков или хостов с установленными агентами, проверяются TI-платформой, отчеты содержатся в поле **Результаты проверки**.

10.19 Проактивный поиск угроз

10.19.1. Проведение расследований на странице «Активность»

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

Современные APT-атаки могут проводиться таким образом, что явных инцидентов, указывающих на вредоносную активность на конечных точках, возникать не будет. Зачастую такие атаки скрываются под легитимными процессами, используют легитимное ПО, которое является нативным для ОС Windows, например, PowerShell или rundll32.

Активный поиск угроз позволяет на ранней стадии выявлять новые и сложные угрозы и рассматривается как дополнение к имеющейся защите информационных систем организации, а не как ее замена. От традиционных методов защиты threat hunting отличает именно проактивность. Активный поиск угроз (охота на угрозы, threat hunting) – это процесс проактивного (то есть упреждающего) обнаружения вредоносной деятельности в компьютерных сетях. Поскольку проникновение в систему может произойти в любой момент, охота на угрозы – это непрерывный процесс, который можно разбить на 3 шага:

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

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

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

Совет

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

Если обнаруженная аномальная активность не укажет на APT-атаку, результаты поиска все равно могут быть полезны. Положительным эффектом выявления аномалий может стать определение слабых мест защищаемой инфраструктуры или возможностей для улучшения ее защиты. Чем больше аналитик будет знать о защищаемой системе, тем лучше он сможет ее оборонять от возможных атак и проникновений злоумышленников. Страница **Активность** позволяет аналитику проводить проактивные расследования и выявлять отклонения от нормы в событиях, поступающих от конечных точек.

Кроме большого количества фильтров, позволяющих сортировать телеметрические события по множеству различных параметров, страница **Активность** предоставляет возможность аналитику использовать строку DSL-запросов на языке Elasticsearch Query DSL (рис. 97).

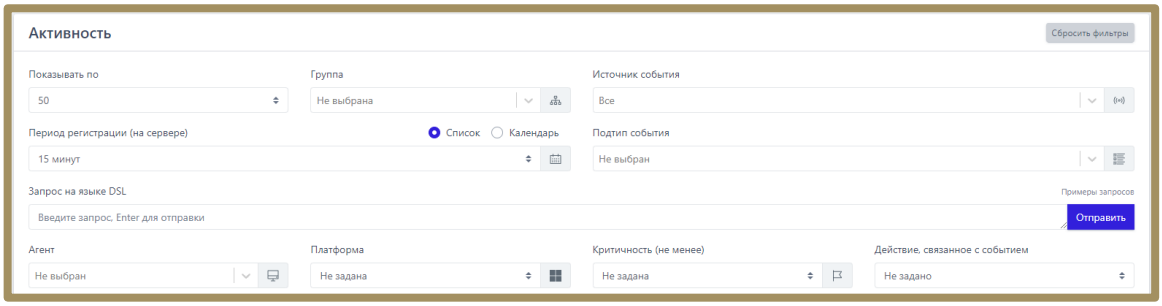


Рисунок 97 – Фильтры на странице «Активность»

Для написания запросов необходимо знать и структуру событий, отправляемых агентами на сервер, и сам язык запросов. Полное описание полей всех событий расположено в разделе 9. Описание языка запросов представлено на официальном сайте elasticsearch (https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html). Далее приведено собственное описание языка запросов с примерами.

Примечание

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

Пример первого варианта представлен на рисунке 98.

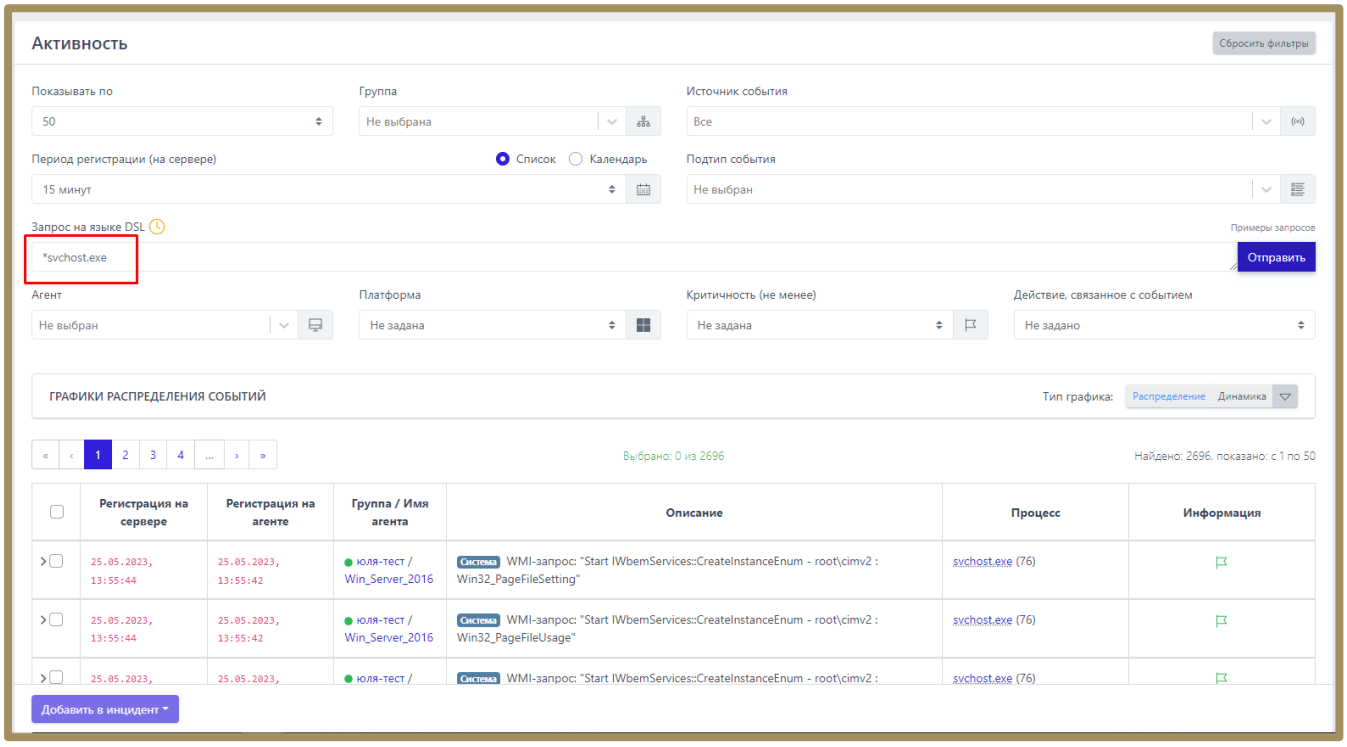


Рисунок 98 – Запрос вне семантики

Результатом строки запроса ****svchost.exe*** являются все события, в которых есть поля, значения которых оканчиваются на подстроку ***svchost.exe***. Это может быть имя исполняемого файла при запуске нового процесса, так и имя файла в событии создания нового файла и др. При этом в работе с большими временными периодами необходимо учитывать, что такой запрос не будет оптимальным с точки зрения производительности системы.

Примечание

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

Если же требуются именно события процессов с исполняемым файлом **svchost.exe**, в запросе необходимо указать имя поля, для которого будет выполнен поиск. Пример такого запроса представлен на рисунке 99.

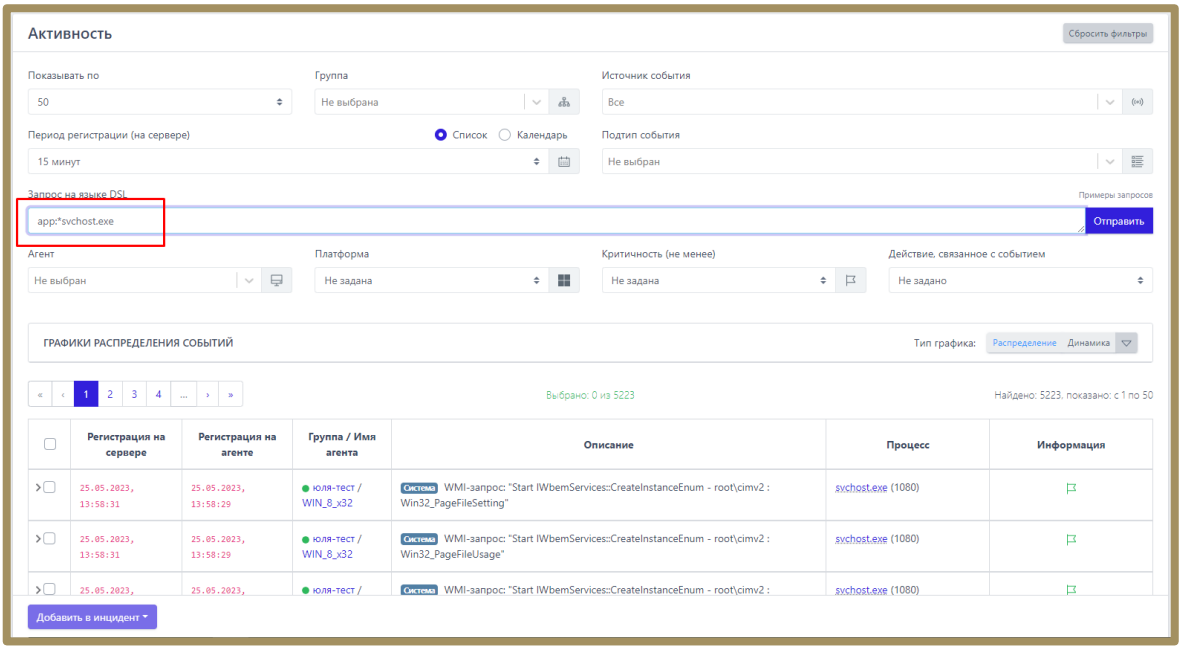


Рисунок 99 – Поиск по заданному полю

Совет

Svchost.exe и другие хост-процессы, например, rundll32.exe скрывают действующий процесс в событии, для того чтобы понять реального актора, необходимо обращать внимание на область **Инициатор** в карточке события на странице **Активность**, а конкретнее, нам нужна строка **Полное имя исполняемого модуля-инициатора операции** (**who**).

Формат запроса с учетом семантики значения имеет вид: **<имя_поля>:<искомое_значение>**. В случае, если искомое значение представляет собой некоторую подстроку, необходимо использовать регулярные выражения. На рисунке, приведенном выше, результатом запроса будут все события, в которых есть поле ***app***, и значение этого поля оканчивается на ***svchost.exe*** (при этом возможно, что значение поля будет в точности равно искомому выражению). Поиск значения ведется с учётом регистра символов. Для того, чтобы регистр не учитывался, к имени поля необходимо указать спецификатор ***lower***.

Пример запроса без учета регистра приведен на рисунке 100.

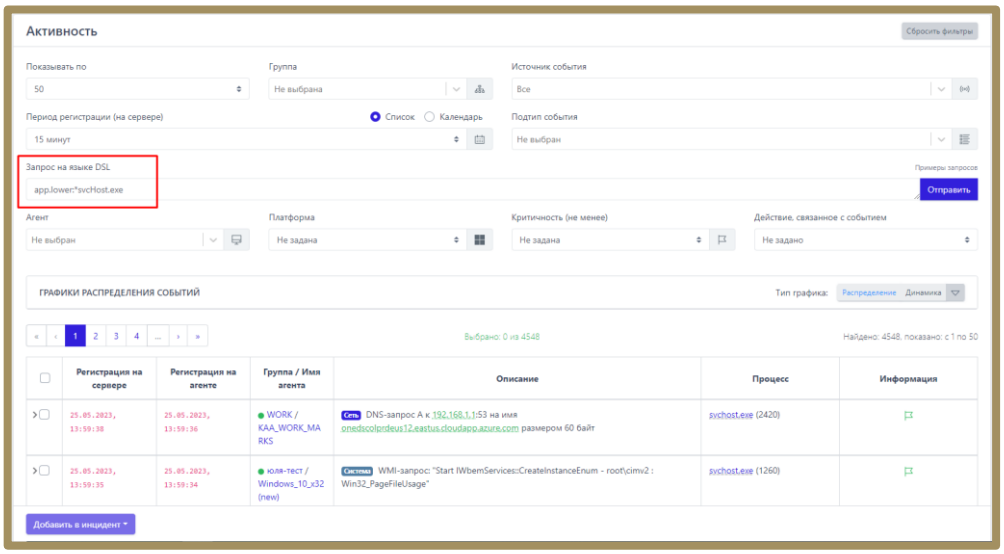


Рисунок 100 – Запрос без учета регистра

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

Язык Elasticsearch Query DSL позволяет осуществлять сложные запросы, состоящие из объединения простых запросов, рассмотренных ранее, с помощью логических операторов: И, ИЛИ, НЕ. Логические операторы задаются с помощью ключевых слов: AND, OR, NOT. Ключевые слова записываются с учетом регистра символов, т.е. And, and не являются логическими операторами. Для группирования результатов выполнения подзапросов используются круглые скобки. Пример сложного запроса представлен на рисунке 101.

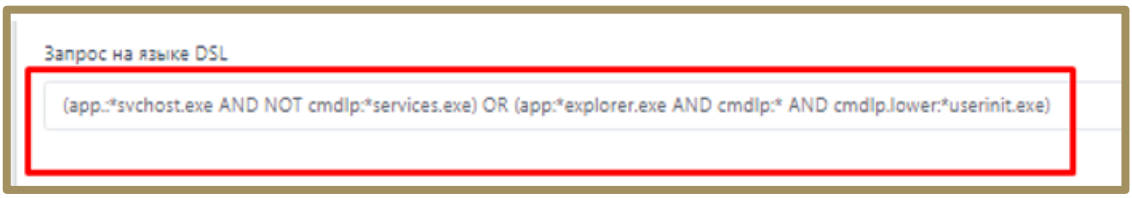


Рисунок 101 – Сложный DSL-запрос

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

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

1) Количество отображаемых событий на странице;

2) Группа (на странице отобразятся события, пришедшие от агентов выбранной группы);

3) Источник события (на странице отобразятся события, соответствующие выбранному источнику: сеть, файлы, реестр 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 формы «Активность» является ретроспективный анализ на предмет выявления артефактов «свежих» угроз. Например, в одном из контуров агентской сети было проведено расследование некоторого инцидента, в результате которого были выявлены: хеши, IP-адреса, DNS-имена, имена исполняемых файлов, связанные с этим инцидентом. Далее обычно происходит поиск в других контурах, с целью определения факта компрометации других агентов. Пример такого запроса представлен на рисунке 102.

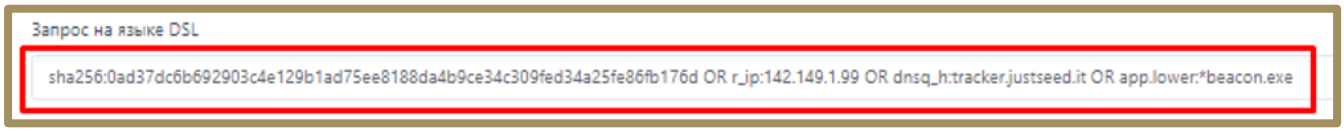


Рисунок 102 – Пример запроса для ретроспективного анализа угроз

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 103.

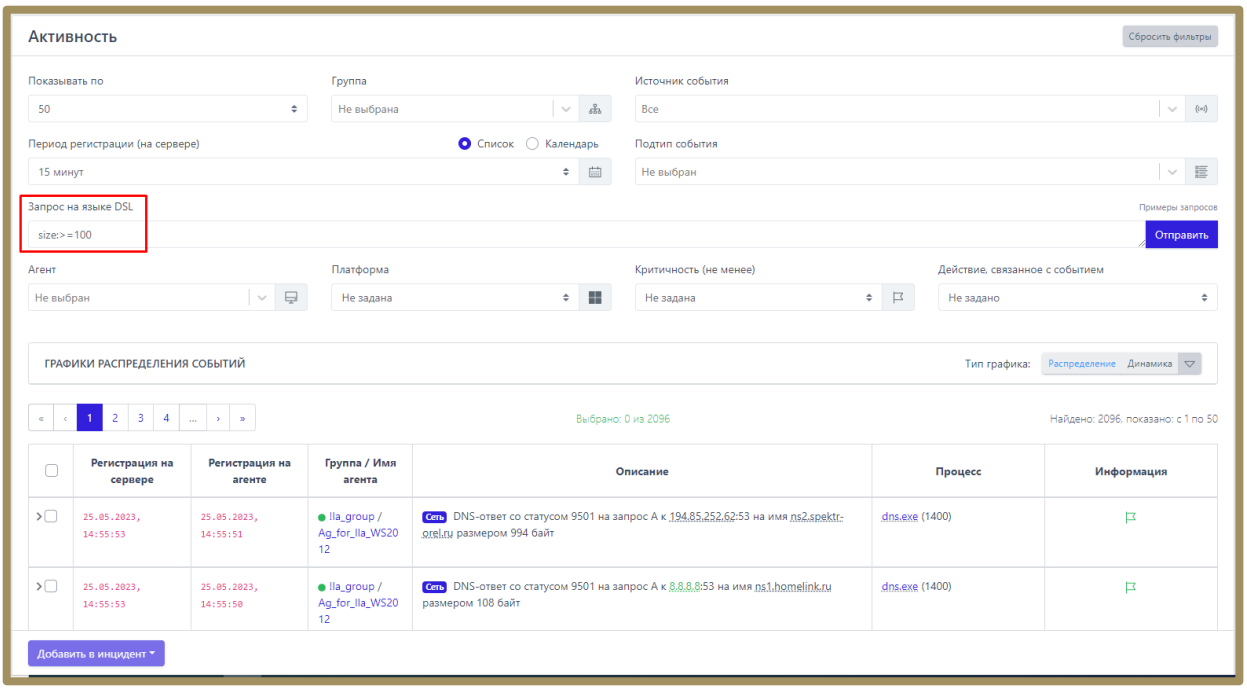


Рисунок 103 – Пример запроса с числовым значением

Также допускается фильтрация для диапазона значений. Пример фильтрации событий входящих сетевых подключений для диапазона сетевых портов [1080;1800] представлен на рисунке 104.

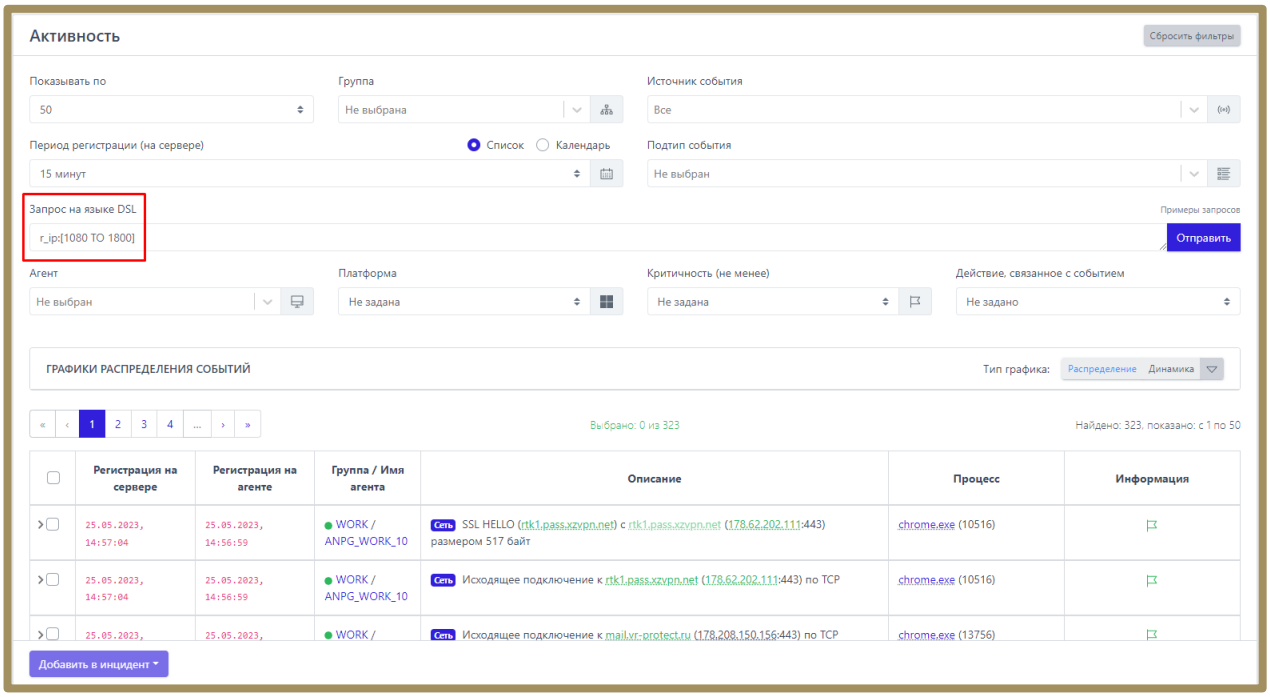


Рисунок 104 – Пример запроса с диапазоном значений

Следует отметить, что наиболее частой ошибкой при поиске, например, исполняемого модуля, является указание его названия без расширения. Иллюстрация такой ситуации представлена на рисунках 105 – 106.

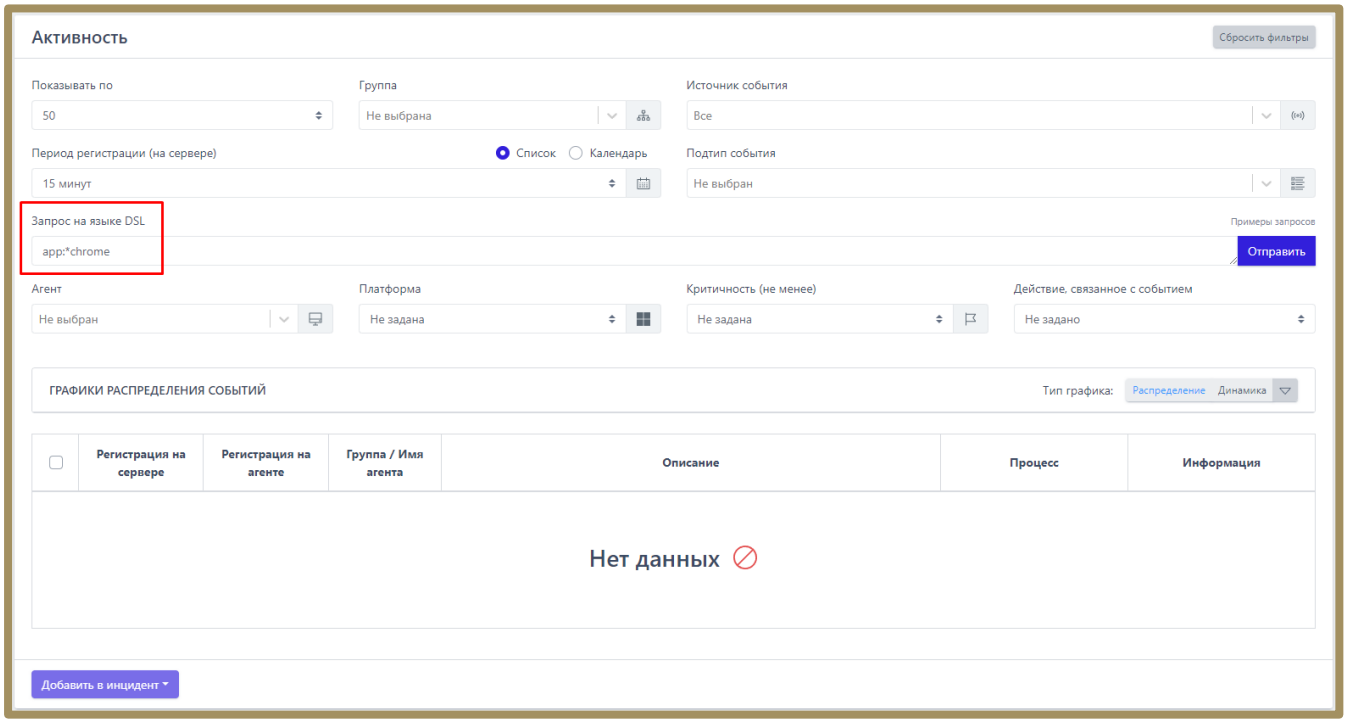


Рисунок 105 – Пример неправильного DSL-запроса

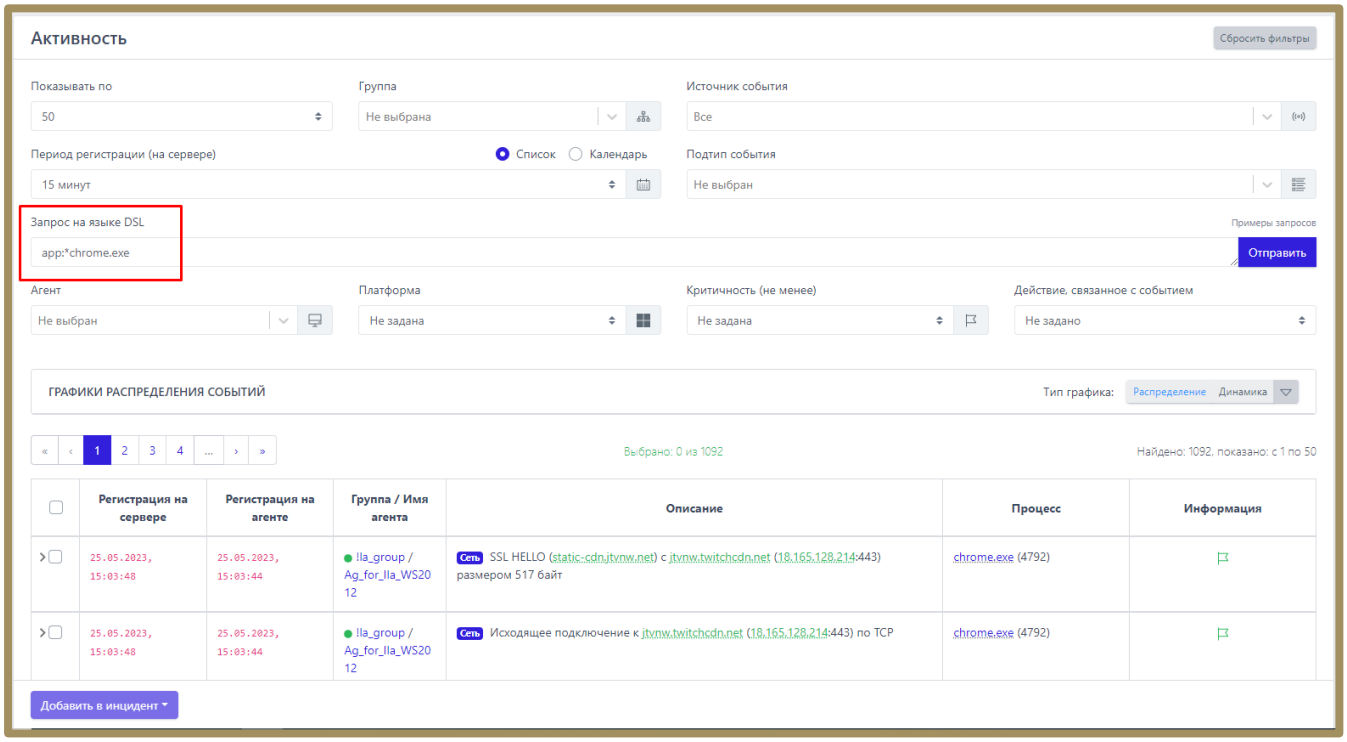


Рисунок 106 – Исправленный вариант DSL-запроса

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 107.

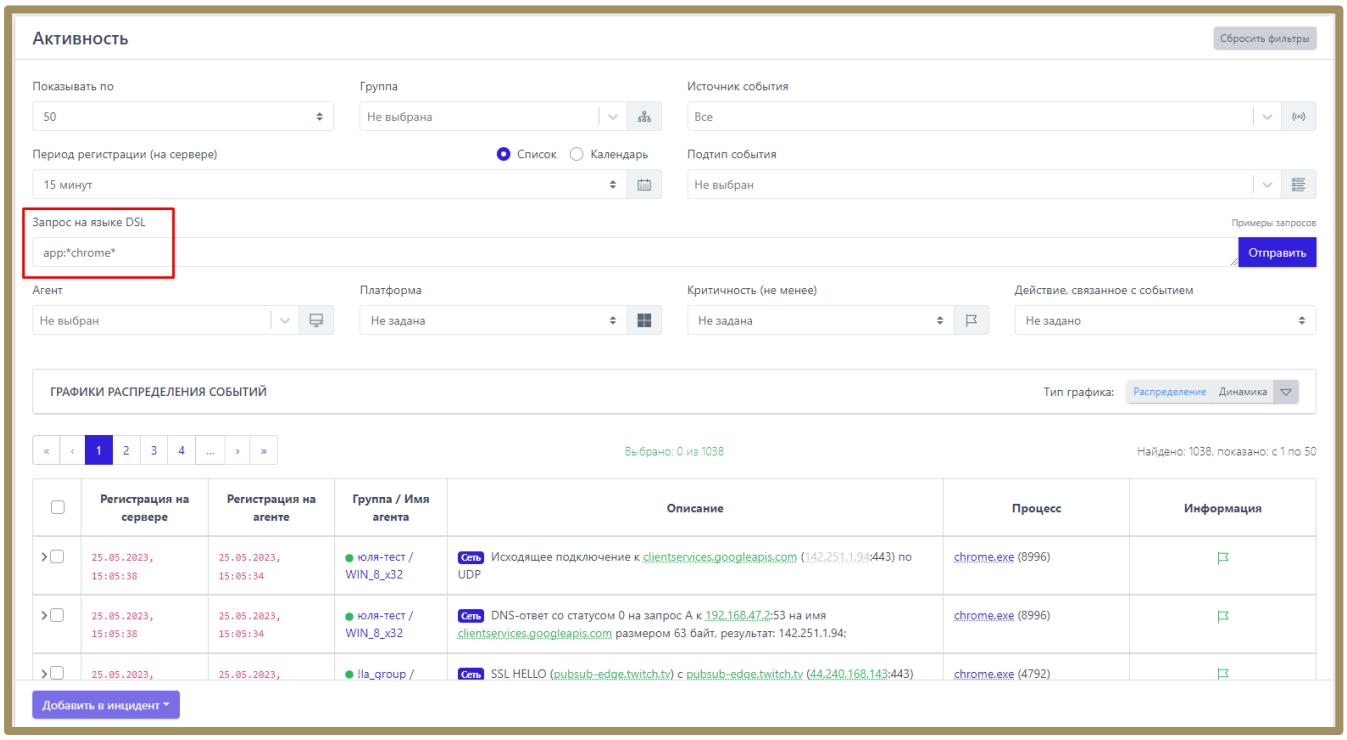


Рисунок 107 – Использование регулярных выражений для DSL-запроса

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. 108).

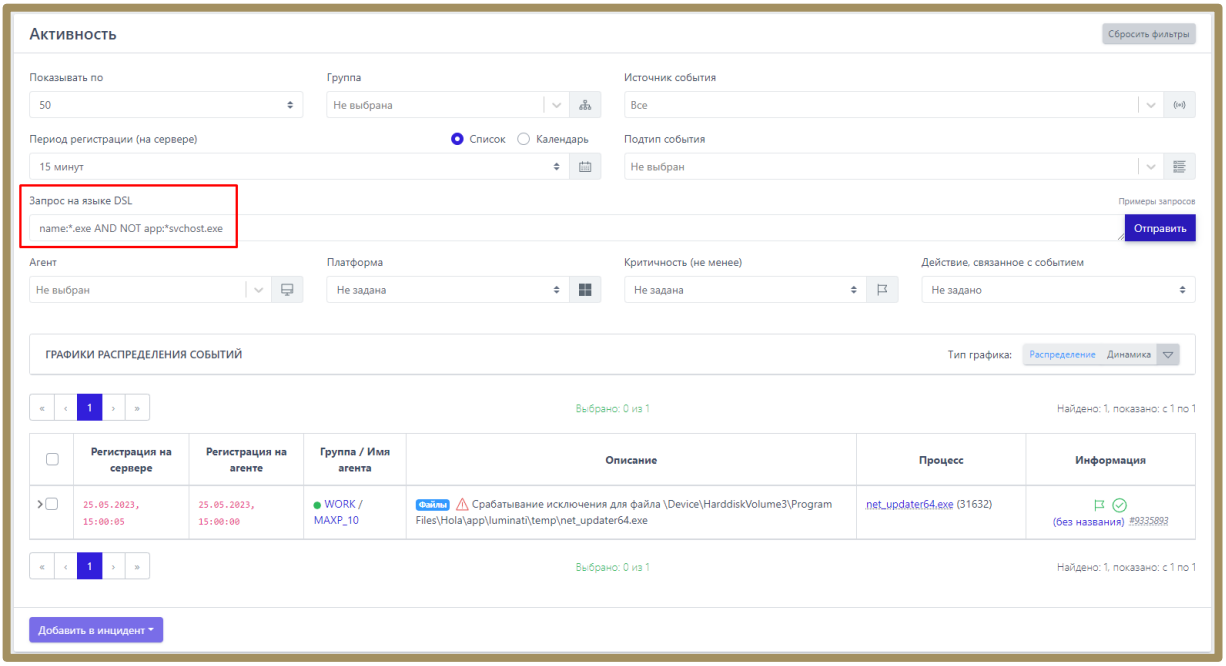


Рисунок 108 – Пример использования оператора NOT

Делая выводы, необходимо сказать, что для проведения ретроспективного анализа и проактивного поиска угроз и аномальной активности в защищаемой инфраструктуре следует использовать DSL-запросы и систему фильтров.

Для глубокого изучения всех обстоятельств и составных частей конкретного события на странице **Активность** предусмотрены карточки события. Они помогают аналитику разобрать информацию, полученную от конечной точки, защищаемой агентом. Эта информация касается всех значимых подсистем операционной системы Windows или Linux: сеть, файлы, процессы т.д. Соответственно, набор этих подсистем в разных ОС будет отличаться. Поля карточки меняются в зависимости от типа и подтипа события, при этом есть данные, которые содержатся во всех карточках, например, имя агента или время регистрации события на сервере.

Значительный интерес для аналитика в карточке события могут представлять битовые флаги, например, поведенческие признаки процесса или флаги исполняемого файла процесса.

Их можно применять при создании индикаторов атак. Подробный перечень битовых флагов содержится в подразделе 9.

В поле **Описание** таблицы на странице **Активность** и в карточке события для некоторых типов событий представлены артефакты, анализируемые TI-платформой:

1) IP-адреса;

2) Доменные имена;

3) Хеш-суммы.

В зависимости от состояния артефакт отображается разным цветом:

— безопасный – зеленый цвет (fe2.update.microsoft.com);

— об артефакте нет информации – светло-серый цвет (150.171.16.39);

— анализ артефакта выполняется в данный момент – синий цвет (s350iva.storage.yandex.net);

— вредоносный – красный цвет (35.155.156.153);

— подозрительный – оранжевый цвет (185.243.218.110).

В верхней части страницы отображается область с диаграммами (**Графики распределения событий**), на которых в графическом виде представлены типы и подтипы событий в соответствии с настроенными в данный момент фильтрами. Чтобы показать графики, необходимо нажать кнопку  . Графики распределения событий можно просматривать в круговых диаграммах, а также линейном и столбчатом виде. Для переключения между этими видами используется сочетание кнопок Динамика / Распределение (рис. 109).

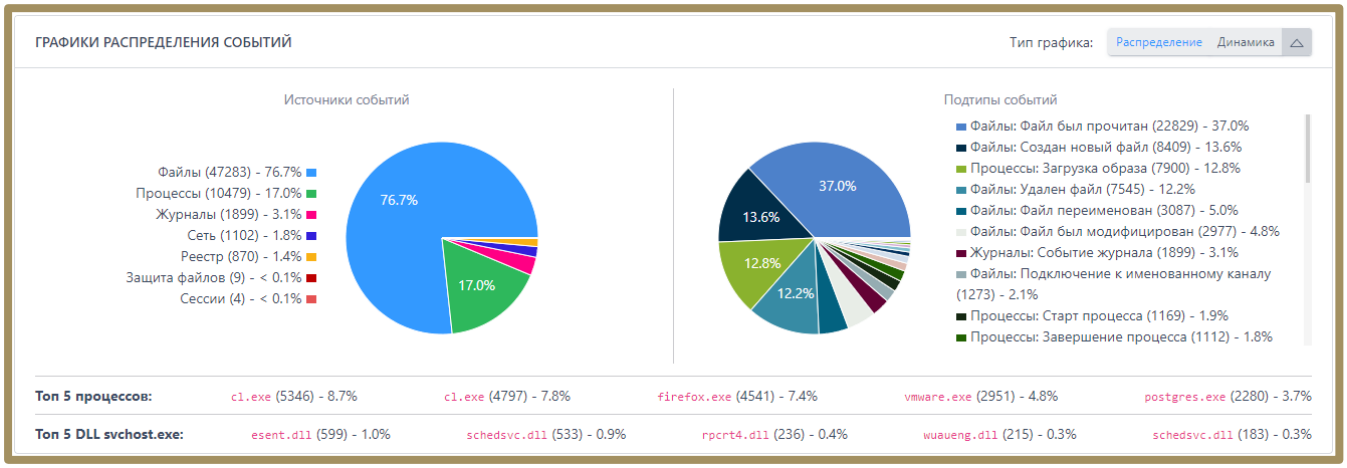


Рисунок 109 – Графики распределения событий

Ниже графиков пользователь EDR может просмотреть топ 5 наиболее часто встречающихся процессов в защищаемой инфраструктуре, а также топ 5 динамически загружаемых библиотек в хост-процессе svchost.exe.

10.19.2. Просмотр зашифрованной информации на страницах «Активность», «Инциденты», «Инцидент» и «Процесс»

При поиске информации на странице **Активность** и **Процесс** или расследовании инцидента аналитик может столкнуться с командными строками, содержащими зашифрованные по алгоритму Base64 команды. Для их расшифровки необходимо выполнить следующие действия:

1) Выделить зашифрованный текст;
2) После выделения текста появится кнопка **Декодировать Base64** ( );
3) Нажать кнопку (откроется окно **Декодирование Base64**);
4) Если необходимо, то скопировать декодированное значение в буфер обмена.

10.19.3. Концепция «Pyramid of Pain»

Все индикаторы, которые могут указывать на присутствие злоумышленников в защищаемой системе, можно ранжировать в соответствии с их значением для атакующего, то есть как много проблем обнаружение этих индикаторов доставит злоумышленнику. Такую концепцию называют «Pyramid of Pain» (рис. 110).

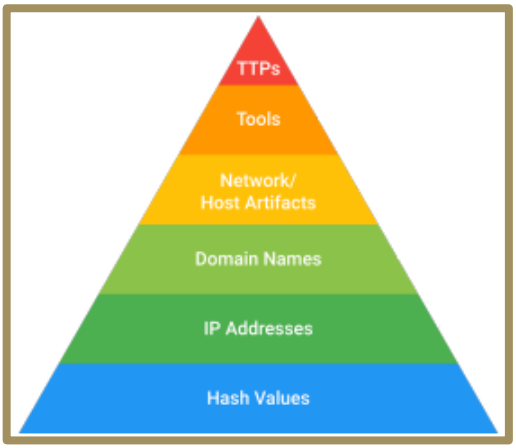


Рисунок 110 – Pyramid of Pain

Внизу пирамиды находятся индикаторы, обнаружение которых доставляет меньше всего проблем злоумышленникам, сверху самые значимые, обнаружение которых наносит максимальный урон их действиям.

Хеши. Большинство хеш-алгоритмов преобразуют входные данные таким образом, что на выходе получается уникальный для этих входных данных хеш. Это значит, что, если содержимое файла отличается хотя бы на один бит, значение его хеша будет также отлично. С одной стороны, индикаторы на основе хешей

являются самыми точными, то есть на их основе можно с наибольшей уверенностью определить вредоносные файлы, а с другой стороны, любое изменение этих файлов, вроде перестановки бита или добавления нуля в конце, изменяет их хеш. Это делает их наименее значимыми индикаторами.

IP-адреса. Любой более или менее продвинутый злоумышленник может менять адреса с помощью небольших усилий, например, используя анонимный прокси-сервер Tor или похожий инструмент. Именно по этой причине IP-адреса находятся внизу пирамиды.

Имена доменов. Имена доменов менять немного сложнее, чем IP-адреса, так как для работы они должны быть зарегистрированы. Однако существует большое количество DNS-провайдеров со слабыми стандартами регистрации, поэтому на практике сменить домен не очень тяжело, в среднем на это может уйти день или два.

Артефакты сети и хоста. Здесь начинается негативное влияние на злоумышленника при обнаружении. Если аналитик может обнаружить и отреагировать на индикаторы этого уровня, то злоумышленнику придется поработать над переконфигурацией или перекомпиляцией своих инструментов. Например, вы обнаруживаете, что утилита HTTP-разведки, которую использует злоумышленник, применяет отличительную строку User-Agent во время изучения вашего веб-контента. Если заблокировать любой запрос, использующий эту строку, то это вынудит злоумышленника потратить свои ресурсы на то, чтобы понять, как именно вы обнаружили их утилиту.

Инструменты. Обнаружение и реагирование на индикаторы этого уровня забирает у злоумышленника возможность использовать один или несколько его инструментов. Чаще всего это происходит, когда аналитик обнаруживает артефакты инструмента различными способами, например, с помощью YARA-сигнатур, если они способны обнаруживать вариации файла даже со средними изменениями.

Тактики, техники и процедуры. Обнаружение и реагирование на индикаторы этого уровня напрямую затрагивает поведение злоумышленника, а не его инструменты. Изменение поведения является самым сложным и затратным для злоумышленника, поэтому, чем больше тактик, техник и процедур можно обнаружить в ходе направленного поиска угроз, тем более защищенной будет система.

10.20 Настройка профилей

В области **Профили** аналитик может настраивать параметры работы профилей агента. Это позволяет задавать требуемый уровень защищенности для определенной инфраструктуры или отдельных элементов защищаемой инфраструктуры, настраивать модуль защиты данных агента, понижать или увеличивать нагрузку на те или иные подсистемы Программы, например, файловый монитор, изменять настройки безопасности сетевого монитора и т.д. Такой подход дает возможность повысить эффективность использования программных инструментов для обнаружения аномальной активности на конечных точках с агентами и эффективно управлять нагрузкой на защищаемую инфраструктуру и Программу.

Важно

Любые изменения профиля приведут к появлению кнопки **Применить профиль**. Информация о пользователе, совершившем последние изменения, появится в правом верхнем углу страницы профиля.

10.20.1. Профили защиты данных

Модуль защиты от шифровальщиков является важной частью EDR: он останавливает работу шифровальщиков на компьютерах с установленным агентом, позволяя защищать от шифрования файлы в защищаемых каталогах. Список каталогов указывается на странице профиля защиты данных.

Модуль Anti-Ransomware прежде всего направлен на защиту от угроз нулевого дня, выполняя перехват и анализ файловой активности каждого процесса в системе в режиме реального времени. Это позволяет выявлять характерные для шифровальщиков паттерны поведения, после чего блокировать их.

Управление модулем осуществляется с помощью профилей защиты данных. На странице **Профили защиты данных** аналитику доступны следующие операции:

– отключить\включить Anti-ransomware-модуль;

– настроить список защищаемых каталогов;

– настроить резервирование данных;

– экспортировать настройки профиля защиты в файл;

– импортировать настройки из ранее экспортированного профиля защиты (поддерживаются файлы в формате txt).

Информация о профилях представлена в табличном виде. В таблице отображаются следующие поля:

– **Название профиля**;

– **Привязано агентов**;

– **Управление** (здесь находятся кнопки редактирования, удаления и сохранения профилей –).

Аналитику, чтобы создать новый профиль защиты данных, необходимо нажать кнопку Добавить профиль и в открывшемся окне ввести название нового профиля, после чего нажать кнопку Добавить (рис. 111).

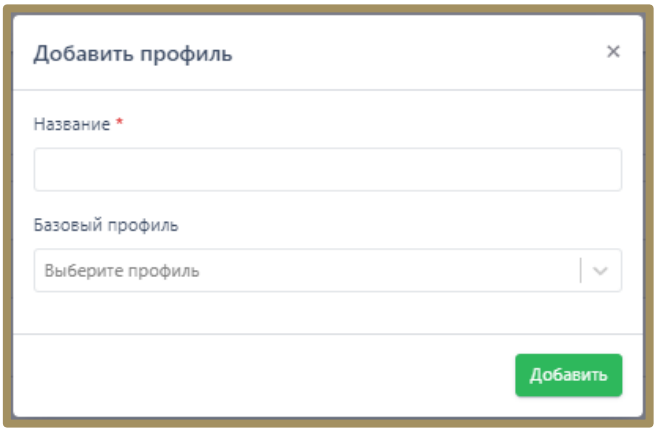


Рисунок 111 – Добавление профиля защиты

Если новый профиль защиты данных требуется создать на основе ранее сохраненного, то в поле выбора **Базовый профиль** следует назначить из выпадающего списка один из существующих профилей защиты и нажать кнопку Добавить.

С помощью кнопки **Редактировать** ( ) можно изменить название профиля (рис. 112).

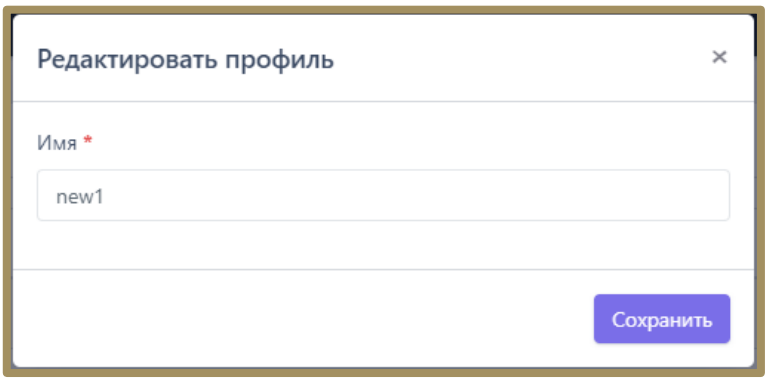


Рисунок 112 – Редактирование названия профиля защиты данных

Значок ⚠ рядом с названием профиля или сверху страницы сообщает пользователю о том, что один или несколько профилей защиты данных не применены, для корректной работы их необходимо применить с помощью кнопки **Применить все профили** ( ).

Для удаления профиля или нескольких профилей защиты данных необходимо отметить их флажками и нажать кнопку Удалить выбранные профили.

Если требуется установить параметры защиты данных, отличающиеся от параметров существующих профилей защиты, то следует нажать название профиля, после чего откроется страница **Профиль защиты данных**.

Страница «Профиль защиты данных»

В любом профиле защиты данных можно выделить три области настроек (рис. 113):

1) Базовые настройки;
2) Настройки резервирования;
3) Список защищаемых каталогов.

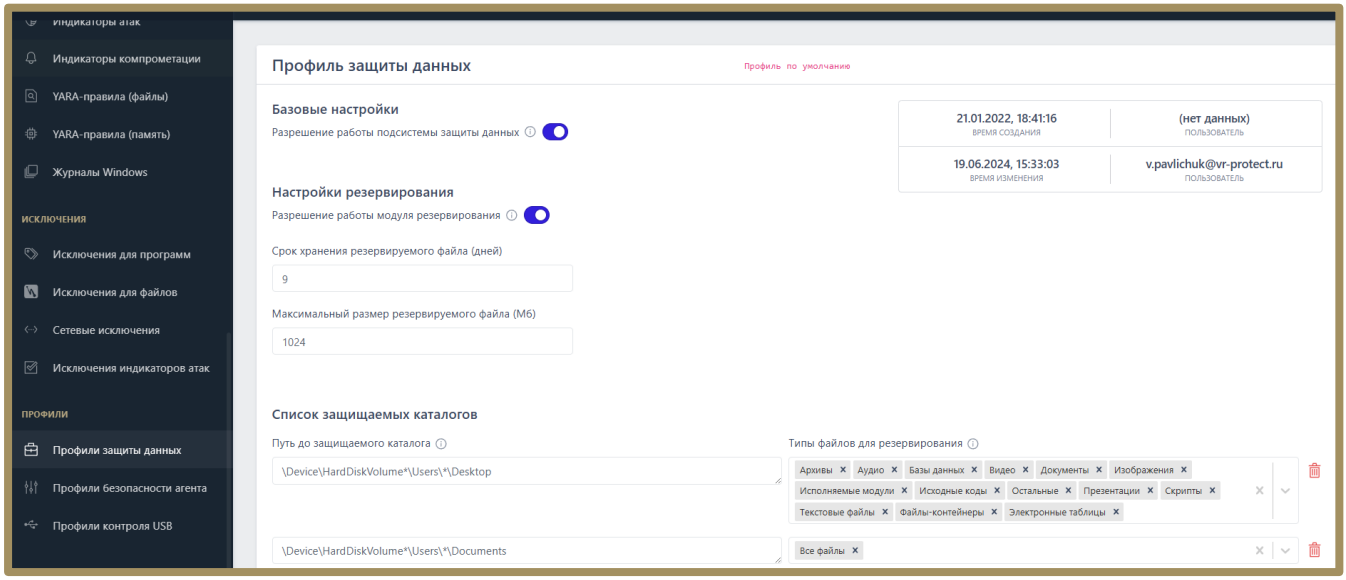


Рисунок 113 – Страница «Профиль защиты данных»

В верхней части страницы отображается информация о пользователе, создавшем профиль, и времени, когда профиль был создан, а также информация о пользователе, сделавшем в профиле последние изменения, и времени внесения этих изменений.

В области **Базовые настройки** профиля аналитик может включить или выключить Anti-ransomware-модуль. Эта настройка задается кнопкой в строке **Разрешение работы подсистемы защиты данных**. Подсистема защищает данные, указанные в списке защищаемых каталогов.

В области **Настройки резервирования** аналитик может выполнить следующие операции:

– разрешить или запретить работу модуля резервирования файлов (кнопка);

– установить срок хранения резервируемого файла в днях;

– установить максимальный размер резервируемых файлов в мегабайтах.

В области **Список защищаемых каталогов** аналитик может настроить каталоги и типы файлов, которые необходимо резервировать.

Типы файлов

Резервирование поддерживает следующие типы файлов:

– документы;

– текстовые файлы;

– электронные таблицы;

– презентации;

– архивы;

– изображения;

– видео;

– исполняемые модули;

– исходные коды;

– скрипты;

– аудио;

– базы данных;

– файлы-контейнеры;

– остальные.

Также на странице профиля предусмотрена функция выбора сразу всех файлов для защищаемого каталога. Каждому типу файла соответствуют определенные расширения файлов. Информация о поддерживаемых расширениях по типу файла может быть показана при нажатии информационной кнопки ⓘ в строке **Типы файлов для резервирования**.

Настройка защищаемых каталогов

Если для определенного каталога не выбран ни один из типов файлов, то резервирование для такого каталога поддерживаться не будет. Аналитик может настроить профиль защиты данных таким образом, чтобы защищать только определенные файлы в определенных каталогах, тем самым снижая нагрузку на систему. Для добавления каталога в список защищаемых необходимо нажать кнопку 

, далее выбрать типы файлов, которые необходимо резервировать для указанного каталога, и применить его (). Новые защищаемые каталоги добавляются с именем по умолчанию **Protected Folder**, поэтому если в профиль требуется добавить два или более каталога, требуется изменять названия добавляемых каталогов. Путь защищаемого каталога должен соответствовать требованиям, полный список которых можно просмотреть, нажав кнопку ⓘ в строке **Путь до защищаемого каталога**. В списке представлены не только требования, но и примеры правильных и неправильных путей.

Если требуется удалить каталог из профиля защиты данных, то в строке с выбранным каталогом необходимо нажать кнопку  .

Для корректного применения на агенте измененных настроек профиля защиты данных должны соблюдаться следующие условия:

1) Профиль защиты данных применен (кнопка  в нижней части страницы);

2) Подсистема защиты данных включена  ;

3) Модуль резервирования включен  ;

4) Конфигурация профиля защиты данных применена для агента.

Профиль защиты данных можно экспортировать в txt-файл, после чего импортировать данные из этого файла в другой профиль. Для этого используются кнопки экспорта () и импорта ().

Как работает резервирование?

После назначения для агента конфигурации с профилем защиты, в котором предусмотрено резервирование данных в одном или нескольких каталогах, администратор сможет восстановить эти данные в случае их шифрования или удаления программой-вымогателем.

Если вирус-шифровальщик проник на конечную точку с установленным агентом и зашифровал данные в защищаемом каталоге, то для восстановления этих данных пользователю необходимо определить процесс, выполнивший шифрование данных и на странице **Процессы** нажать кнопку **Восстановить файлы** и подтвердить выбранную операцию.

Для восстановления файлов также может использоваться команда терминала. Пользователю необходимо выполнить следующие действия:

1) Определить **uuid** процесса, выполнившего шифрование данных;

2) Открыть страницу **Терминал**;

3) Выбрать агента, данные которого были зашифрованы вирусом-шифровальщиком;

4) Выполнить в терминале команду **restore** с указанием **uuid** процесса, зашифровавшего данные на агенте, например, restore -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}.

Важно

Резервирование файлов происходит при попытке шифровальщика совершить какие-либо действия с этими файлами в защищаемых каталогах. Зарезервированные файлы можно восстановить в течение 10 дней.

10.20.2. Профили безопасности агента

Профили безопасности позволяют настраивать нагрузку на систему, увеличивая или уменьшая поток событий, регистрируемых на агенте, а также управлять уровнем безопасности, который будет предоставлять агент. На странице **Профили безопасности агента** аналитик может создавать и редактировать профили, с помощью которых для верифицированных агентов устанавливаются параметры безопасности. В соответствии с этими параметрами будут формироваться события и инциденты, присылаемые агентом в модуль администрирования (рис. 114).

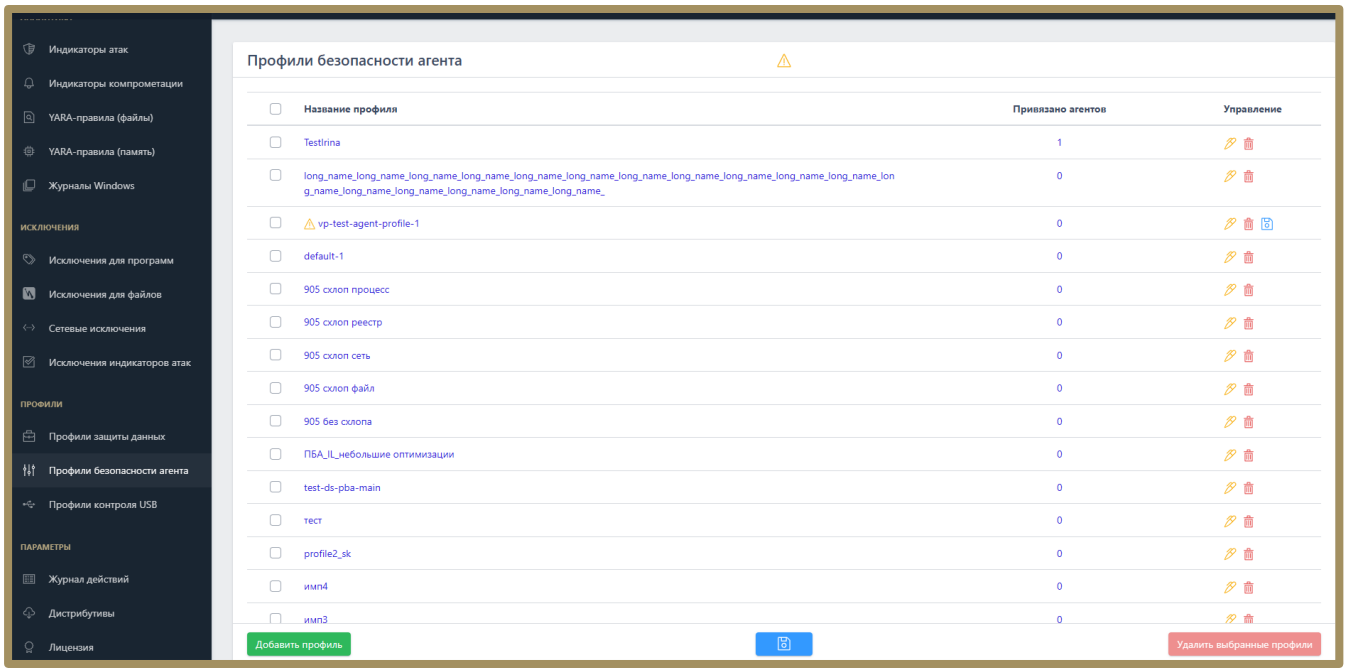


Рисунок 114 – Профили безопасности агента

Набор инструментов для работы с профилями не отличается от набора инструментов для настроек профилей защиты данных или создания и редактирования наборов индикаторов компрометации, атак и т.д.

Аналитик может выполнить следующие операции на странице **Профили безопасности агента**:

– добавить новый профиль безопасности;

– сохранить изменения в профиле и применить изменения для агентов, которым назначен выбранный профиль;

– редактировать название профиля безопасности;

– удалить один или несколько профилей безопасности.

Чтобы изменить параметры безопасности, аналитику необходимо выбрать профиль безопасности агента и настроить его в соответствии с требуемыми параметрами.

Профиль безопасности агента

На странице **Профиль безопасности агента** аналитик может настроить параметры, в соответствии с которыми будут обнаруживаться события на агентах.

Настройки профиля безопасности агента подразделяются на следующие группы:

– параметры оптимизации потока событий;

– общие настройки безопасности.

– параметры безопасности монитора процессов;

– параметры безопасности файлового монитора;

– настройки безопасности сетевого монитора;

– настройки безопасности монитора реестра.

В нижней части страницы находятся кнопки применения настроек, экспорта и импорта профиля безопасности (). Экспорт и импорт файла осуществляется в формате txt.

В области **Оптимизация потока событий** аналитик может управлять отправкой с агентов следующих событий:

1) Исключать файловые события ранней стадии запуска процессов;

2) Фильтровать файловые события;

3) Исключать файловые события префетчера;

4) Исключать события чтения исполняемых файлов, связанные с их исполнением;

5) Исключать события чтения исполняемых файлов;

6) Исключать события чтения любых файлов;

7) Исключать файловые события процесса-создателя файла;

8) Исключать события доступа к процессам и нитям;

9) Исключать события загрузки известных модулей:

10) Исключать события со статусом «Разрешено» (кроме ключевых);

11) Исключать все события со статусом «Разрешено»;

12) Исключать события RPC-вызовов;

13) Фильтровать события модификации реестра;

14) Оптимизировать представление стека вызовов в событиях;

15) Принудительное подавление событий процессов при превышении лимита.

Установив или сняв определенные флаги, аналитик может увеличить или уменьшить количество событий, присылаемых агентом в модуль администрирования. Это позволяет снизить информационный шум или, наоборот, увеличить отображаемую активность, чтобы изучить ее в полном объеме. Кроме того, в области с оптимизацией потока событий находится раздел с настройками событий, получаемых от инструментария управления (WMI). Для WMI доступны три способа фильтрации:

1) По вызову метода;

2) По созданию процесса;

3) По ключевым словам, указанным в профиле безопасности.

В добавление к вышеуказанным методам фильтрации в профиле добавлена опция для отключения генерации событий WMI. Для этого необходимо выбрать пункт фильтрации **Не отправлять события**.

Ключевые слова задаются аналитиком по принципу включения/исключения подстрок, то есть можно задать, какие слова должны содержать строки WMI-запросов, или можно задать, какие слова при фильтрации событий, поступающих от WMI, строки запросов содержать не должны.

С помощью общих настроек безопасности аналитик может установить режим «только детектирование», который позволяет отключить противодействие угрозам в режиме реального времени, то есть действия, которые могут нанести вред защищаемой инфраструктуре не будут блокироваться, но при этом не будет и ложноположительных срабатываний, которые могут привести к запрету на запуск какой-либо полезной программы, действия которой EDR может посчитать нелегитимными в соответствии со своими внутренними или созданными аналитиками правилами.

Важно

Режим «только детектирование» не распространяется на работу блокирующих исключений, то есть действие «блокировать», установленное по отношению к исключениям для программ, файлов или сетевых исключений будет исполняться, несмотря на выбор этого режима.

В области **Настройки безопасности монитора процессов** аналитик может настроить реакции Программы на события определенного типа:

– создание нити в стороннем процессе (кроме авторизованных программ Windows);

– доступ к стороннему процессу/нити (кроме авторизованных программ Windows. Доступны следующие реакции:

1) Разрешить;

2) Блокировать только для неподписанных программ;

3) Блокировать.

При выборе реакции **Блокировать** события соответствующего типа будут отображаться в разделе **Инциденты**, а их активность будет блокироваться Программой. Кроме того, для событий создания нити в стороннем процессе и доступа к стороннему процессу/нити возможно настроить уровень важности, который соответствует уровню критичности события (от уровня **Информация** до уровня **Критичный**). Также аналитик может поставить флаг **Оптимизировать поток событий межпроцессного взаимодействия**, чтобы сократить количество отображаемых на сервере управления событий, связанных с обменом данными между потоками различных процессов.

Для безопасности файлового монитора в Программе предусмотрена настройка реакции на прямой доступ к жесткому диску (кроме авторизованных программ Windows), а также выбор режима глубокого сканирования файлов. Аналитик может выбрать для профиля безопасности одну из следующих реакций на события прямого доступа к жесткому диску:

– блокировать;

– блокировать запись;

– блокировать запись только для неподписанных программ;

– разрешить.

Также в настройках безопасности файлового монитора можно установить флаги **Подсчитывать хеш SHA-1** и **Подсчитывать хеш MD5**. По умолчанию эти функции отключены, так как создают существенную нагрузку на файловый монитор.

В случае выбора режима «только детектирование» изменение настроек безопасности монитора процессов и файлового монитора будет заблокировано, за исключением выбора режима глубокого сканирования файлов. Доступно четыре режима глубокого сканирования файлов:

1) **Не сканировать**;
2) **ML** (сканирование с помощью машинного обучения);
3) **YARA-правила** (сканирование на основе YARA-правил, созданных в разделе с аналитикой);
4) **ML и YARA-правила**.

По умолчанию также устанавливается режим **Не сканировать**, чтобы снизить нагрузку на файловый монитор.

Совет

Не рекомендуется включать глубокое сканирование в случае совместной работы с антивирусами сторонних вендоров. Это создает значительную нагрузку на файловую систему.

В настройках файлового монитора пользователь может задать расширения файлов с потенциально активным содержимым, которые необходимо проверять при файловом сканировании. Это позволит добавить к сканируемым по дефолтным настройкам PE-файлам файлы с потенциально активным содержимым (PDF, PS1, PSM1 и т.д.), то есть пока расширения скриптов или pdf-файлов не указаны в профиле безопасности агента, сканирование файлов с такими расширениями производиться не будет. При этом необходимо учитывать, что добавление новых расширений приведет к пропорциональному росту нагрузки на файловый монитор.

Если включен режим глубокого сканирования файлов, то аналитик может определить какие исполняемые файлы, с точки зрения их подписи, будут просканированы. Предусматривается 3 режима проверки:

1) Все файлы;

2) Неподписанные файлы (т.е. любая подпись подразумевает доверие), режим включается опцией **Без ЭП**;

3) Неподписанные доверенной подписью файлы (т.е. файлы с доверенными подписями не проверяются, а остальные файлы, в том числе и с подписями отправляются на сканирование), режим включается опцией **Без доверенной ЭП**.

Примечание

Список программ с доверенными подписями содержит проверенное общеупотребительное ПО.

Кроме указанных выше настроек в Программе предусмотрены настройки безопасности сетевого монитора и монитора реестра. Настройки безопасности сетевого монитора включаются и отключаются флагами **Оптимизировать поток сетевых событий**, **Активная защита от сканирования сетевых портов** и **Запретить входящие сетевые подключения**, а настройки монитора реестра флагом **Оптимизировать поток событий реестра**.

Чтобы логика настроек применялась на агентах, для которых установлен профиль безопасности, после его изменения необходимо нажать кнопку **Применить профиль** ().

В некоторых случаях профиль безопасности может иметь некорректный или устаревший формат, его можно исправить, нажав кнопку **Восстановить по умолчанию** или **Актуализировать профиль**. Актуализация профиля необходима, если в профиле безопасности появляются новые параметры со значениями по умолчанию.

Подробное описание опций, доступных в профиле безопасности агента

Опции блока «Оптимизация потока событий»

Исключать файловые события ранней стадии запуска процессов. Ранней стадией запуска процессов считается период разворачивания процесса с момента его старта и до момента начала загрузки им критических системных библиотек (например, ntdll, kernel32 и т.п. в Windows). Если данная опция выставлена, то в обозначенный период файловые события процессов отправляться не будут. Считается, что в этот период работает только код системного загрузчика процессов, а его файловые события нерелевантны в контексте ИБ.

Фильтровать файловые события. Если данная опция выставлена, то из потока исключаются следующие файловые события:

– операции чтения для файлов desktop.ini, *.mui, *.manifest, *.icm со стороны любых процессов;

– операции чтения для файлов tzres.dll, stdole2.tlb, sortdefault.nls, hosts, *.ttf в системном каталоге (подкаталоге) со стороны любых процессов;

– операции чтения/записи файлов в каталогах (подкаталогах) c:\users\<username>\appdata\{local|locallow|roaming} со стороны процессов браузеров;

– операции с именованными каналами mojo.*, crashpad_*, wkssvc со стороны процессов браузеров.

Исключать файловые события префетчера. Префетчер – это компонент ОС, ускоряющий запуск процессов за счет предподготовки определенных данных. Если данная опция выставлена, то файловые события префетчера отправляться не будут. Поскольку префетчер – это доверенный системный компонент, работающий на начальном этапе разворачивания процессов, его файловые события нерелевантны в контексте ИБ.

Исключать события чтения исполняемых файлов, связанные с их исполнением.

Для загрузки исполняемых файлов ОС производит их чтение с диска. Агент может отличить обычное чтение файлов (в т.ч. исполняемых), которое может выполнять любой процесс, от чтения с целью исполнения их кода, которое выполняет сама система, что является менее значимым в контексте ИБ. Поэтому предусмотрена опция, позволяющая полностью исключить из потока подобные файловые события.

Исключать события чтения исполняемых файлов. Система или процессы могут производить чтение исполняемых файлов для тех или иных целей, например, доступ к ресурсам (исполняемые файлы Windows в формате PE) или получение файловых метаданных. Данная опция позволяет исключить из потока такие файловые события.

Исключать события чтения любых файлов. Данная опция позволяет безусловно исключить из потока любые события чтения любых файлов. Поскольку события чтения файлов являются одними из самых массовых, исключение их из потока существенно (кратно) сокращает событийный трафик, однако может сократить возможности аналитика по расследованию инцидентов ИБ.

Исключать файловые события процесса-создателя файла. Если тот или иной процесс создает новый файл на диске, то он в дальнейшем, как правило, записывает в него какие-то данные. Сам факт создания

нового файла в большинстве случаев уже является достаточным в контексте ИБ, поэтому дальнейшую файловую активность процесса-создателя файла в отношении созданного им файла можно исключить, установив данную опцию.

Исключать события доступа к процессам и нитям. Данная опция позволяет безусловно исключить из потока любые события межпроцессного взаимодействия. Поскольку события межпроцессного взаимодействия являются достаточно частыми, исключение их из потока существенно сокращает событийный трафик, однако может сократить возможности аналитика по расследованию инцидентов ИБ.

Исключать события загрузки известных модулей. Данная опция позволяет исключать из потока события загрузки «известных» исполняемых модулей. Поскольку события загрузки исполняемых модулей множатся событиями старта процессов, данная оптимизация позволяет существенно сократить поток событий. К «известным» модулям относятся следующие модули:

1) Модули, подписанные Microsoft Windows или Microsoft Corporation;

2) Модули, чьи хеши или имена файлов внесены в файловые исключения, назначенные агенту, со статусом «Разрешено»;

3) Следующие модули:

– %systemdisk%\windows\system32\shcore.dll;

– %systemdisk%\windows\system32\sechost.dll;

– %systemdisk%\windows\system32\rpcrt4.dll;

– %systemdisk%\windows\system32\combase.dll;

– %systemdisk%\windows\system32\ntdll.dll;

– %systemdisk%\windows\system32\wow64.dll;

– %systemdisk%\windows\system32\wow64win.dll;

– %systemdisk%\windows\system32\wow64cpu.dll;

– %systemdisk%\windows\system32\kernel32.dll;

– %systemdisk%\windows\system32\kernelbase.dll;

– %systemdisk%\windows\system32\advapi32.dll;

– %systemdisk%\windows\system32\msvcrt.dll;

– %systemdisk%\windows\system32\ucrtbase.dll;

– %systemdisk%\windows\system32\gdi32.dll;

– %systemdisk%\windows\system32\user32.dll;

– %systemdisk%\windows\system32\win32u.dll;

– %systemdisk%\windows\system32\comdlg32.dll;

– %systemdisk%\windows\WinSxS*\comdlg32.dll;

– %systemdisk%\windows\system32\comctl32.dll;

– %systemdisk%\windows\WinSxS*\comctl32.dll;

– %systemdisk%\windows\system32\shell32.dll;

– %systemdisk%\windows\system32\shlwapi.dll;

– %systemdisk%\windows\system32\oleaut32.dll;

– %systemdisk%\windows\system32\version.dll;

– %systemdisk%\windows\system32\imm32.dll;

– "%systemdisk%\windows\system32\winmm.dll";

– "%systemdisk%\windows\system32\ws2_32.dll";

– "%systemdisk%\windows\system32\mswsock.dll";

– "%systemdisk%\windows\system32\setupapi.dll";

– "%systemdisk%\windows\system32\dwmapi.dll";

– "%systemdisk%\windows\system32\winspool.drv";

– "%systemdisk%\windows\system32\msctf.dll";

– "%systemdisk%\windows\system32\uxtheme.dll";

– "%systemdisk%\windows\system32\userenv.dll";

– "%systemdisk%\windows\system32\msimg32.dll";

– "%systemdisk%\windows\system32\usp10.dll";

– "%systemdisk%\windows\system32\lpk.dll";

– "%systemdisk%\windows\system32\mscoree.dll";

– "%systemdisk%\windows\system32\bcrypt.dll";

– "%systemdisk%\windows\system32\sspicli.dll";

– "%systemdisk%\windows\system32\sxs.dll";

– "%systemdisk%\windows\system32\windows.storage.dll";

– "%systemdisk%\windows\system32\wininet.dll";

– "%systemdisk%\windows\system32\ole32.dll".

4) Для ОС семейства Linux точный путь до каждого «известного» модуля индивидуален для конкретной ОС (Ubuntu, RedOs, Debian и т. д.), ниже представлен перечень модулей (слева) и пример пути для ОС Ubuntu 20.04 (справа):

– libcap - /usr/lib/x86_64-linux-gnu/libcap-ng.so.*;

– libpcre - /usr/lib/x86_64-linux-gnu/libpcre.so.*;

– libpthread - /usr/lib/x86_64-linux-gnu/libpthread-*.so;

– librt - /usr/lib/x86_64-linux-gnu/librt-*.so;

– libcrypt - /usr/lib/x86_64-linux-gnu/libcrypt.so.*;

– libcrypto - /usr/lib/x86_64-linux-gnu/libcrypto.so.*;

– libdl - /usr/lib/x86_64-linux-gnu/libdl-*.so;

– libgcc - /usr/lib/x86_64-linux-gnu/libgcc_s.so.*;

– libm - /usr/lib/x86_64-linux-gnu/libm.so;

– libc - /usr/lib/x86_64-linux-gnu/libc-*.so, /usr/lib/x86_64-linux-gnu/libc.so;

– libstdc++ - /usr/lib/x86_64-linux-gnu/libstdc++.so.*;

– libz - /usr/lib/x86_64-linux-gnu/libz.so.*;

– libzstd - /usr/lib/x86_64-linux-gnu/libzstd.so.*;

– libselinux - /usr/lib/x86_64-linux-gnu/libselinux.so.*.

Исключать события со статусом "Разрешено" (кроме ключевых). Статус «Разрешено» назначается событиям в результате действия исключений (заданных аналитиком или встроенных в агент). Данная опция позволяет исключать из потока те из событий со статусом «Разрешено», у которых нет ассоциированного с ними правила.

Исключать все события со статусом "Разрешено". Данная опция подразумевает безусловное исключение из потока всех событий со статусом «Разрешено» (вне зависимости от наличия или отсутствия ассоциированного с ними правила).

Исключать события RPC-вызовов. Опция позволяет исключить из потока события источника «Вызовы: RPC».

Фильтровать события модификации реестра. Данная опция управляет режимом отправки событий модификации значений реестра Windows. Если опция установлена, то отправляются только события модификации релевантных с точки зрения ИБ значений реестра (точки автозапуска, настройки безопасности, опции групповых политик и др. – конкретный перечень может меняться от версии к версии агента), что сокращает поток событий без существенного ухудшения защитных свойств системы. Если опция не установлена, то отправляются все без исключения события модификации значений реестра.

Оптимизировать представление стека вызовов в событиях. Данная опция управляет способом представления стэка вызовов в событиях. Если опция задана, то стэк вызовов передается и отображается в компактной форме, где несколько последовательных одинаковых модулей «сворачиваются» в один, а информация о смещениях полностью исключается из стэка вызовов. Такое минималистическое представление позволяет сократить размер передаваемых агентом данных, в то же время оставляя аналитику достаточно возможностей для определения инициатора того или иного события, посредством анализа стека вызовов. Если опция не задана, то стэк вызовов передается и отображается в полном виде – без сокращений.

Принудительно подавлять события процессов при превышении лимита. Данная опция включает/отключает механизм принудительного ограничения потока событий процессов. Если процесс в течение 10 минут генерирует более 100 тысяч событий, то передача на сервер его событий с критичностью **Информация** прекращается на 1 час (события с более высокой критичностью продолжат передаваться). Передача событий процесса возобновляется при назначении ему исключений или их изменении, а также по истечении периода ограничения. Кроме того, предусматривается возможность запрещения принудительного подавления событий с помощью флага **Запрет принудительного подавления событий** исключений для программ.

Важно

При этом необходимо помнить о возможности исключения телеметрии основных источников (процессы, файлы, сеть, реестр) или аналитической активности (файловые и сетевые исключения, а также индикаторы атак) путем указания соответствующего флага в разделе **Исключения для программ**

Фильтрация WMI-событий

Данная опция позволяет выбрать один из режимов фильтрации WMI-событий Windows:

1) Создание процесса – будут доступны только события создания процессов посредством WMI (вызов метода Create объекта класса Win32_Process);

2) Вызов метода – будут доступны только события вызовов методов классов;

3) По ключевым словам – будут доступны события WMI, удовлетворяющие условиям наличия/отсутствия подстрок, перечисленных в соответствующих полях ниже;

4) Не отправлять события – WMI-события полностью исключаются из потока.

В любых режимах фильтрации внутренняя аналитика, направленная на выявление техник закрепления в системе Windows посредством WMI, продолжает работать.

Опции блока «Общие настройки безопасности»

Режим "только детектирование" (противодействие угрозам в режиме реального времени на агенте отключено). Если режим «только детектирование» включен, то все блокирующие реакции переопределяются агентом на «детектирование». В этом случае в поле **Причина предпринятого действия** события делается соответствующая пометка, которая позволяет понять, что то или иное событие не заблокировано из-за включенного режима «только детектирование», но будет блокироваться в «боевом» режиме. Такой режим работы агента может использоваться в двух сценариях:

– начальный период развертывания EDR, когда аналитиками изучается профиль событий новой информационной системы и подавляются ложные срабатывания;

– демонстрационный режим, позволяющий наблюдать этапы развития атаки и оценивать возможности агента по детектированию/реагированию на каждом этапе (в «боевом» режиме атака была бы заблокирована на раннем этапе).

Опции блока «Настройки безопасности монитора процессов»

Реакция на создание нити в стороннем процессе (кроме авторизованных программ Windows). Данная опция управляет политикой агента для Windows в отношении внедрения кода одним процессом в другой (сторонний). Указанная здесь критичность будет использована при формировании агентом события внедрения кода. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке внедрения кода.

Действие определяет автоматизированную реакцию на внедрение кода со стороны агента. Логика опции не распространяется на программы, у которых есть право внедрения кода в сторонние процессы, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Реакция на доступ к стороннему процессу/нити (кроме авторизованных программ Windows). Данная опция управляет политикой агента для Windows в отношении доступа одного процесса к другому процессу (стороннему) или его нити (потоку). Указанная здесь критичность будет использована при формировании агентом события доступа. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке доступа. Действие определяет автоматизированную реакцию на доступ со стороны агента. Логика опции не распространяется на программы, у которых есть право доступа к сторонним процессам/нитям, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Оптимизировать поток событий межпроцессного взаимодействия. Оптимизация потока событий межпроцессного взаимодействия заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Опции блока «Настройки безопасности файлового монитора»

Реакция на прямой доступ к жесткому диску (кроме авторизованных программ Windows). Данная опция управляет политикой агента для Windows в отношении прямого доступа того или иного процесса к жесткому диску для его чтения или записи. Указанная здесь критичность будет использована при формировании агентом события доступа. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке доступа. Действие определяет автоматизированную реакцию на доступ со стороны агента. Логика опции не распространяется на программы, у которых есть право доступа к жесткому диску, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Подсчитывать хеш SHA-1. По умолчанию агент при обработке файлов с потенциально активным содержимым подсчитывает хеш SHA-256. Данная опция заставляет его подсчитывать еще и хеш SHA-1, а также проводить матчинг файловых индикаторов компрометации и исключений соответствующего типа. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Подсчитывать хеш MD5. По умолчанию агент при обработке файлов с потенциально активным содержимым подсчитывает хеш SHA-256. Данная опция заставляет его подсчитывать еще и хеш MD5, а также проводить матчинг файловых индикаторов компрометации и исключений соответствующего типа. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Режим глубокого сканирования файлов. Обязательная часть анализа со стороны агента для всех файлов с потенциально активным содержимым включает в себя подсчет хеш-сумм, матчинг индикаторов компрометации и файловых исключений. Для файлов формата PE (Windows Portable Executable) дополнительно производится разбор электронной подписи и метаинформации о файле. Глубокое сканирование подразумевает дополнительные проверки – YARA-правила и/или статический анализ на основе машинного обучения (ML), способный выявить характерные признаки вредоносного файла с использованием технологий искусственного интеллекта. Следует иметь в виду, что сканирование с использованием ML может давать большое количество ложных срабатываний. YARA-правила являются эффективным средством сигнатурного анализа и позволяют

выявить известные угрозы. При выборе данной опции для сканирования будет использован набор YARA-правил, назначенный агенту. Большое количество YARA-правил может замедлить работу системы.

Не обрабатывать файлы *.ni.dll (нативные образы .NET Framework). Файлы нативных образов .NET Framework создаются в результате предкомпиляции утилитой NGEN управляемых (managed) образов для ускорения работы .NET-приложений. При каждой перекомпиляции меняется хеш-сумма нативного образа даже несмотря на то, что исходный управляемый образ не изменялся. Это приводит к многочисленным проверкам по сути одного и того же файла (хеш меняется из-за изменения метаданных) и «засорению» кеша (cash trashing) модуля мониторинга файловой активности агента, что в конечном итоге оказывает негативный эффект на производительность агента в целом. Кроме того, многочисленные вариации хеш-сумм одного и того же файла отправляются для проверки на ti-платформу и учитываются в подсистеме мониторинга распространения, что тоже создает избыточную нагрузку на эти модули. Данная опция отключает обработку со стороны агента нативных образов .NET Framework – подсчет хешей, матчинг исключений и индикаторов, и отправку соответствующих событий в поток.

Оптимизировать поток файловых событий. Оптимизация потока файловых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Расширения файлов с потенциально активным содержимым

По умолчанию файловая аналитика (подсчет хешей, матчинг индикаторов и др.) производится только для исполняемых файлов и только при их запуске (или загрузке, если исполняемый файл – это динамически загружаемая библиотека). Данная опция позволяет дополнительно указать расширения файлов (помимо исполняемых), для которых также требуется включить файловый анализ, который будет производиться в режиме реального времени при доступе к ним.

Примечание

Расширения должны указываться без точки перед ними и не зависят от регистра.

Опции блока «Настройки безопасности сетевого монитора»

Оптимизировать поток сетевых событий. Оптимизация потока сетевых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Активное противодействие сканированию портов. Данная опция включает режим эмуляции открытых TCP-портов таким образом, что при сканировании все TCP-порты выглядят открытыми. Это существенно затрудняет для злоумышленника идентификацию работающих сетевых сервисов, снижает вероятность атаки на них и осложняет горизонтальное распространение в сети.

Запретить все входящие подключения. При включении данной опции все входящие TCP-подключения будут отвергаться. Если агент не выполняет роль сервера в информационной системе, то в целях безопасности все входящие подключения к нему можно запретить.

Отправлять события ICMP. При включении данной опции в поток событий будут включаться события сетевого взаимодействия по протоколу ICMP.

Опции блока «Настройки безопасности монитора реестра»

Оптимизировать поток событий реестра. Оптимизация потока событий реестра заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

10.20.3. Профили контроля USB

Профили контроля USB работают для агентов, устанавливаемых на конечных точках с ОС Windows, и позволяют управлять различными устройствами, присоединяемыми к конечным точкам посредством USB-интерфейса. Контроль осуществляется как над отдельными устройствами, так и над их классами:

1) Накопители;
2) Медиа-устройства;
3) Принтеры;
4) Сканеры;
5) Беспроводные устройства;
6) Коммуникационные устройства и мобильные телефоны;
7) Устройства взаимодействия с пользователями (HID-устройства);
8) Прочие устройства.

Под управлением понимается задание различных разрешений для выбранных устройств: на чтение, запись, запуск программ с устройства, сбор статистики операций ввода/вывода или блокирование устройства. При этом в потоке событий будут формироваться события, связанные в том числе с нарушением разрешающей

политики, например, пользователь попытается запустить программу с USB-накопителя при наличии соответствующего запрета на запуск, что приведет к формированию события на странице **Активность.**

Доступны следующие типы событий:

1) Устройство USB подключено;
2) Устройство USB отключено;
3) Зафиксирована запрещенная попытка чтения;
4) Зафиксирована запрещенная попытка записи;
5) Зафиксирована запрещенная попытка выполнения управляющего запроса;
6) Зафиксирована запрещенная попытка запуска исполняемого кода;
7) Статистика чтения/записи данных.

Страница «Профили контроля USB»

На странице отображается таблица с профилями с тремя основными полями:

1) **Название профиля**;
2) **Привязано агентов** (показывает, сколько агентов работает с этим профилем);
3) **Управление** (содержит кнопки управления профилем).

На странице можно выполнить следующие операции:

1) Добавлять профили контроля USB;
2) Применить все профили, созданные и сохраненные на странице, а также отдельный профиль;
3) Редактировать название профиля;
4) Удалить профиль.

Чтобы добавить профиль, необходимо нажать кнопку **Добавить профиль**. Откроется окно **Добавить профиль**. Обязательной для заполнения является строка **Название**. Можно добавить любой из ранее созданных профилей в качестве базового профиля, но это действие является необязательным.

Для удаления профиля необходимо нажать кнопку  или воспользоваться групповым удалением, выделив соответствующие профили и нажав кнопку **Удалить выбранные профили**.

Для применения всех профилей, имеющихся на странице **Профили контроля USB**, возможно нажать по кнопке  .

Страница «Профиль контроля USB»

Страница **Профиль контроля USB** разделена на две основные области:

1) Базовые настройки;

2) Конфигурации контроля USB-устройств.

Базовой настройкой является то, включена ли подсистема контроля USB-устройств или нет. Включение выключение осуществляется с помощью кнопок  / .

В области конфигурации контроля USB-устройств по умолчанию представлены общие универсальные конфигурации устройств.

Пользователь может добавить уникальную конфигурацию, нажав кнопку **Добавить правило**. Откроется окно **Создание правила контроля устройства USB**. Здесь нужно ввести информацию об уникальном идентификаторе устройства в формате **VID_PID_MI_SERIAL** или группы устройств в формате **VID_PID_MI**, эту информацию об устройствах можно узнать на странице **Активность** в событии **Устройство USB подключено.**

VID – идентификатор производителя в шестнадцатеричном формате (2 байта).

PID – идентификатор продукта в шестнадцатеричном формате (2 байта).

MI – номер интерфейса в шестнадцатеричном формате (1 байт, задается опционально, если у устройства есть несколько интерфейсов).

SERIAL – серийный номер устройства (задается опционально в виде строки без пробелов).

После ввода уникального идентификатора следует выбрать тип контролируемого устройства и добавить необходимые разрешения, по умолчанию устройство будет заблокировано. Возможно установить следующие разрешения:

1) На чтение;

2) На запись;

3) На запуск программ;

4) На получение статистики операций ввода/вывода.

Для завершения операции по добавлению правила необходимо нажать кнопку **Создать**.

Примечание

Номер интерфейса может быть не задан, если у устройства отсутствует интерфейс или требуется задать правило для всех интерфейсов.

Если серийный номер не задан, то правило будет применяться ко всем устройствам заданного производителя с указанным кодом продукта.

Уникальные конфигурации, в отличие от универсальных (они выделяются желтым цветом на странице), можно удалять, для этого в строке с конфигурацией присутствует кнопка  или можно воспользоваться групповым удалением, выделив нужные правила и нажав кнопку **Удалить выбранные**.

Для редактирования любых конфигураций в каждой из них присутствует кнопка  .

Для сохранения изменений и последующего применения профиля требуется нажать по кнопке  , после чего откроется окно подтверждения действия. После того, как пользователь нажмет по кнопке **Подтвердить**, профиль будет применяться для назначенного агента.

На странице профиля имеется возможность для импорта/экспорта данных из профиля в формате txt.

Данные кнопки имеют вид:

–  – экспортировать профиль в файл формата txt;

–  – импортировать данные из файла в профиль (формат txt).

Конфигурации в профиле можно активировать и деактивировать по отдельности или группой. Для выполнения операций по отдельности используются кнопки **Деактивировать/Активировать** (). Каждая операция требует подтверждения. Для активации/деактивации группы конфигураций необходимо отметить их флагом () и нажать кнопку группового применения **Активировать выбранные элементы** () или **Деактивировать выбранные элементы** ().

Быстрое создание конфигураций контроля USB на странице «Активность»

Для событий, источником которых является модуль контроля USB, конфигурационное правило может быть добавлено с помощью мастера создания правил для USB-устройств на странице **Активность**. Для этого в

каждой строке события, источником которого является **Контроль USB**, присутствует кнопка . Нажатие кнопки открывает окно **Мастер создания правил для USB-устройств** с предзаполненными полями **Уникальный идентификатор** (VID_PID_MI_SERIAL), **Тип устройства** и полем **Профиль**, в котором можно выбрать профиль для сохранения правила. Уникальный идентификатор отличается в зависимости от типа устройства, например, может отсутствовать номер интерфейса или серийный номер.

При нажатии кнопки **Далее** открывается окно **Создание правила контроля USB-устройства**, в котором необходимо установить разрешения для выбранного устройства. Для завершения операции необходимо нажать кнопку **Создать**, после чего новая конфигурация появится на странице выбранного профиля контроля USB.

10.21 Журнал действий пользователей

В журнале действий аналитик может просмотреть информацию, связанную с действиями пользователей в модуле управления. Это может быть полезно аналитику, чтобы выяснить, кто был инициатором назначения инцидента, его закрытия, кто ответственен за изменение тех или иных параметров сервера управления или выполнил другие действия. Все возможные действия разделяются на типы и подтипы.

Для типа действия **Авторизация пользователя** предусмотрены следующие подтипы:

– вход в систему;

– выход из системы;

– выход из системы на всех устройствах.

Для типа действия **Работа с пользователем** предусмотрены следующие подтипы:

– создание нового пользователя;

– изменение пароля пользователя;

– удаление пользователя из системы;

– блокировка пользователя;

– разблокировка пользователя;

– запрос ссылки для сброса пароля;

– сброс пароля пользователя.

Для типа действия **Работа с агентом** предусмотрены следующие подтипы:

– отмена верификации агента;

– добавление агентов в группу;

– удаление агентов из группы;

– верификация агентов;

– отправка команды агенту;

– отправка команды группе агентов;

– загрузка нового дистрибутива агента на сервер;

– удаление дистрибутива агента с сервера;

– сетевая изоляция агентов;

– функции защиты агента выключены;

– выключение автоматического обновления агентов;

– выключение сопоставления с золотым образом;

– выключение парольной защиты от удаления агентов;

– снятие сетевой изоляции агентов;

– функции защиты агента включены;

– включение автоматического обновления агентов;

– включение сопоставления с золотым образом;

– включение парольной защиты от удаления агентов;

– назначение агентам набора исключений для файлов;

– назначение агентам набора исключений для программ;

– назначение агентам набора индикаторов компрометации;

– назначение агентам набора журналов Windows;

– назначение агентам набора YARA-правил (файлы);

– назначение агентам набора YARA-правил (память);

– назначение агентам набора индикаторов атак;

– назначение агентам профиля защиты данных;

– назначение агентам профиля безопасности;

– назначение агентам профиля контроля USB-устройств.

Для типа действия **Конфигурация** предусмотрены следующие подтипы:

– создание нового набора;

– удаление набора;

– добавление новых данных в набор;

– удаление данных из набора;

– импорт данных в набор;

– редактирование данных в наборе;

– копирование данных между наборами;

– перемещение данных между наборами.

Для типа действия **Работа с файлами агента** предусмотрены следующие подтипы:

– загрузка файла агента на сервер;

– удаление файла агента с сервера;

– загрузка файла пользователя на сервер;

– удаление файла пользователя с сервера.

Для типа действия **Работа с инцидентом** предусмотрены следующие подтипы:

– создание инцидента;

– смена ответственного за инцидент;

– закрытие инцидента;

– назначение инцидента;

– удаление инцидента;

– добавление событий в инцидент;

– исключение событий из инцидента.

Для типа действия **Действие с лицензией** предусмотрен следующий подтип:

– установка новой лицензии на сервере.

10.22 Дистрибутивы

Сборки агентов, сохраняемые на странице с дистрибутивами, позволяют обновлять агентов в автоматическом режиме, если у них включена опция **Автообновление** на странице **Агент** или **Агенты** (опция

включается по умолчанию при верификации новых агентов). На странице **Дистрибутивы** отображается информация о Windows и Linux-дистрибутивах агента в виде таблицы со следующими полями (рис. 115):

1) Имя (содержит название дистрибутива агента);
2) Версия;
3) Дата изменения;
4) Размер (показывает размер файла дистрибутива агента);
5) Платформа (показывает название ОС, на которую устанавливается дистрибутив агента);
6) Архитектура (показывает разрядность ОС, на которую устанавливается дистрибутив агента);
7) Управление (содержит кнопку скачивания дистрибутива).

При нажатии кнопки скачивания дистрибутива произойдет сохранение выбранного дистрибутива на хост, с которого осуществлен доступ к серверу управления.

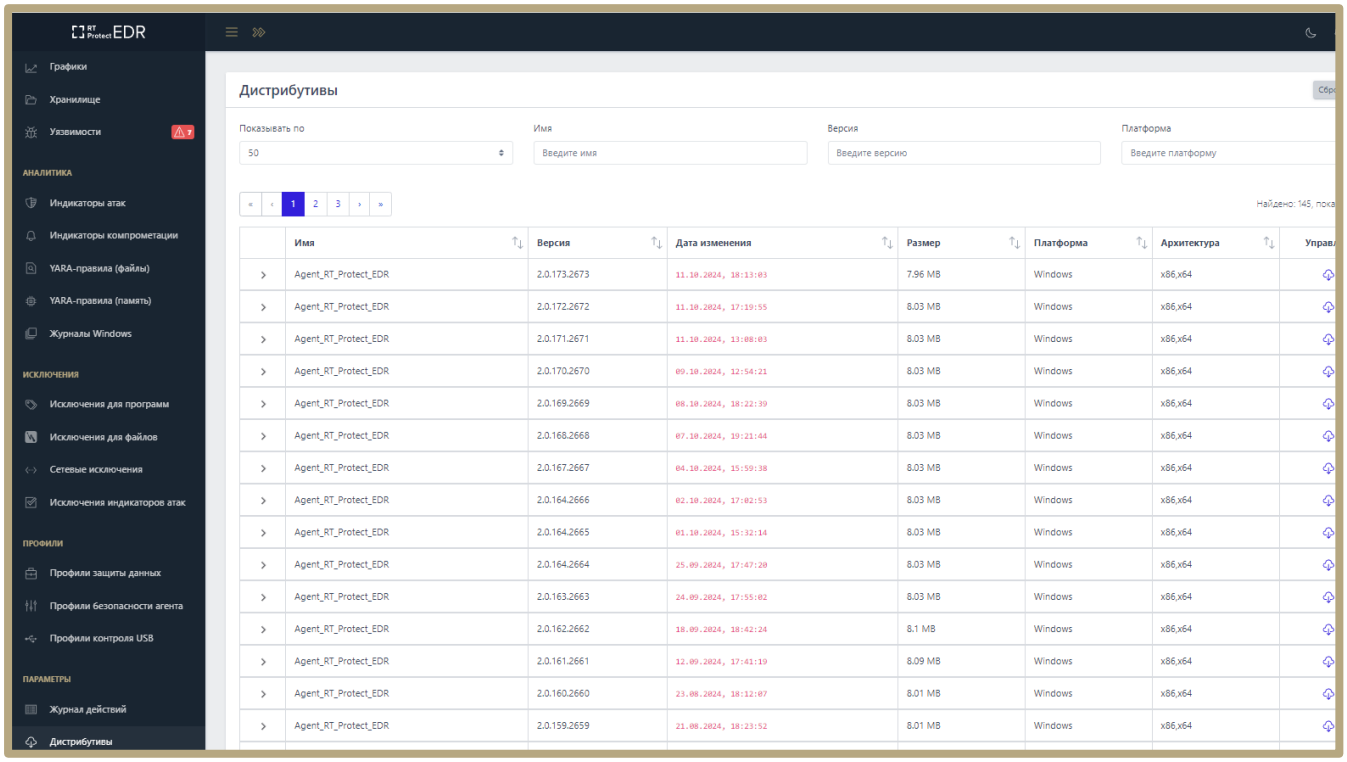


Рисунок 115 – Дистрибутивы

С помощью элемента > рядом с названием дистрибутива агента можно просмотреть дополнительную информацию:

1) Минимальная версия целевой платформы;

2) Описание (содержит описание изменений дистрибутива по сравнению с предшествующей версией);

3) MD5 (содержит 32-х символьное значение хеша для дистрибутива агента, рассчитанного по алгоритму MD5).

4) Кнопки просмотра лога изменений дистрибутива для фронтенда и бэкенда.

На странице **Дистрибутивы** для фильтрации информации имеется система фильтров, которая представлена следующими фильтрами:

– Показывать по (изменяется количество записей в таблице);

– Имя (данные фильтруются по имени агента);

– Версия (данные фильтруются по номеру версии дистрибутива агента);

– Платформа (данные фильтруются по имени целевой платформы: версии Linux, Windows).

При нажатии кнопки 

происходит сброс выставленных фильтров.

11. Машинное обучение в Программе

11.1 Классификация на сервере

В RT Protect EDR реализован статистический анализ инцидентов на основе ИИ. Модель состоит из encoder-трансформера на основе RoBERTa и полносвязной нейронной сети, на вход которой поступают исходные данные инцидентов информационной безопасности (рис. 116). Данная архитектура модели выбрана в связи с большим количеством текстовых признаков, присущих инцидентам. Модель представляет собой отдельный модуль, взаимодействие с которым происходит с помощью API-вызовов. Входным параметром данного модуля является текст, содержащий в себе один или несколько JSON-объектов. Дальнейшие преобразования включают в себя проверку на валидность переданных объектов, нормализацию JSON, агрегацию нескольких JSON в один (в случае, если на вход модуля поступило несколько связанных объектов), фильтрацию полей и приведение их названий к общему виду, а также обогащение с помощью RT Protect TI и дополнительной информации из источника данных Elastic, не вошедшей в исходные JSON-объекты. К признакам, используемым для работы модели машинного обучения, относятся: сработавшее правило, название организации, имя пользователя, командная строка процесса (а также родительского и прародительского процессов), имя модуля-инициатора, путь к модулю-инициатору, путь к запущенному приложению, результаты проверок индикаторов компрометации (sha256, md5, IP-адреса, домены, url), информация о локальном/удалённом хосте, IP-адреса задействованных хостов, описание данных хостов, изменения реестра Windows. Все перечисленные значения опциональны, что позволяет классифицировать различные инциденты информационной безопасности, которые, из-за своей специфики, могут иметь лишь те или иные признаки.

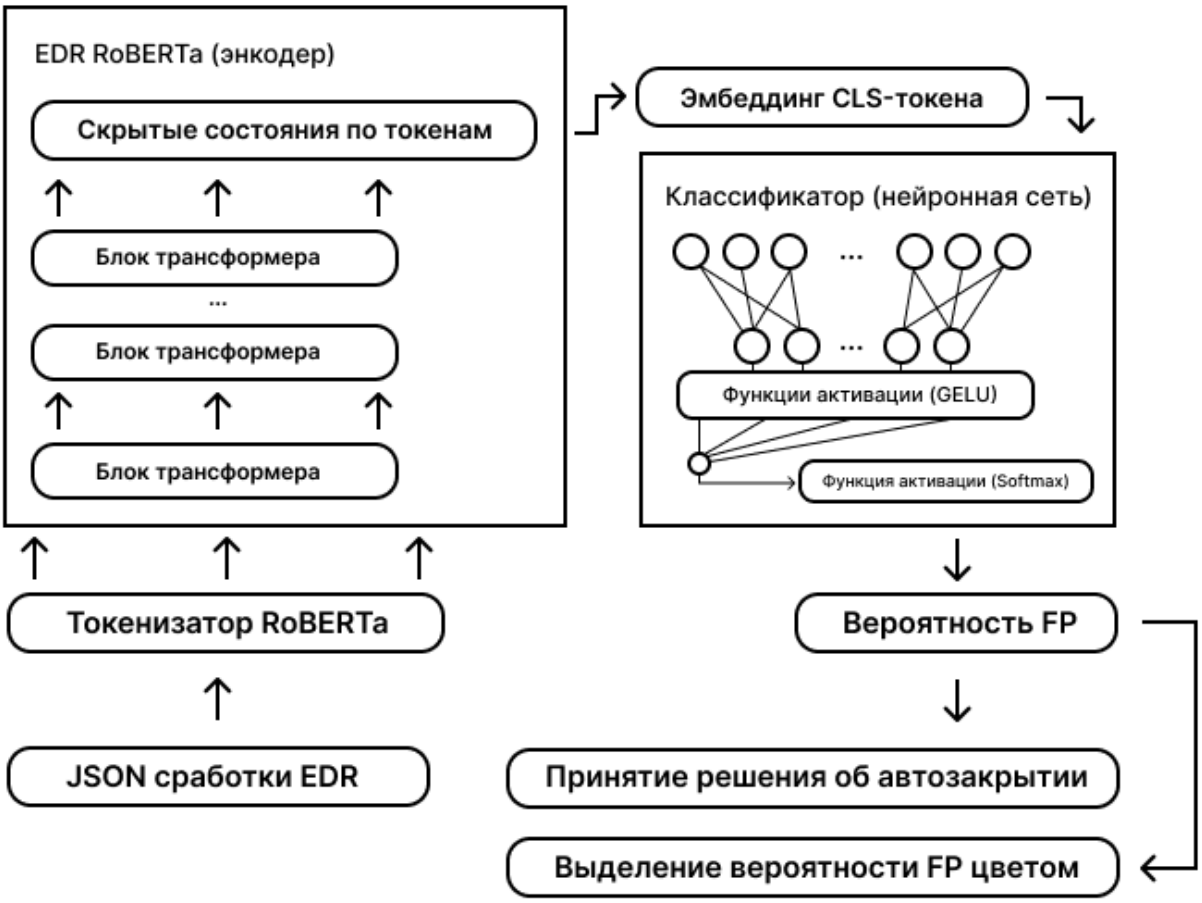


Рисунок 116 – Схема применения модели классификации инцидентов

После данного этапа происходит классификация инцидента. В качестве результата выдается значение в диапазоне [0;1], соответствующее вероятности того, что инцидент является ложноположительным срабатыванием, а также идентификатор autoClose, определяющий, можно ли автоматически закрыть данный инцидент. Модель содержит в себе несколько порогов срабатывания, которые уточняются при переобучении модели. Первая группа порогов содержит один порог (приблизительно от 0.9 до 0.95), который говорит о том, что инцидент является ложным срабатыванием правила и должен быть автозакрыт. Второй тип порогов (примерно 0.3, 0.5 и 0.7) используется для сопоставления инциденту цветовой метки («Красный», «Оранжевый», «Жёлтый» или «Зелёный»), отражающей серьёзность инцидента. Вердикт модели передается как ответ API-вызова, который обрабатывается SOAR-системой для автоматического закрытия инцидента или добавления цветовой метки, использующейся для составления приоритета обработки инцидентов аналитиками первой линии.

Сама модель представляет собой конфигурационные файлы в формате safetensors и json, которые содержит в себе веса признаков модели, словарь токенизатора модели, а также пороговые значения

вынесения вердиктов автозакрытия и соответствия цветовым меткам. Эти файлы формируются в результате обучения модели в тестовой лаборатории в автоматическом режиме с помощью Airflow, что позволяет модели оставаться актуальной с течением времени.

Обучение модели производится на языке python с использованием библиотек scikit-learn, pytorch и transformers. В качестве обучающих выборок используется собственные наборы данных. Первый из них это набор данных для обучения без учителя, используемый для получения качественного численного представления посредством моделей, основанных на Bert-архитектуре, а второй уже является набором данных для обучения с учителем roBERTa-подходом с целью оптимизации классификатора над признаками, полученными из Bert-модели.

11.2 Классификация на агенте

В RT Protect EDR реализован статический анализ исполняемых файлов на основе ИИ. В частности, применяется модель логистической регрессии, на вход которой поступают статические признаки исполняемых файлов. Данный тип модели выбран ввиду ее быстродействия и минимальных требований к вычислительным ресурсам, поскольку она работает в синхронном режиме на агентских компьютерах.

Далее будет описана схема применения модели классификации ПО, применяемая в агенте RT Protect EDR (рис. 117).

Для отслеживания запуска файлов на исполнение драйвер агента в обработчике открытия файлов анализирует флаги открытия файла.

При наличии запрашиваемого доступа «на исполнение» (FILE_EXECUTE), модуль минифильтра драйвера открывает секцию файла (для его последующего чтения в службе) и передает задачу на анализ файла службе агента посредством специального порта взаимодействия (CommunicationPort). Служба, получив задание на анализ файла, передает управление в модуль сбора признаков исполняемого файла. К признакам, необходимым для модели машинного обучения, относятся: физический и виртуальный размер файла (в байтах), флаги из заголовков исполняемого файла (PE-headers), наличие оверелея, имя секции, содержащей точку входа программы, энтропия файла, количество url-строк, количество строк-путей, количество сигнатур ‘MZ’, количество экспортируемых и импортируемых функций, имена секций и др.

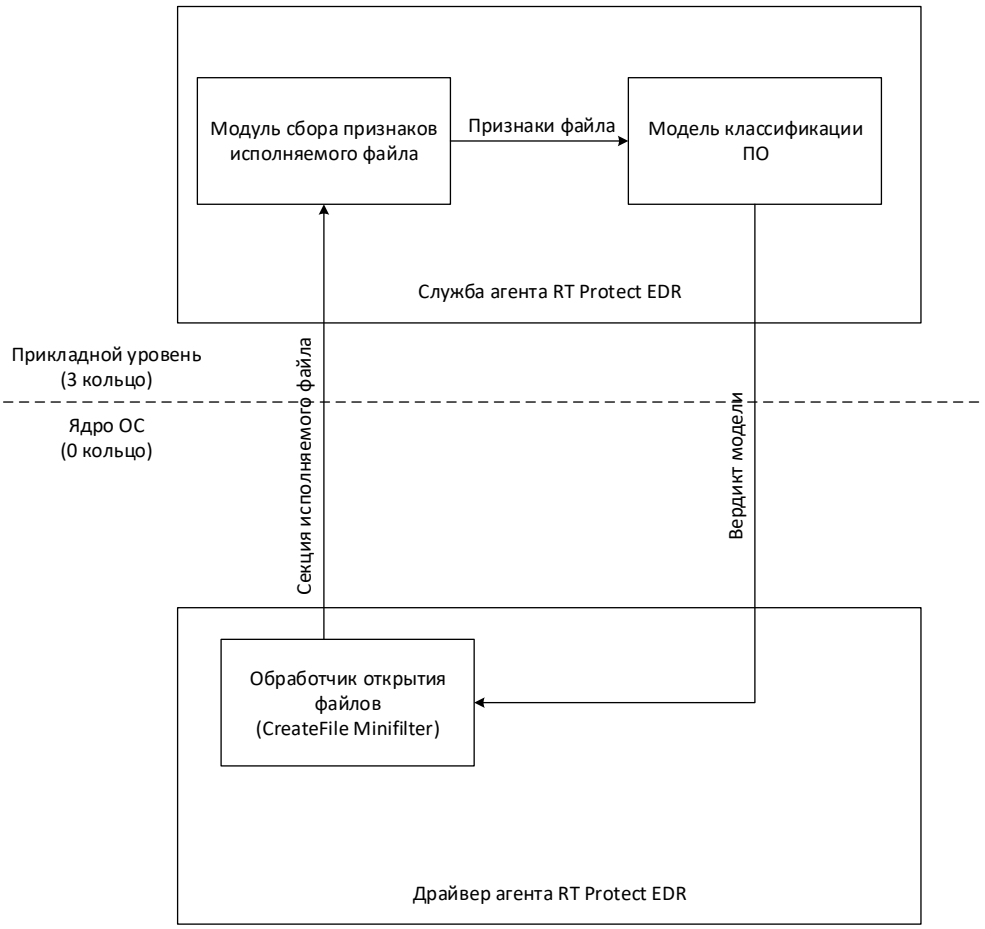


Рисунок 117 – Схема применения модели классификации ПО

После сбора перечисленных признаков вызывается функция классификации файла. На вход она принимает собранные признаки. В качестве результата выдает значение в диапазоне [0;1], соответствующее вероятности того, что файл является вредоносным. Модель содержит в себе 2 порога срабатывания, которые уточняются от версии к версии модели. Первый более низкий порог (приблизительно от 0.8 до 0.9) говорит о том, что файл подозрительный, второй (ближе к 1) – файл вредоносный. Вердикт модели передается обратно в драйвер, который на его основе выполняет предписываемые действия: пропустить, отправить предупреждение (alert) или заблокировать запуск файла с уведомлением.

Сама модель представляет собой конфигурационный файл в формате json, который содержит в себе веса признаков, а также пороговые значения вынесения вердикта. Это файл формируется в результате обучения модели в тестовой лаборатории, а затем загружается на сервер EDR. В свою очередь сервер EDR рассылает конфигурационный файл модели по агентам.

Обучение модели производится на языке python с использованием библиотеки sklearn. В качестве обучающих выборок используется наборы: sophos/SOREL-20M (https://github.com/sophos/SOREL-20M), bodmas (https://github.com/whyisyoung/BODMAS), Malware Dataset IDN (https://ieee-dataport.org/documents/malware-dataset-idn), а также собственный набор файлов, собранных в тестовой лаборатории.

11.3 Список компонентов, используемых в модели ИИ

Полный список сторонних компонентов, используемых в модели машинного обучения, приведен в таблице 59.

Таблица 59 – Сторонние компоненты

№ п/п	Наименование стороннего компонента	Правообладатель	Сведения о документах, подтверждающих наличие оснований на использование компонента	Лицензии	Вид лицензии
1	scikit-learn	The scikit-learn developers	https://github.com/scikit-learn?tab=BSD-3-Clause-1-ov-file#readme	BSD 3-Clause	Свободная лицензия
2	pytorch	Facebook, Inc, Idiap Research Institute, Deepmind Technologies, NEC Laboratories America, NYU	https://github.com/pytorch/pytorch/blob/main/LICENSE	BSD-Style	Свободная лицензия
3	pandas	AQR Capital Management, LLC, Lambda Foundry, Inc. and PyData Development Team, Open source contributors	https://github.com/pandas/dev/pandas/blob/main/LICENSE	BSD 3-Clause	Свободная лицензия
4	numpy	NumPy Developers	https://github.com/numpy/numpy/blob/main/LICENSE.txt	numpy	Свободная лицензия
5	transformers	The Hugging Face team	https://github.com/huggingface/transformers/blob/main/LICENSE	Apache License 2.0	Свободная лицензия
6	fastapi	Sebastián Ramírez	https://github.com/fastapi/fastapi/blob/master/LICENSE	MIT	Свободная лицензия
7	uvicorn	Encode OSS Ltd.	https://github.com/encode/uvicorn?tab=BSD-3-Clause-1-ov-file	BSD 3-Clause	Свободная лицензия
8	joblib	The joblib developers	https://github.com/joblib/blob/main/LICENSE.txt	BSD 3-Clause	Свободная лицензия

12. Создание аналитики на основе MITRE CAR

12.1 Общая информация

Реестр методов обнаружения угроз в сфере кибербезопасности (CAR) MITRE – это база знаний с аналитикой, основанной на модели угроз MITRE ATT&CK.

Данные модели CAR записаны псевдокодом, но могут также включать другие реализации.

Представленная в CAR аналитика содержит следующую информацию:

1) Гипотезу, которая описывает идею аналитического решения;
2) Информационную область, для которой метод обнаружения угрозы был разработан;
3) Ссылки на тактики и техники ATT&CK, которые обнаруживает аналитика;
4) Словарь терминов;
5) Описание на псевдокоде алгоритма того, как аналитический метод может быть внедрен в реальных условиях;
6) Модульный тест, с помощью которого может проверяться аналитическое решение.

Вместе с аналитическими методами обнаружения угроз CAR содержит модель данных для запуска аналитики и сенсоры, которые используются для сбора этих данных.

Интерпретируя псевдокод, можно создавать индикаторы атак в RT Protect EDR. Для этого необходимо, следуя описанию аналитического метода обнаружения угроз и алгоритму, прописанному в шагах псевдокода, записать его в виде индикатора атак в разделе **Индикаторы атак**.

12.2 Пример написания индикатора атаки

Рассмотрим пример с написанием правила для метода обнаружения угроз CAR-2020-11-009: **Доступ к скомпилированному HTML**.

В описании к методу указано, что злоумышленники могут прятать вредоносный код в файлах .chm, когда эти файлы читаются, Windows использует утилиту hh.exe. Запуск утилиты необходимо обнаруживать с помощью индикатора атаки.

В качестве имени индикатора необходимо прописать произвольное значение, например, **RT_win_hh**.

В строке **Критичность** указать низкий уровень критичности.

В строке **Тип индикатора** в качестве типа индикатора атаки необходимо указать **Процессы: старт процесса**.

В строке **Действие** указать значение **детектировать**, а в качестве идентификатора в строке **MITRE «T1218\001»**. Далее выбрать один из режимов обнаружения ИА (обычный, без генерации обнаружения или с однократной генерацией обнаружения).

В поле **Описание** и **Комментарий** можно добавить соответствующие записи для разъяснения созданного правила.

В строке **Условие** необходимо написать, что должно обнаруживаться событие создания процесса hh.exe. В RT Protect EDR лучше всего это сделать с помощью флагов исполняемого файла процесса (exclf).

После описания условий можно проверить его с помощью проверки синтаксиса (кнопка </>), после чего необходимо сохранить правило, нажав кнопку **Добавить** (рис. 118). После сохранения правила в нижней части страницы появится всплывающее окно с сообщением о том, что правило добавлено.

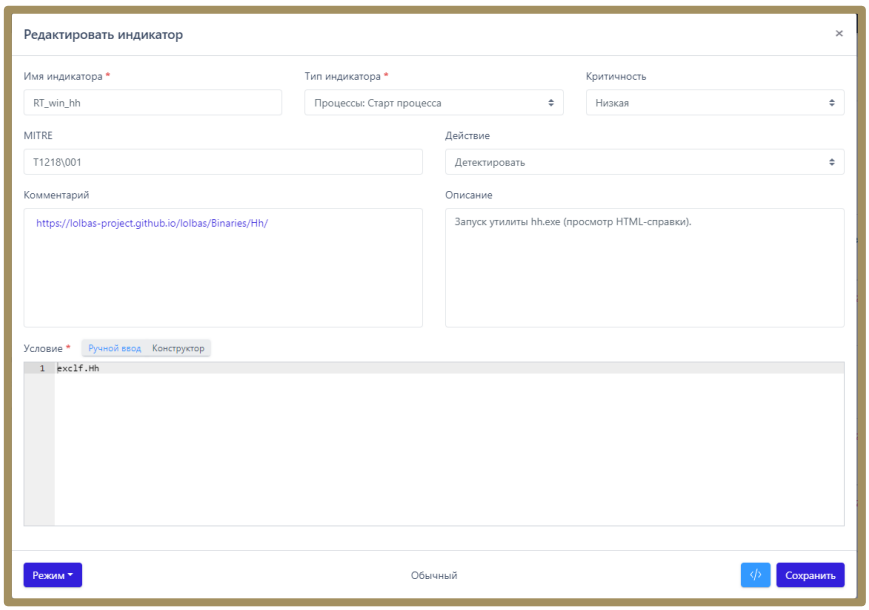


Рисунок 118 – Правило, обнаруживающее запуск hh.exe

После закрытия окна **Добавить индикатор** на странице **Индикаторы атак** появится новая строка с созданным правилом. Для применения правила в наборе необходимо нажать кнопку  внизу страницы.

После сохранения правила следует назначить набор с этим правилом для агентов, на которых будет детектироваться активность, описанная в наборе. Для этого необходимо перейти в раздел **Агенты** и выбрать в списке нужных агентов. Далее нажать кнопку  , откроется окно **Выбор набора**, после чего в строке **Индикаторы атак** выбрать из выпадающего списка набор с правилом **RT_win_hh** и нажать кнопку **Сохранить**.

После обновления аналитических наборов на соответствующих агентах любой запуск утилиты hh.exe на конечных точках с агентами приведет к обнаружению этого события Программой и созданию соответствующей записи на странице **Активность**. Так как в нашем случае указан уровень критичности **Низкая**, то создаваться инцидент не будет (инциденты создаются для событий с уровнем критичности **Средняя** или выше).

13. Перечень сокращений

Аббревиатура	Расшифровка
ГОСТ	Государственный стандарт
ИА	Индикаторы атак
ИК	Индикаторы компрометации
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Средство обнаружения вторжений
ФСТЭК	Федеральная служба по техническому и экспортному контролю
APT	Advanced Persistent Threat
ASCII	American standard code for information interchange
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
C2 (C&C)	Command and Control
CAR	Cyber Analytics Repository
DLL	Dynamic Link Library
DNS	Domain Name System
DSL	Domain-specific language
EDR	Endpoint Threat Detection & Response
ETW	Event Tracing for Windows
FTP	File Transfer Protocol
HEX	Hexadecimal
HTTP	Hyper Text Transfer Protocol
IOA	Indicator of Attack
IOC	Indicator of Compromise
JSON	Java Script Object Notation
ML	Machine Learning
NTFS	New Technology File System
PE	Portable Executable
RAT	Remote Access Trojan
RPC	Remote Procedure Call
SHA-256	Secure Hash Algorithm
SOC	Security Operations Center
SSL	Secure Sockets Layer
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TLSH	Trend Locality Sensitive Hash
TTP	Tactics, Techniques, and Procedures
UAC	User Access Control

Аббревиатура	Расшифровка
UUID	Universally Unique Identifier
WMI	Windows Management Instrumentation

14. Перечень терминов и определений

Термин	Расшифровка термина
Аналитик безопасности	Человек, который занимается анализом информационных рисков компании, разрабатывает и внедряет мероприятия по их предотвращению. В его обязанности также может входить установка, настройка и сопровождение технических средств по защите данных.
Белая команда	Группа лиц, которая является связующим звеном между красной и синей командой, помогая им в разработке стратегии нападения и мер защиты.
Брандмауэр	Технологический барьер, предназначенный для предотвращения несанкционированного или нежелательного сообщения между компьютерными сетями или хостами.
Дамп памяти	Содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы, например, значения регистров процессора и содержимое стека.
Диспетчер служб	Особый системный процесс, реализующий технологию удалённого вызова процедур (RPC). Обеспечивает создание, удаление, запуск и остановку служб ОС. Стартует при загрузке системы, обеспечивает работу журнала событий, а также позволяет выполнять манипуляцию процессами удалённой машины.
Именованный канал	Именованный односторонний или дуплексный канал для обмена данными между сервером канала и одним или несколькими клиентами канала. Все экземпляры именованного канала имеют одно и то же имя канала, но каждый экземпляр имеет собственные буферы и дескрипторы и предоставляет отдельный канал для обмена данными между клиентом и сервером. Использование экземпляров позволяет нескольким клиентам канала одновременно использовать один и тот же именованный канал.
Исполняемый модуль процесса	Набор инструкций, загружаемый в виде исполняемого файла или dll в процесс.
Корреляция событий	Метод для понимания большого количества событий и выявления немногих событий, которые действительно важны в этой массе информации.
Красная команда	Группа лиц, которая выполняет комплексную имитацию реальных атак с целью оценки кибербезопасности атакуемых систем.
Матчинг	Метод анализа и обработки структур данных в языках программирования, основанный на выполнении определённых инструкций в зависимости от совпадения исследуемого значения с тем или иным образцом, в качестве которого может использоваться константа, предикат, тип данных или иная поддерживаемая языком конструкция.

Термин	Расшифровка термина
Нити (Threads)	Еще может переводиться как поток, но в терминологии RT Protect EDR встречается чаще всего как нить. Основная единица, которой операционная система выделяет время процессора. Каждая нить имеет приоритет планирования и набор структур, в которых система сохраняет контекст нити, когда ее выполнение приостановлено. Контекст нити содержит все сведения, позволяющие ей безболезненно возобновить выполнение, в том числе набор регистров процессора и стек нити. В контексте процесса может выполняться несколько нитей. Все нити процесса используют общий диапазон виртуальных адресов. Нить может исполнять любую часть программного кода, включая части, выполняемые в данный момент другой нитью.
Образ	Исполняемый файл, библиотека DLL или драйвер, загруженный Windows в рамках процесса пользовательского режима или ядра.
Поведенческий анализ	Механизм, построенный на технологии принятия решения о предоставлении доступа на основе анализа характера выполняемых объектом или программой действий.
Провайдер ETW	Любой компонент, который использует Event Tracing API. Это могут быть как классические провайдеры, созданные до Windows Vista и применяющие MOF-классы, так и провайдеры на основе манифестов, использующие новые интерфейсы, появившиеся в Windows Vista.
Проксирование	Перенаправление трафика.
Процесс	В простейших терминах – это исполняемая в операционной системе программа, активный объект ОС, а иначе, последовательность инструкций, исполняемых в ОС предопределенным образом. В данном случае такими инструкциями будет программный код. При этом программа будет называться процессом в том случае, если загружается в память вместе со всеми ресурсами, которые необходимы для ее работы.
Псевдокод	Компактный, зачастую неформальный язык описания алгоритмов, использующий ключевые слова императивных языков программирования, но опускающий несущественные для понимания алгоритма подробности и специфический синтаксис. Предназначен для представления алгоритма человеку, а не для компьютерной трансляции и последующего исполнения программы.
Ретроспективный анализ	Детальное исследование образов систем, журналов событий, дампов памяти и сетевого трафика за определенный промежуток времени в прошлом с целью выявить следы компрометации.
Синяя команда	Группа лиц, которая проводит анализ информационных систем для обеспечения безопасности, выявления недостатков безопасности, проверки эффективности каждой меры безопасности и обеспечения того, чтобы все меры безопасности продолжали действовать после реализации.
Телеметрия	Совокупность методов сбора информации и измерения параметров, позволяющих получить необходимые сведения об удаленных объектах.
Утилита mimikatz	Программное обеспечение, которое позволяет извлечь пароли пользователей непосредственно из памяти (путем инъекции в lsass.exe библиотеки sekurlsa.dll), из сохраненного дампа памяти компьютера или даже из файла гибернации (используемый в Windows файл для хранения данных и их последующей быстрой загрузки в оперативную память при включении компьютера или ноутбука).

Термин	Расшифровка термина
Фишинг	Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.
Форензика	Прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. Форензика является подразделом криминалистики.
Хеш-сумма	Уникальный идентификатор, который задаётся (автором программы или первым владельцем файла) с помощью «перемешивания» и шифрования содержимого файла по специальному алгоритму с последующей конвертацией результата в обычную строчку символов.
Хост	Любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети.
Эвристический анализ	Метод обнаружения вредоносных программ, при котором антивирусная программа контролирует все действия, выполняемые проверяемой программой. В ходе эвристического анализа отслеживаются потенциально опасные действия, характерные для вирусов и вредоносных программ других типов.
Эксплойт	Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой, так и нарушение её функционирования.
Эксфильтрация	Несанкционированное копирование, передача или получение данных с компьютера или сервера жертвы. Эксфильтрация может осуществляться через интернет или по локальной сети. Как правило, при передаче данных атакующие сжимают и шифруют их, чтобы избежать обнаружения.
Эмуляция	Комплекс программных, аппаратных средств или их сочетание, предназначенный для копирования (или эмулирования) функций одной вычислительной системы на другую, отличную от первой вычислительной системы, таким образом, чтобы эмулированное поведение как можно ближе соответствовало поведению оригинальной системы.
Advapi32.dll	Часть расширенной библиотеки служб API, поддерживающей множество API, в том числе вызовы безопасности и реестра.
Anti-Ransomware	Программное обеспечение, защищающее конечные точки от вирусов-шифровальщиков.
APT-атака	Целевая кибератака (таргетированная кибератака) – вид кибератаки, процесс которой контролируется вручную в реальном времени человеком, являющимся центром атаки. Целью данной атаки является хищение защищенной информации из информационной системы конкретной компании, организации или государственной службы.
ASCII	Название таблицы (кодировки, набора), в которой некоторым распространённым печатным и непечатным символам сопоставлены числовые коды. Таблица была разработана и стандартизирована в США, в 1963 году.
ATT&CK	База знаний компании MITRE Corporation, содержащая описание тактик, приемов и методов, используемых киберпреступниками.

Термин	Расшифровка термина
Base64	Стандарт кодирования двоичных данных при помощи только 64 символов ASCII.
BCDEdit	Программа командной строки Windows для управления хранилищами BCD (данных конфигурации загрузки)
C&C (C2)	Инфраструктура управления и контроля (C2), используемая злоумышленниками для управления зараженными устройствами и кражи конфиденциальных данных во время кибератаки.
CAR	Репозиторий аналитики информационной безопасности MITRE.
Cmd	Команда для запуска интерпретатора команд.
Cmd.exe	Интерпретатор командной строки для операционных систем OS/2, Windows CE и для семейства операционных систем, базирующихся на Windows NT.
CMSTP	Утилита командной строки Windows, которая позволяет устанавливать профили менеджера соединений.
Cobalt Strike	Программная платформа для сетевых атак, которая сочетает в себе социальную инженерию, инструменты несанкционированного доступа, обфускацию сетевых шаблонов, сложный механизм развертывания вредоносного кода и т.д.
Combase.dll	Библиотека динамической компоновки, являющаяся основой архитектуры COM для MS Windows. Библиотека содержит заголовки и функции для манипулирования объектами COM: «COM – это независимая от платформы, распределенная, объектно-ориентированная система для создания двоичных программных компонентов, которые могут взаимодействовать. COM является базовой технологией для технологий Microsoft OLE (составные документы) и ActiveX (компоненты с поддержкой Интернета)».
Comctl32.dll	Библиотека динамической компоновки, отвечающая за корректное отображение графических элементов при работе в Windows.
D3FEND	Каталог защитных методов кибербезопасности и их отношения к наступательным/противодействующим методам.
Desktop.ini	Файл конфигурации, который содержит данные настроек внешнего вида системной папки в ОС Microsoft Windows: значок, цвет текста, фоновый рисунок и т. д.
DiskShadow	Утилита командной строки Windows, которая предоставляет функциональные возможности службы теневого копирования томов (VSS).
DismHost	Процесс, который используется для обслуживания образа Windows и исправления различных ошибок, связанных с файлами образа Windows. Обычно он находится в C:\Windows\System32\dism или C:\Windows\SysWoW64\dism
DLL	Динамически подключаемая библиотека.
DNS	Служба имён доменов (механизм, используемый в сети Internet и устанавливающий соответствие между числовыми IP-адресами.
DSL	Предметный язык программирования, специализированный для конкретной области применения.

Термин	Расшифровка термина
Dwmapi.dll	Библиотека динамической компоновки, предоставляющая API-интерфейс диспетчера окон рабочего стола Microsoft (общий интерфейс диспетчера окон рабочего стола DWM), который представляет собой обычный файл и в основном используется в качестве API-интерфейса для эффектов рабочего стола (таких, как эффекты Aero).
EDR	Класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, и других устройствах.
ETW	Высокоэффективная масштабируемая система трассировки с минимальными затратами ресурсов, реализуемая в операционных системах Windows.
False positive	Ложноположительные срабатывания – неправильно обозначенные предупреждения системы безопасности, указывающие на наличие угрозы при ее реальном отсутствии. Эти события увеличивают шум для групп безопасности и могут включать ошибки программного обеспечения, плохо написанное программное обеспечение или нераспознанный сетевой трафик.
FsUtil	Утилита командной строки Windows, которая позволяет решать задачи, связанные с таблицей размещения файлов (FAT) и файловой системой NTFS.
FTP	Протокол передачи файлов по сети.
Gdi32.dll	Библиотека динамической компоновки, которая содержит функции для Windows GDI (интерфейс графического устройства). Эти функции помогают создавать простые двумерные объекты.
HEX	Позиционная система счисления по целочисленному основанию 16.
Hh	Утилита Windows, которая позволяет работать с HTML-справками.
HTTP	Протокол прикладного уровня передачи данных, изначально – в виде гипертекстовых документов в формате HTML, в настоящее время используется для передачи произвольных данных.
Icacls	Утилита командной строки Windows, которая позволяет управлять списками доступа (ACL) к каталогам и файлам.
Imm32.dll	Библиотека динамической компоновки, которая используется диспетчером методов ввода Microsoft Windows (IMM). IMM – это технология, используемая приложением для связи с редактором методов ввода (IME), который работает как служба. IME позволяет пользователям компьютеров вводить сложные символы, такие как иероглифы, с помощью стандартной клавиатуры.
Imphash	Хеш импортируемых библиотек, то есть всех импортируемых программой библиотек, прописанных в исполняемом файле Windows Portable Executable (PE).
Inhibit System Recovery	Техника атаки по методологии MITRE, которая предполагает отключение служб, отвечающих за восстановление операционной системы.
InstallUtil	Утилита командной строки Windows, которая позволяет работать с INF-файлами (файлы сведений об установке, то есть определяющие, какие файлы необходимы для установки программного обеспечения или обновления).
IOA	Индикаторы атак.
IOC	Индикаторы компрометации.
JSON	Текстовый формат обмена данными, основанный на JavaScript.

Термин	Расшифровка термина
Kerberos	Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы.
Keylogger	Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя – нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши.
Kernel32.dll	Динамически подключаемая библиотека, являющаяся ядром всех версий ОС Microsoft Windows. Она предоставляет приложениям многие базовые API Win32, такие как управление памятью, операции ввода-вывода, создание процессов и нитей, а также функции синхронизации.
Kernelbase.dll	Системная динамическая библиотека, которая необходима для связи других динамических библиотек Windows. Другими словами, KernelBase.dll позволяет многим программам использовать одни и те же опции. Яркий пример тому обращение разных приложений к тому же самому общему для всех них файлу принтера DLL при необходимости печати. Повреждение KernelBase.dll, а также отсутствие элемента в системе может привести к закрытию программ, при этом проблема сопровождается сообщениями об ошибке.
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux, включающих тот или иной набор утилит и программ проекта GNU.
Loopback	Программный метод, который направляет полученные данные обратно отправителю без специальной обработки или модификации.
Lpk.dll	Динамическая библиотека языковых пакетов. Применяется Windows и многими приложениями для управления языковым пакетом, используемым для диалогов и сообщений.
Lsass.exe	Служба проверки подлинности локальной системы безопасности. Процесс lsass проверяет данные для авторизации пользователей.
MD5	128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности.
MITRE (The MITRE Corporation)	Американская некоммерческая организация с двумя штаб-квартирами в Бедфорде, штат Массачусетс, и Маклине, штат Вирджиния. Сотрудники компании занимаются исследованиями и разработками в области обороны, здравоохранения, авиации, внутренней безопасности и кибербезопасности.
ML	Класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение за счёт применения решений множества сходных задач.
Mmc	Утилита, которая позволяет администрировать консоль управления Windows.
Msctf.dll	Библиотека динамической компоновки, которая позволяет сделать доступным TSF (Text Services Framework) для использования независимым вендором в приложениях третьих лиц. TSF – это среда COM и API в Windows XP и более поздних операционных системах Windows, которые поддерживают расширенный ввод и обработку текста.

Термин	Расшифровка термина
Msimg32.dll	Компонент расширения для Windows GDI, который содержит новые API для улучшения функциональности GDI32. Интерфейс графического устройства Microsoft Windows (GDI) позволяет приложениям использовать графический и отформатированный текст как на видео, так и на принтере. приложения на основе Windows напрямую не обращаются к графическому оборудованию. Вместо этого GDI взаимодействует с драйверами устройств от имени приложений.
Network containment	Сетевое сдерживание.
Ntdll.dll	Специальная библиотека системной поддержки, необходимая при использовании DLL подсистем. Она содержит функции двух типов: — интерфейсы диспетчера системных сервисов (system service dispatch stubs) к сервисам исполнительной системы Windows; — внутренние функции поддержки, используемые подсистемами DLL и другими компонентами ОС.
NTFS	Стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft. NTFS поддерживает хранение метаданных.
Odbcconf	Утилита командной строки Windows, которая позволяет настраивать драйверы ODBC (интерфейс доступа к базам данных) и имена источников данных.
Ole32.dll	Библиотека динамической компоновки, содержащая основные функции OLE (технологии связывания и внедрения объектов в другие документы и объекты).
Oleaut32.dll	Библиотека динамической компоновки, идентичная ole32.dll.
PE	Формат исполняемых файлов, объектного кода и динамических библиотек, используемый в 32-х и 64-разрядных версиях операционной системы Microsoft Windows.
Powershell	Расширяемое средство автоматизации от Microsoft с открытым исходным кодом, состоящее из оболочки с интерфейсом командной строки и сопутствующего языка сценариев.
Prefetcher	Компонент операционной системы Microsoft Windows, ускоряющий процесс её начальной загрузки, а также сокращающий время запуска программ.
PsExec	Утилита командной строки Windows. Инструмент от Microsoft, который позволяет удалённо запускать процессы с использованием учётных данных любого пользователя. Функционал программы схож с программой удалённого доступа, но вместо того, чтобы управлять удаленным компьютером с помощью мыши, команды отправляются на компьютер через командную строку.
RAT	Троян удаленного доступа – утилита для несанкционированного доступа к системе удаленного пользователя с корыстными целями.
RegAsm	Утилита командной строки Windows, которая позволяет регистрировать .NET-сборки.
Regsvr32	Утилита командной строки Windows, которая позволяет регистрировать или отменять регистрацию элементов управления OLE (технология связывания и внедрения объектов в другие объекты и документы)
RPC	Класс технологий, позволяющих программам вызывать функции или процедуры в другом адресном пространстве. Обычно реализация RPC-технологии включает два компонента: сетевой протокол для обмена в режиме клиент-сервер и язык сериализации объектов.

Термин	Расшифровка термина
Rpcrt4.dll	Библиотека динамической компоновки, которая предоставляет API удаленного вызова процедур (RPC), используемый приложениями Windows для связи по сети и через Интернет.
Rundll32	Хост-процесс Windows. Компонент операционных систем семейства Microsoft Windows, запускающий программы, находящиеся в динамически подключаемых библиотеках.
Screenshot	Изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора или другого визуального устройства вывода.
Setupapi.dll	Библиотека динамической компоновки, которая предоставляет два набора функций: — общие функции установки; — функции установки устройств. Программное обеспечение для установки устройств может использовать эти функции для выполнения настраиваемых операций в установщиках классов, соустановщиках и приложениях установки устройств.
SHA-1	Алгоритм криптографического хеширования. Описан в RFC 3174. Для входного сообщения произвольной длины алгоритм генерирует 160-битное хеш-значение, называемое также дайджестом сообщения, которое обычно отображается как шестнадцатеричное число длиной в 40 цифр.
SHA-256	Алгоритм хеширования. Криптографическая хеш-функция, разработанная Агентством национальной безопасности США.
Shell32.dll	Библиотека динамической компоновки, которая отвечает за отображение иконок в различных диалоговых окнах операционной системы Windows.
Shlwapi.dll	Библиотека динамической компоновки, которая содержит функции для путей UNC и URL, записей реестра и настроек цвета.
Sigma	Унифицированный формат описания правил детектирования событий.
SOC	Центр обеспечения безопасности.
SSDeep	Программа для расчета нечетких хешей.
SSL	Криптографический протокол, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
Svchost.exe	Хост процесс Windows, главный процесс для служб, загружаемых из динамических библиотек.
Task Sheduler	Компонент Microsoft Windows, который предоставляет возможность запланировать запуск программ или скриптов в определённые моменты времени или через заданные временные интервалы.
TCB	Применительно к EDR – флаг, который указывает, что исполняемый файл, который отмечен этим флагом, является максимально доверенным для ОС.
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.

Термин	Расшифровка термина
Threat Hunting	Охота на киберугрозы – это активная деятельность по киберзащите. Процесс упреждающего и итеративного поиска в сетях для обнаружения и изоляции сложных угроз, которые обходят существующие решения безопасности.
TLSH	Библиотека для матчинга нечетких хешей, разработанная компанией Trend Micro.
Trustlets	Программы, запускаемые как IUM-процессы (Isolated User Mode) в VSM (Virtual Secure Mode)
TTP	Тактики, техники и процедуры, используемые злоумышленниками для осуществления атак
User32.dll	Библиотека динамической компоновки, содержащая функции Windows API, связанные с пользовательским интерфейсом Windows (обработка окон, основные функции пользовательского интерфейса и т. д.)
Userenv.dll	Библиотека динамической компоновки, которая содержит функции интерфейса прикладного программирования (API) для создания профилей пользователей и управления ими.
Usp10.dll	Библиотека динамической компоновки, которая содержит набор функций интерфейса прикладного программирования (API), позволяющие клиенту макета текста форматировать сложные сценарии.
UTC	Стандарт, по которому общество регулирует часы и время. Отличается на целое количество секунд от атомного времени и на дробное количество секунд от всемирного времени UT1.
UUID	Стандарт идентификации, используемый в создании программного обеспечения, основное назначение которого – позволить распределённым системам уникально идентифицировать информацию без центра координации.
Uxtheme.dll	Библиотека динамической компоновки, отвечающая за изменение графических тем системы.
Verclsid	Утилита Windows, которая позволяет верифицировать в ОС COM-объекты. Может использоваться злоумышленниками для скрытного выполнения вредоносного кода.
Version.dll	Библиотека динамической компоновки, содержащая функции интерфейса прикладного программирования (API), используемые приложениями для проверки версии Windows.
Virus Total	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ. Кроме бесплатной существует корпоративная платная версия.
Vssadmin	Утилита Windows, которая позволяет администрировать в командной строке службы теневого копирования (резервирования) томов.
Wbadmin	Утилита Windows, которая позволяет в командной строке выполнять резервное копирование и восстановление операционной системы, томов, файлов и приложений.
Whoami	Утилита Windows, позволяющая получить информацию о пользователе, вошедшем в локальную систему, а также его группе и привилегиях.
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса.

Термин	Расшифровка термина
Winmm.dll	Библиотека динамической компоновки для Windows Multimedia API, который содержит низкоуровневый звук и функции джойстика.
Winspool.drv	DLL-библиотека, содержащая API-методы, которые используется GDI (интерфейс графических устройств) и приложениями для взаимодействия с сервисом печати.
WMI	Инструментарий управления Windows. Одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.
Wmic	Утилита, которая предоставляет интерфейс командной строки для инструментария управления Windows (WMI).
WmiPrvSE	Системный процесс Windows, который позволяет программам, установленным на компьютере, получать различную информацию об ОС.
Ws2_32.dll	Библиотека динамической компоновки, содержащая API-интерфейс Windows Sockets, используемый большинством интернет-приложений и сетевых приложений для обработки сетевых подключений.
YARA	Инструмент для матчинга текстовой информации, направлен на помощь исследователям вредоносных программ в выявлении и классификации образцов вредоносных программ.