Содержание

Обнаружение SSH брутфорс атак с использованием триггеров в QoE

Триггеры используются для поиска данных в QoE Stor по заданным параметрам. После срабатывания триггера возможно одно из действий:

- уведомление в GUI
- HTTP действие
- отправка email

Необходимые опции CKAT DPI:

- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

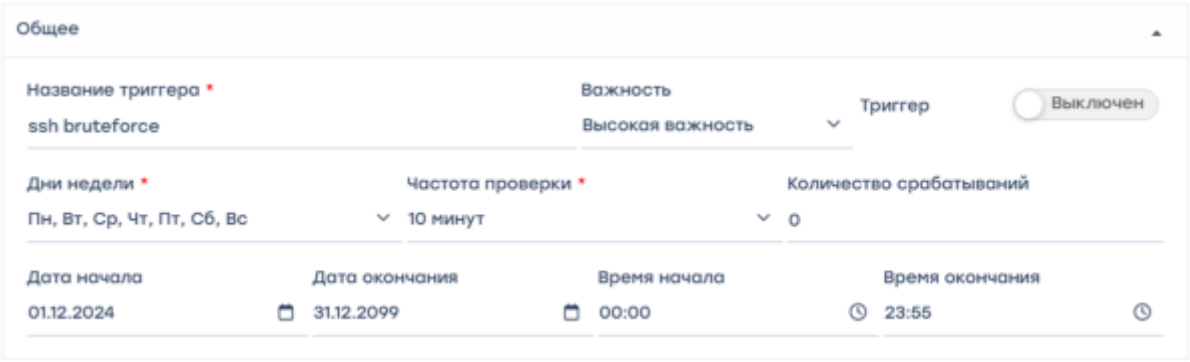
Необходимые дополнительные модули:

- DPIUI2 (GUI - Графический интерфейс управления)
- Внедрение и администрирование

Системный триггер на обнаружение SSH брутфорс атак

Триггер на обнаружение SSH брутфорс атак (Имя - "ssh bruteforce") является системным и доступен в разделе QoE Аналитика → Триггеры и нотификации (по умолчанию выключен).

Общая информация триггера

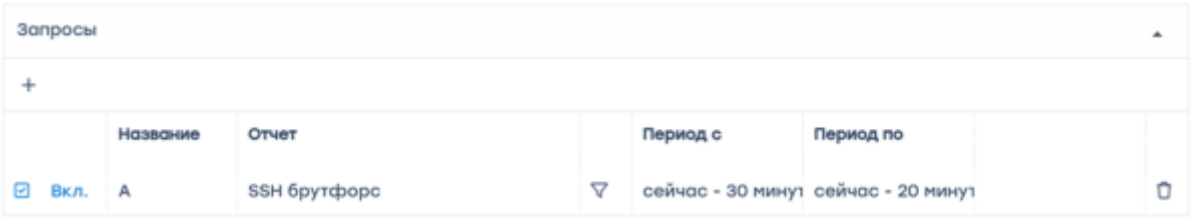


- Название триггера "ssh bruteforce";
- Дни недели - все;
- Частота проверки - 10 минут;
- Частота срабатывания триггера - 0;
- Даты и время начала/окончания работы настраиваются при необходимости.

Каждый день периодичностью в 10 минут будет происходить проверка по

условиям описанным ниже.

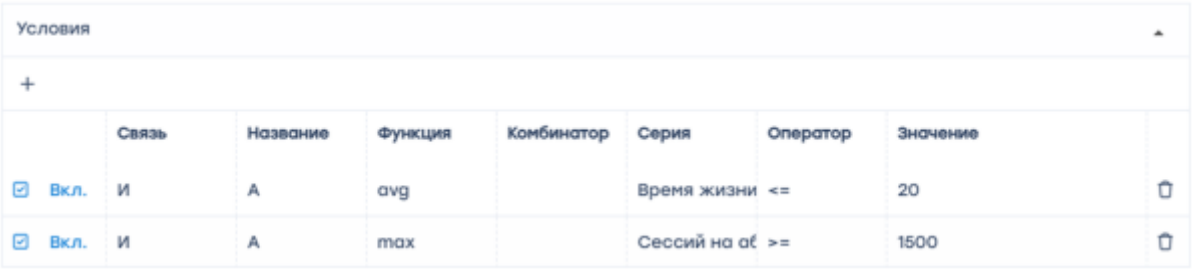
Запросы



Для данного тригера установлен не редактируемый запрос со следующими параметрами:

- Таблица для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → SSH брутфорс;
- Период с: сейчас - 30 минут
- Период по: сейчас - 20 минут

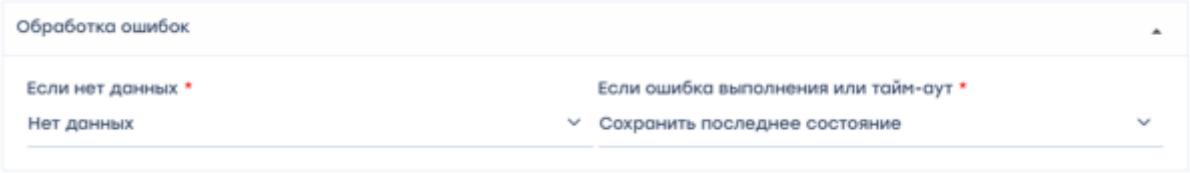
Условия



- Добавить "+" 2 поля
- Связка – И
- Функция – avg для 1 поля, max для 2 поля
- Серия в 1 поле – Время жизни сессии к абоненту, мс <= 20
- Серия во 2 поле – Сессий на абонента >= 1500

Мы задали условия для срабатывания триггера: Средняя продолжительность SSH-сессии к абоненту меньше 20мс и количество SSH-сессий для абонента больше 1500 за обрабатываемый период времени.

Обработка ошибок

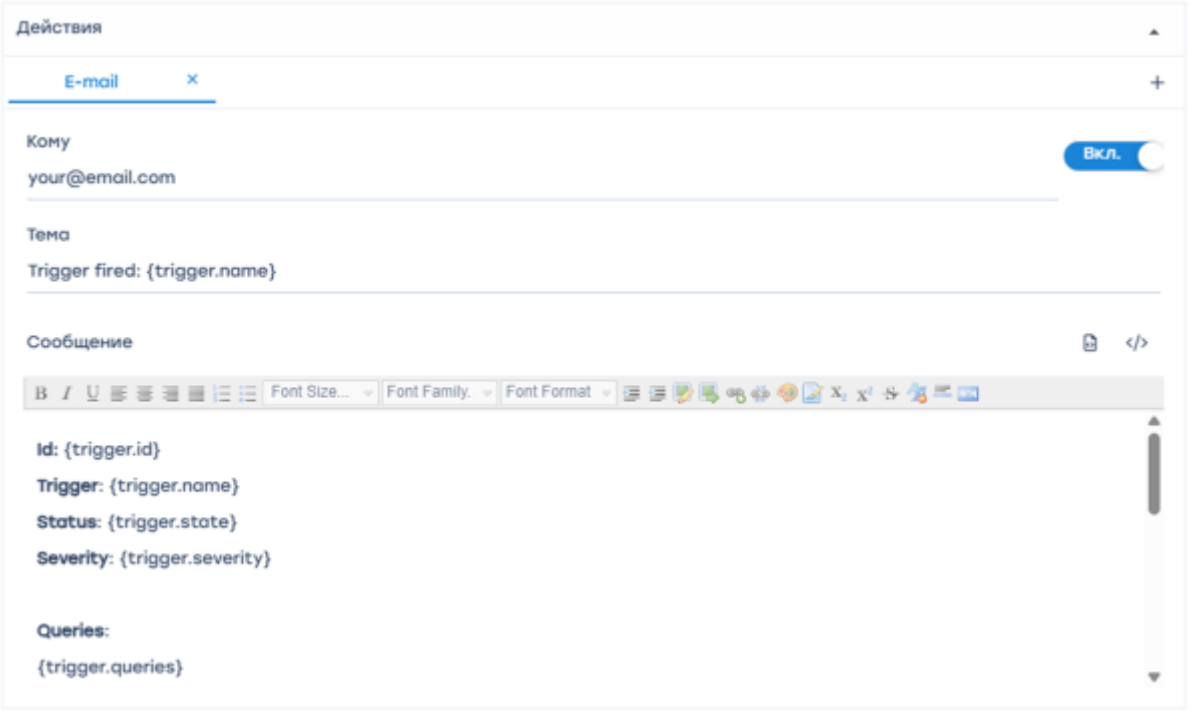


- В поле "Если нет данных" — Нет данных
- В поле "Если ошибка выполнения или тайм-аут" — Сохранить последнее состояние

В данной конфигурации при отсутсвии ошибок данные не будут сохранены, в случае, если ошибки есть - сохранится информация о подозрительной активности.

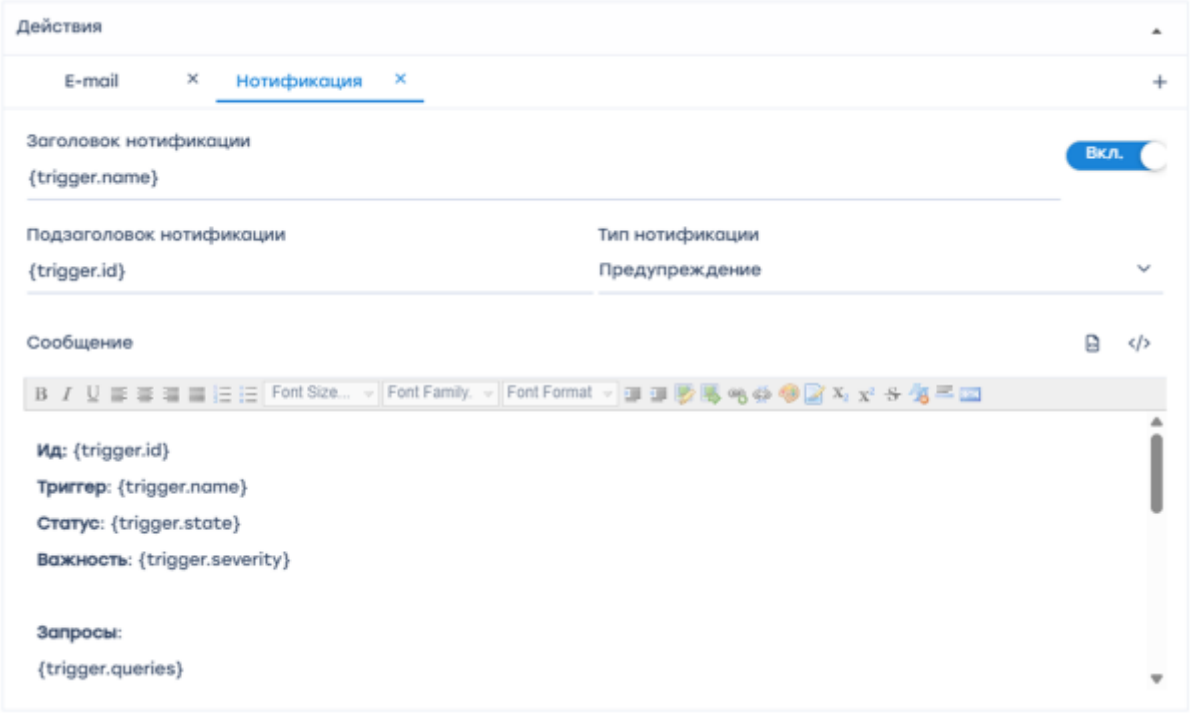
Действия

E-mail действие

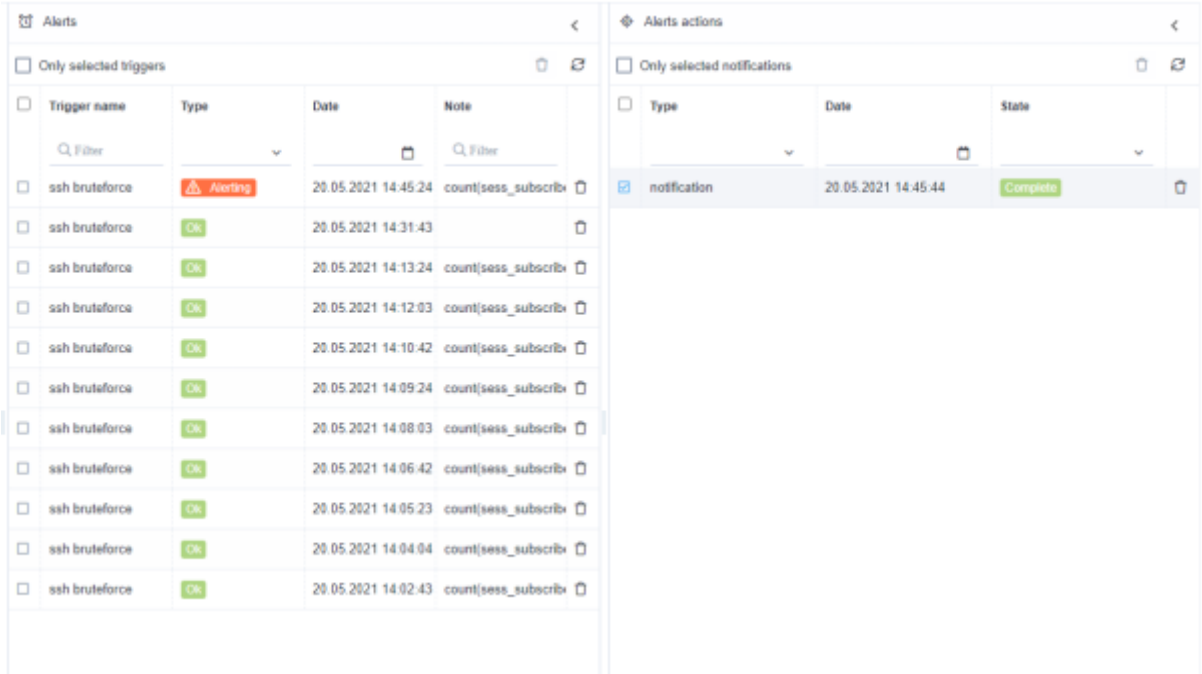


- Для автоматического заполнения — кликнуть по иконке  (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты
- При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние)

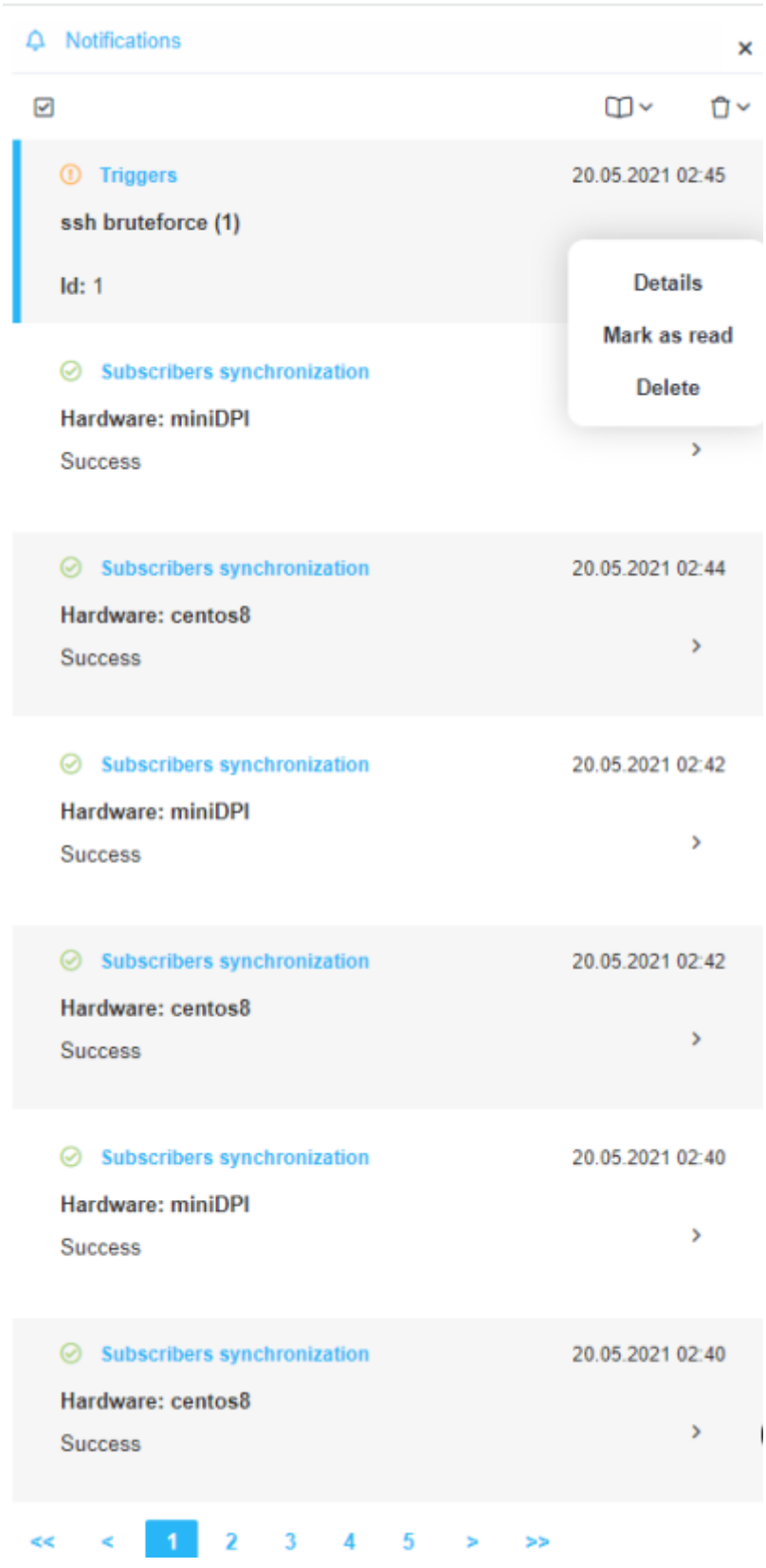
Нотификация



- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ



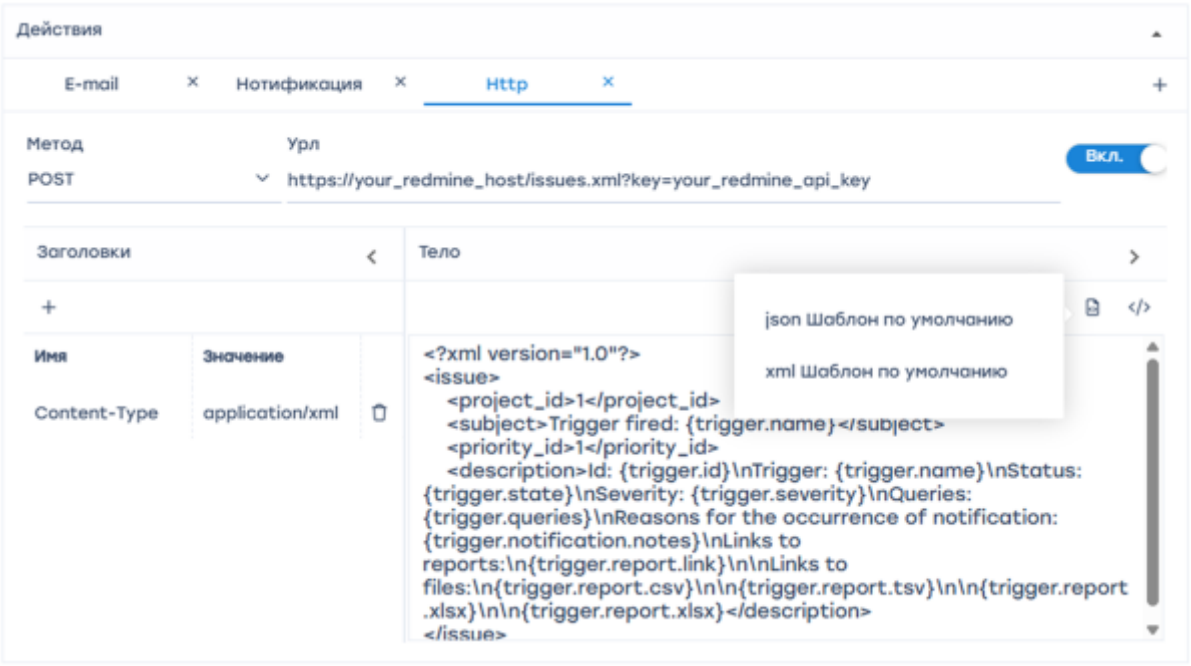
Получить ссылку на отчет можно через меню нотификаций



Выбрать нотификацию Выбрать — "Детали"

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

HTTP действие



Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес