# Содержание

Обнаружение SSH брутфорс атак с использованием триггеров в	3 QoE	3
Системный триггер на обнаружение SSH брутфорс атак		3

# 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
- НТТР 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: Raw full netflow → Tables → Attacks detection → Ssh bruteforce;
- Период с: now 30 minutes
- Период по: now 20 minutes

#### **Условия**



- Добавить "+" 2 поля
- Связка И
- Функция avg
- Серия в 1 поле время жизни сессии к абоненту <= 20(мс)
- Серия во 2 поле количество 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 ошибок" нет данных
- В поле "Если есть ошибка или таймаут" 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.

# НТТР действие

×

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