Содержание

Поиск DDoS атак, BotNet и перехода на конкретный ресурс 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:

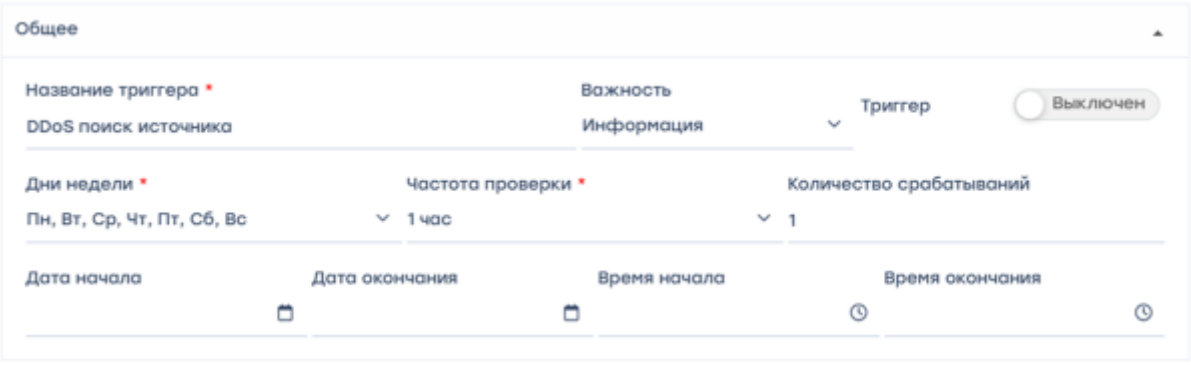
- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

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

Пример настройки триггера на поиск источника DDOS-атаки типа Flood

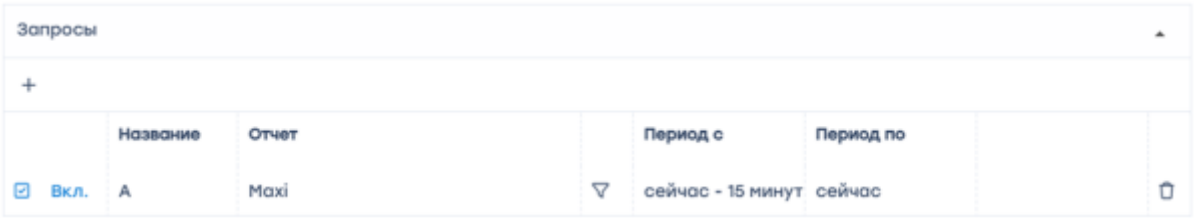
Общая информация триггера



Название триггера «DDoS поиск источника», дни недели – все, частота проверки – 1 час, частота срабатываний триггера – 1 раз, даты и время начала/окончания не установлены.

Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

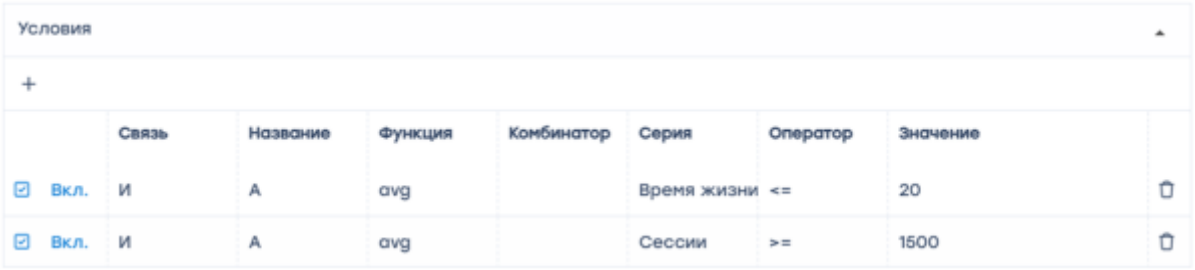
Запросы



- Добавить поле
- Название A
- Выбрать таблицу для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 15 минут», период по: «сейчас»

В этом случае будет происходит анализ трафика по выбранной странице в период — последние 15 минут.

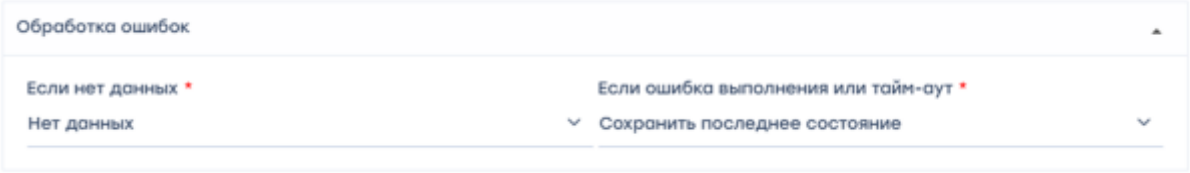
Условия



- Добавить "+" 2 поля
- Связка – И
- Функция – avg
- Серия в 1 поле – Время жизни сессии, мс <= 20
- Серия во 2 поле – Сессии >= 1500

Мы задали условие — для срабатывания триггера необходимо, чтобы были детектированы: И сессии с жизнью меньше или равно 20мс, И с одного IP-хоста было более 1500 сессий.

Обработка ошибок

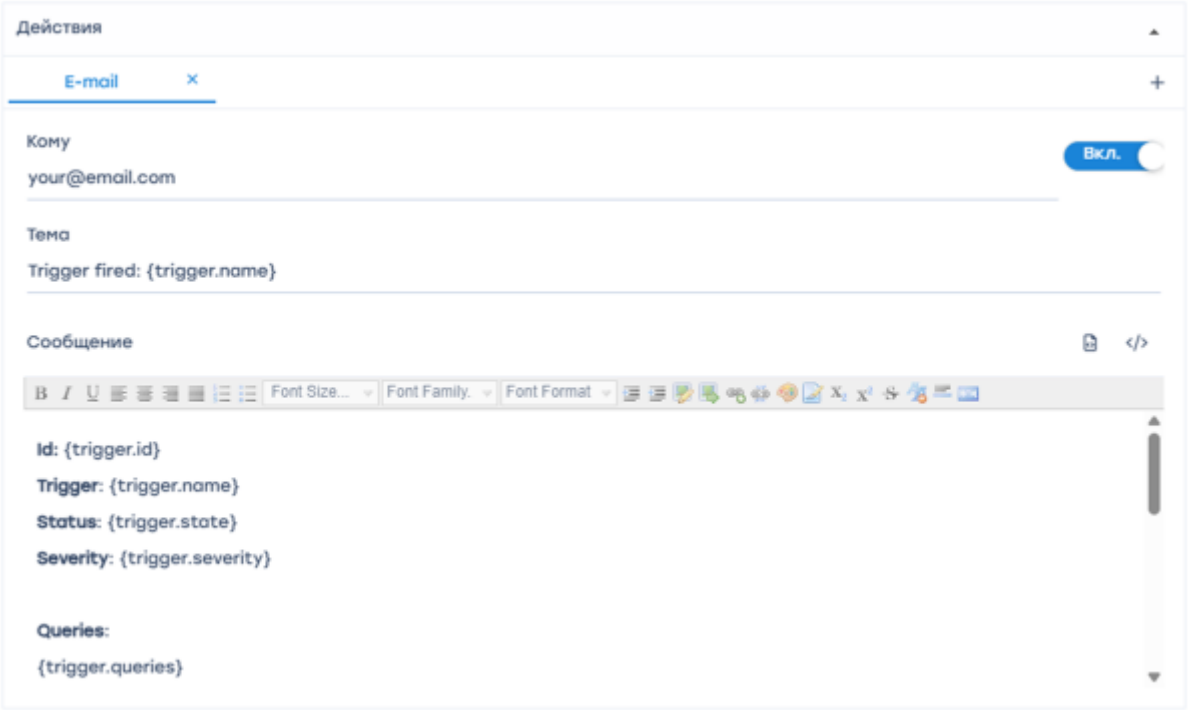


- В поле "Если нет данных" — нет данных
- В поле "Если есть ошибка или тайм-аут" — сохранить последнее состояние

в этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

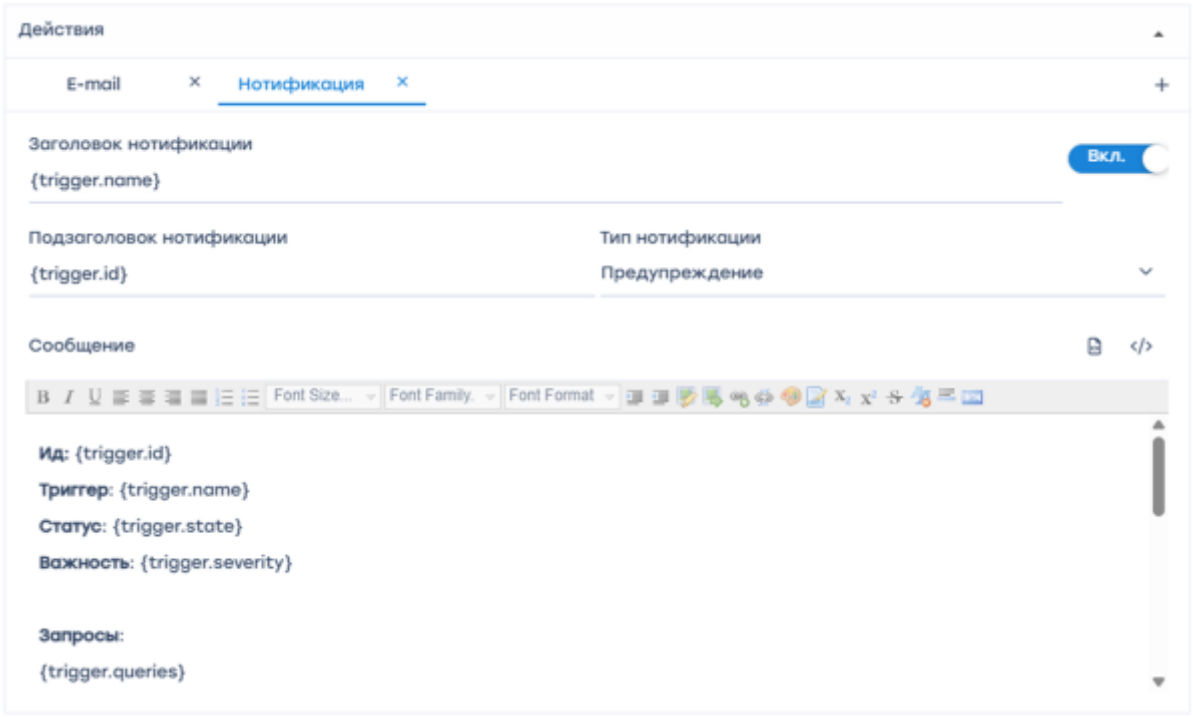
Действия

E-mail действие

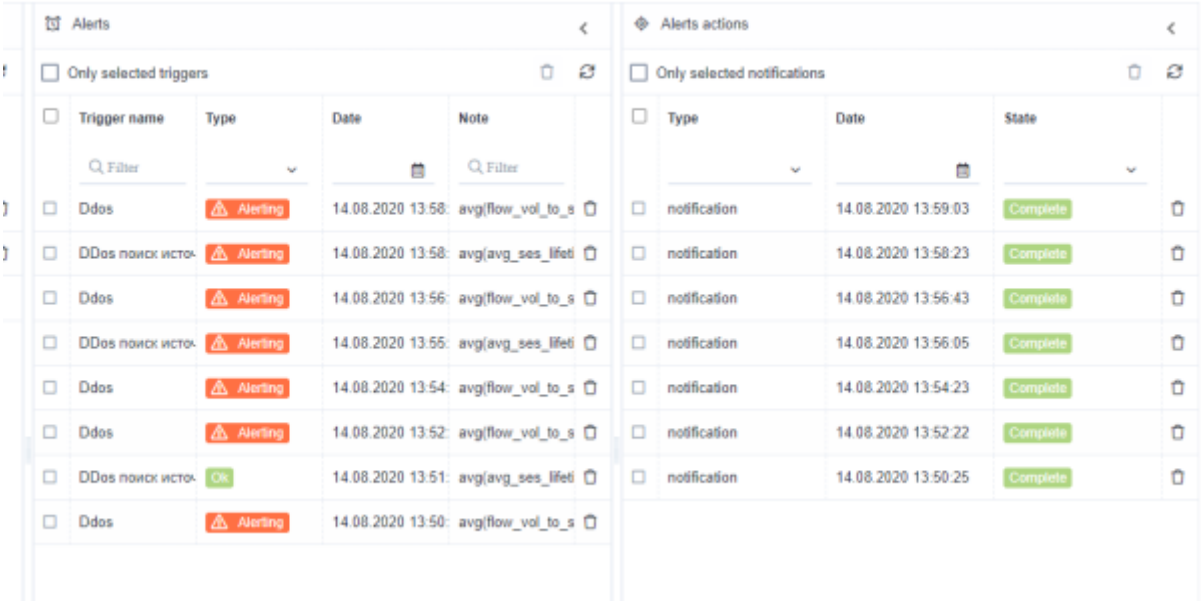


- Для автоматического заполнения — кликнуть по иконке  (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты
- При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус,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

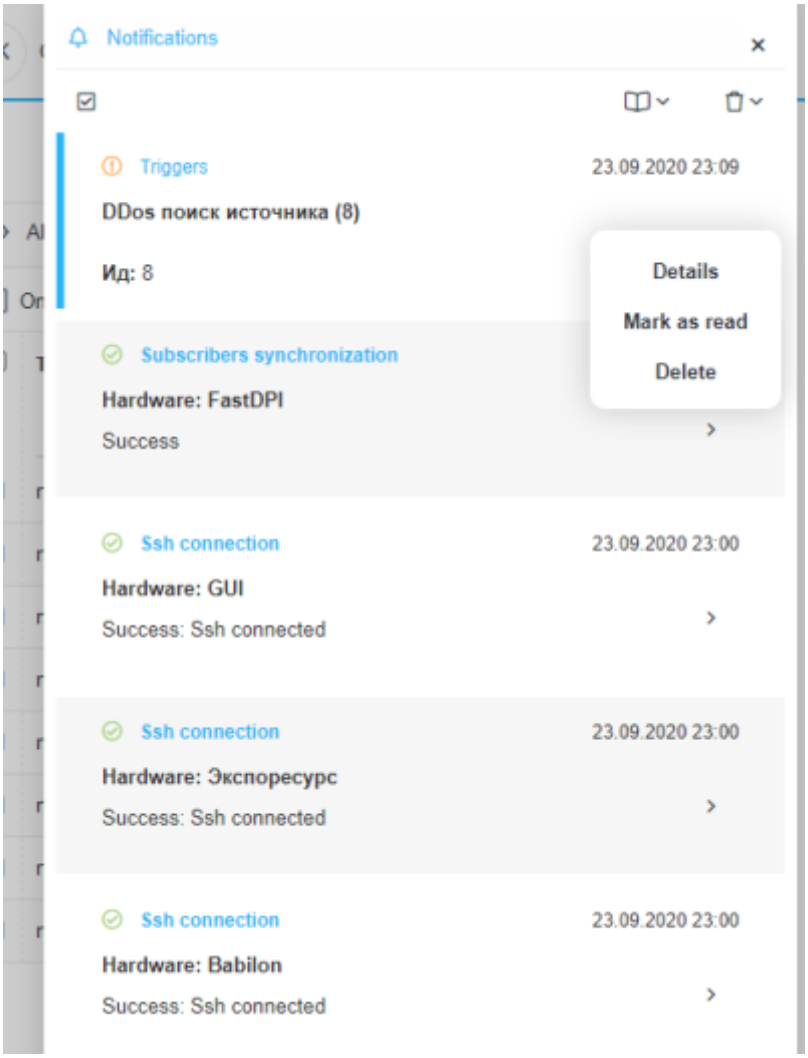
Нотификация



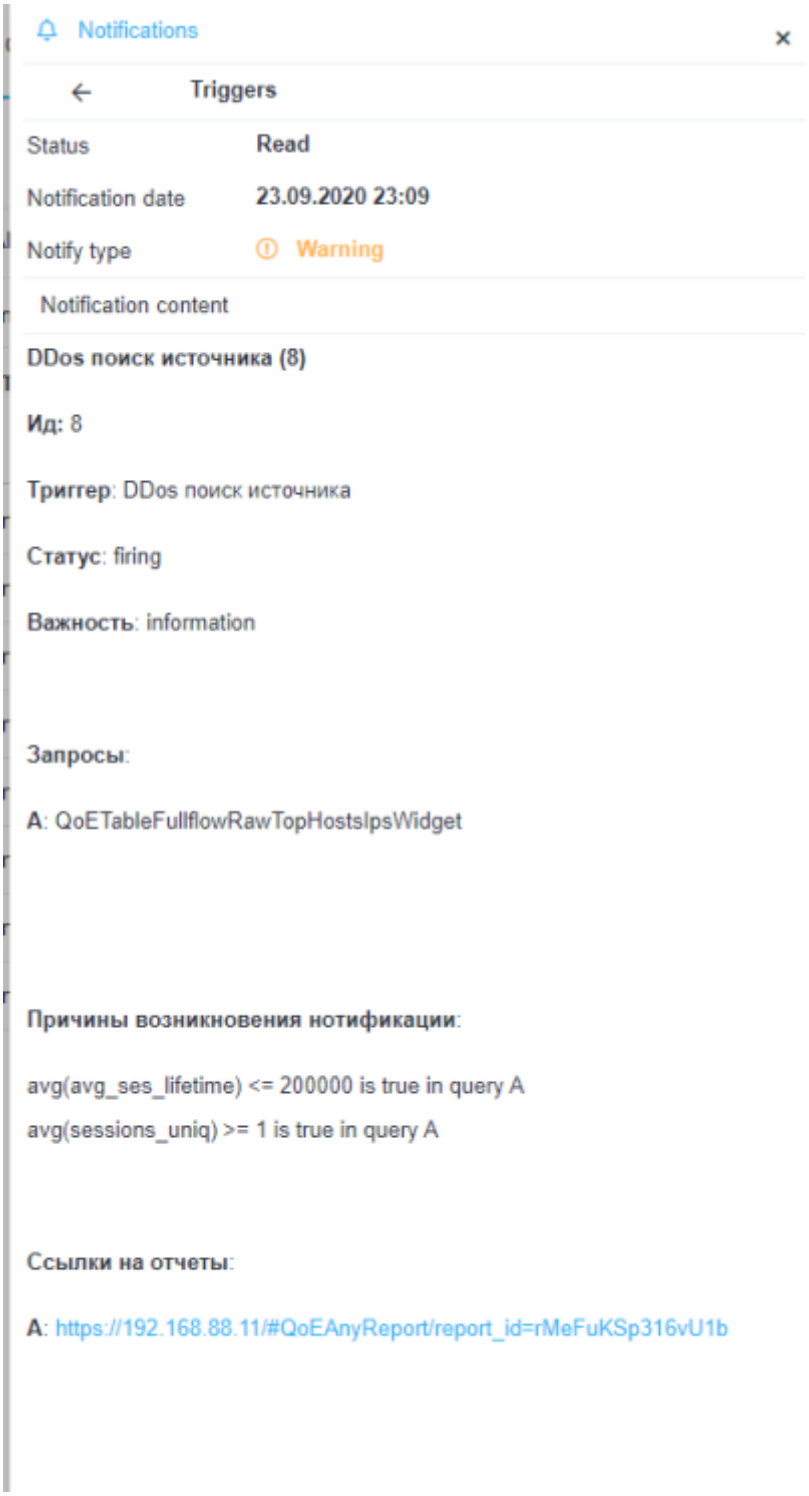
- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ



Получить ссылку на отчет можно через меню нотификаций

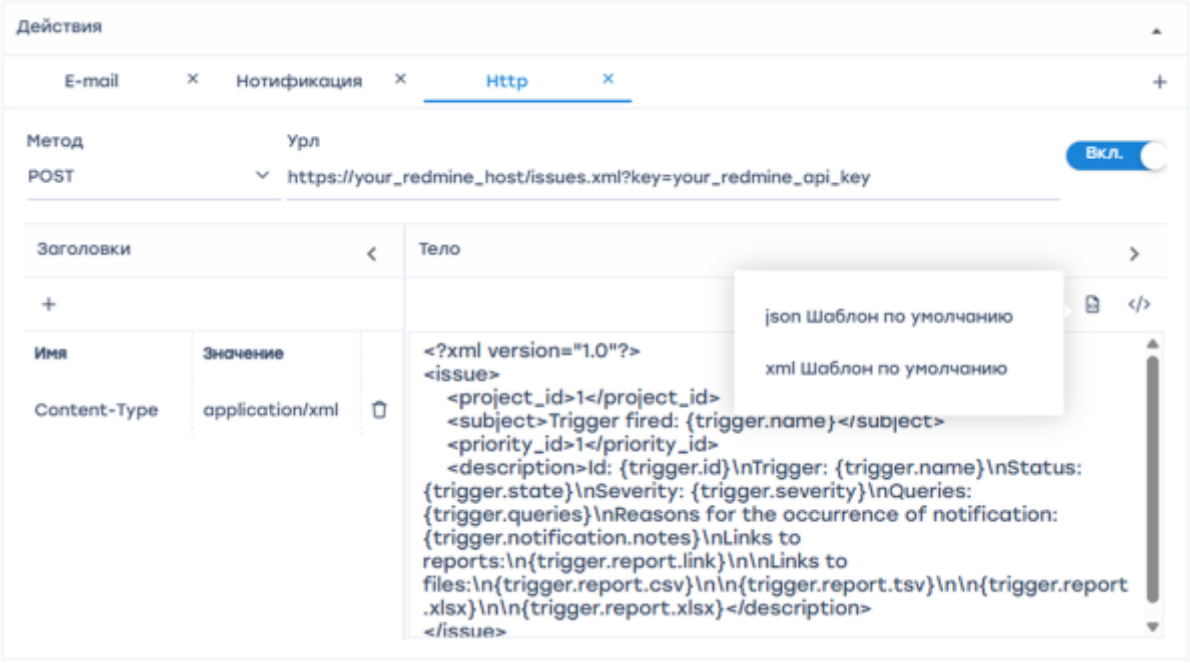


Выбрать нотификацию Выбрать — "Детали"



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

HTTP действие



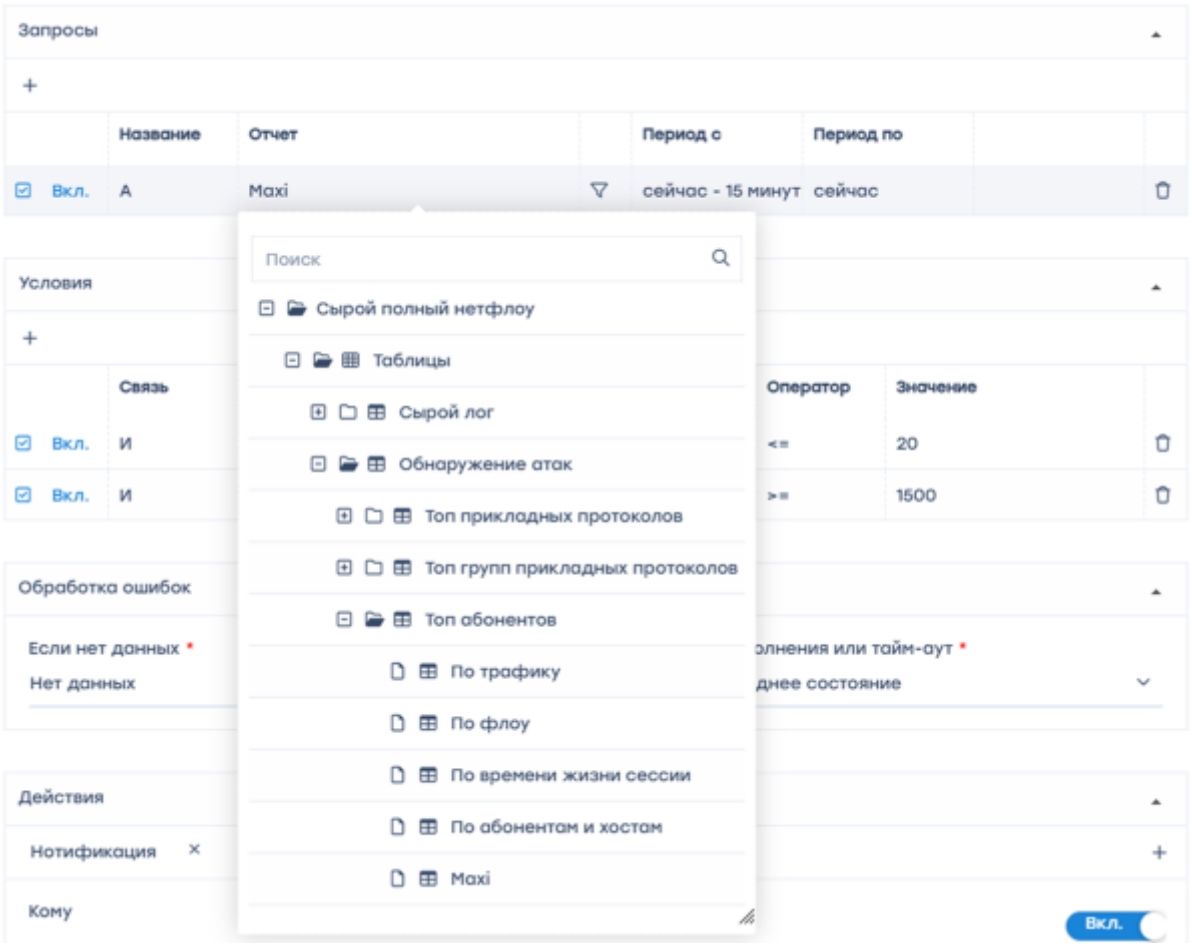
Для автоматического заполнения — кликнуть (автоматическое заполнение формы)
Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес

Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Пример настройки триггера на поиск цели DDOS-атаки типа Flood

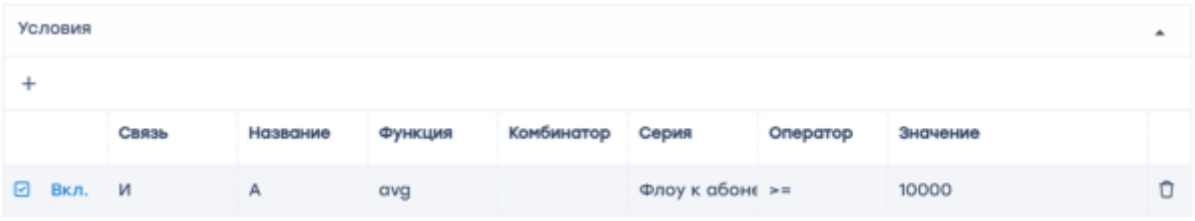
От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

Запросы



в поле отчет выбрать Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ абонентов → Maxi

Условия



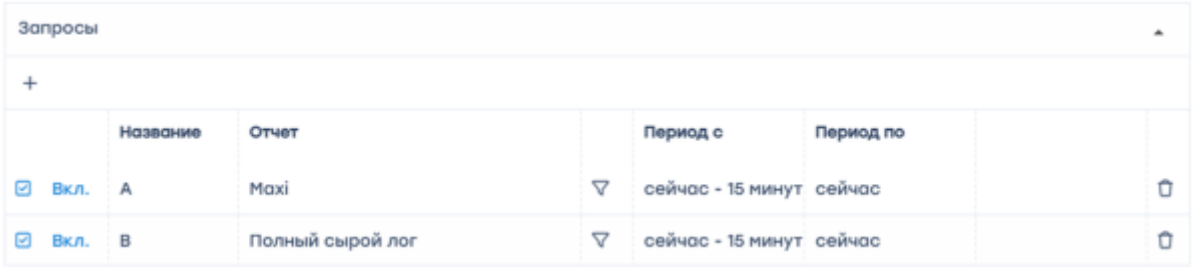
Серия — "Объем Flow к абонентам, Пак", >= 10000

Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Анализ BotNet

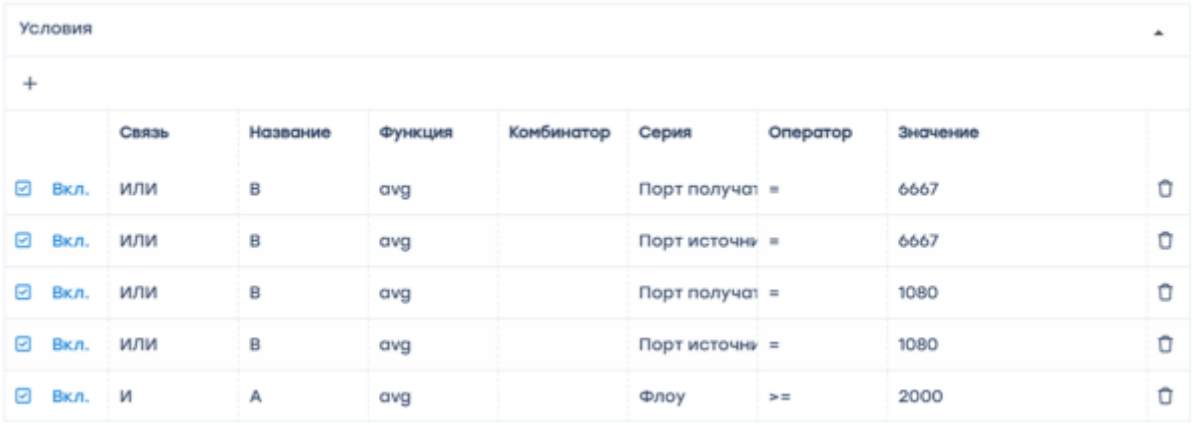
От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

Запросы



- Выбрать Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ прикладных протоколов → Maxi для значения "A"
- Сырой полный нетфлоу → Сырой лог → Полный сырой лог для значения "B"

Условия



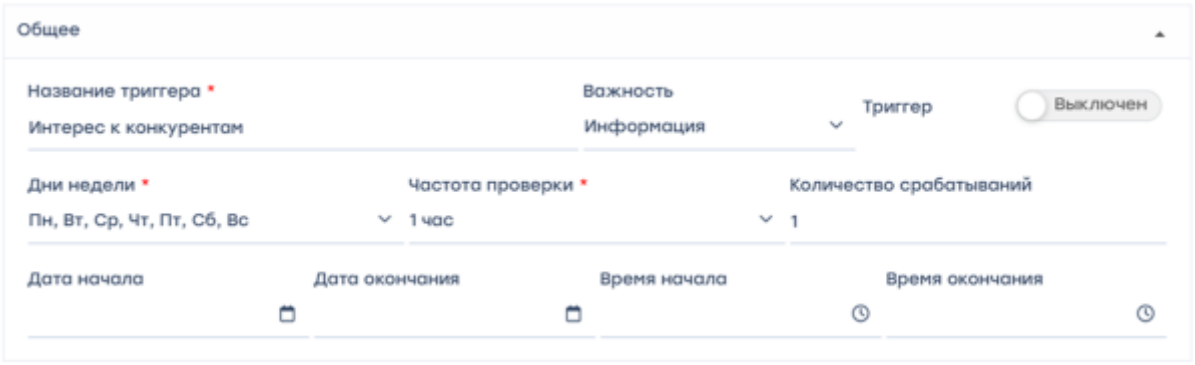
Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "B" со значением "ИЛИ", и Флоу больше или равно 2000.

При этой конфигурации в случае если: хоть на одном из портов (6667/1080) количество проходящих пакетов будет более 2000 в секунду — сработает триггер.

Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Фиксация перехода абонента на ресурс конкурента

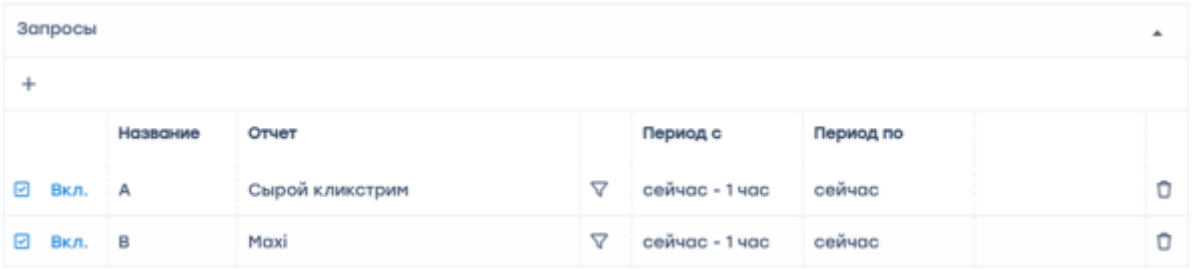
Общая информация триггера



Название триггера «Интерес к конкурентам», дни недели – все, частота проверки – 1 час, частота срабатываний триггера – 1 раз, даты и время начала/окончания не установлены.

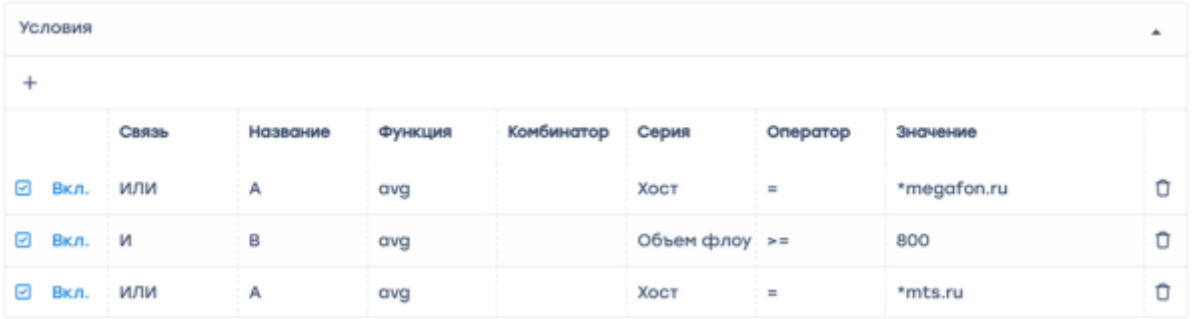
Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

Запросы



- Добавить "+" поле
- Название A
  Выбрать таблицу для сканирования: Сырой кликстрим → Таблицы → Сырой кликстрим
- Название B
  Выбрать таблицу для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 1 час», период по : «сейчас»
- В этом случае будет происходит анализ трафика каждый час по выбранным таблицам.

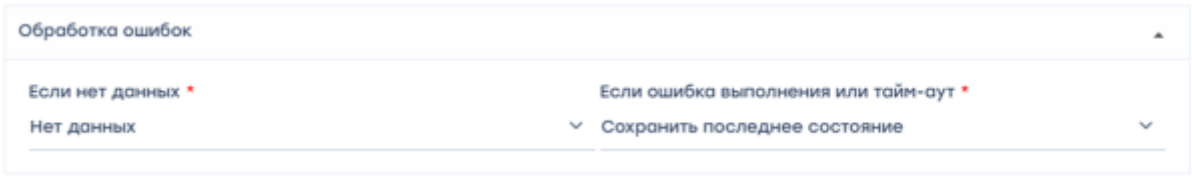
Условия



- Добавить "+" 3 поля
- Первое поле — выбрать таблицу "A"; Связка – "Или"; Функция – "avg"; Серия Хост = *megafon.ru (или ваш любимый конкурент)
- Второе поле — выбрать таблицу "B"; связка "И"; Функция – "avg"; Серия Объем флоу от абонентов >= 800
- Третье поле — выбрать таблицу "A"; Связка – "Или"; Функция – "avg"; Серия Хост = *mts.ru

Мы задали условие — для срабатывания триггера необходимо, чтобы было детектировано: не менее 800 пакетов (не случайный а осмысленный переход) от абонента к сайту конкурента.

Обработка ошибок

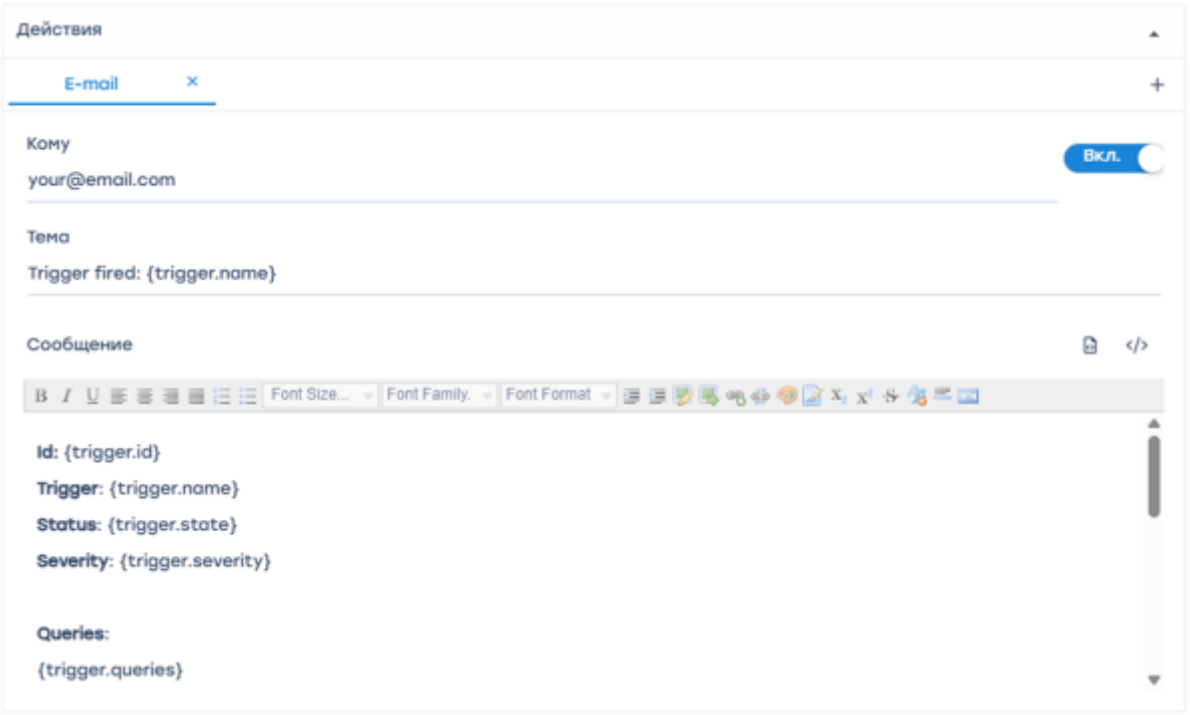


- В поле "Если нет данных" — Нет данных
- В поле "Если ошибка выполнения или тайм-аут" — Сохранить последнее состояние.

В этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

Действия

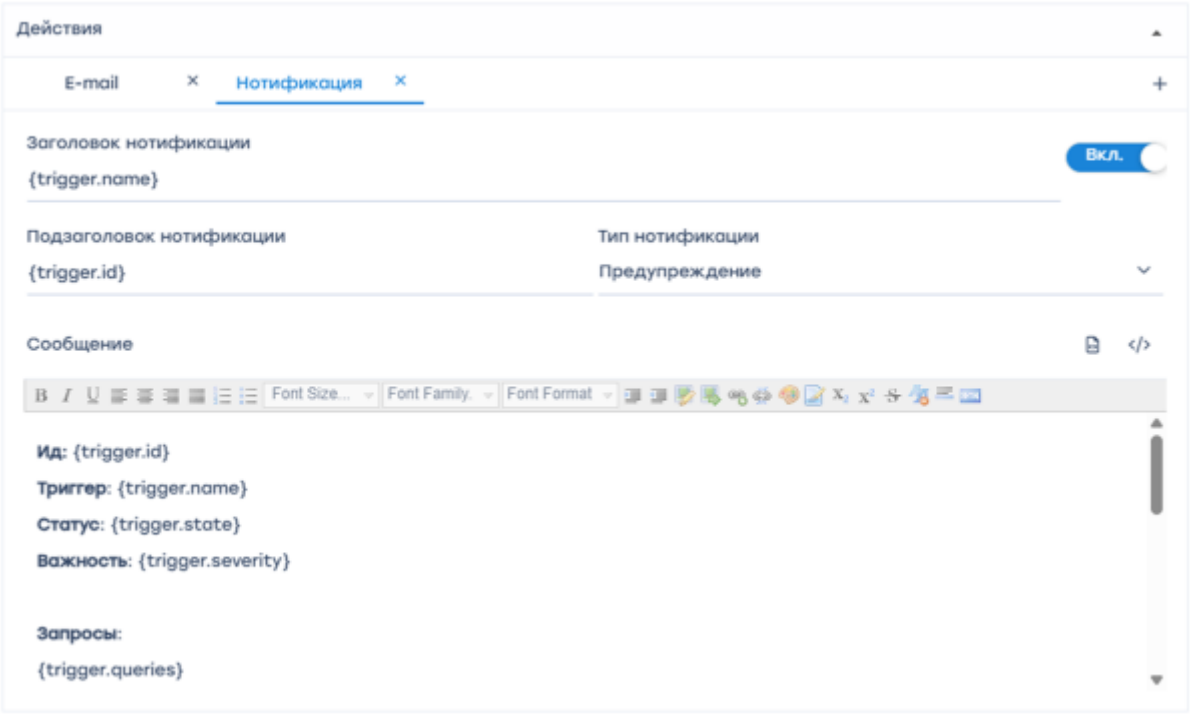
E-mail действие



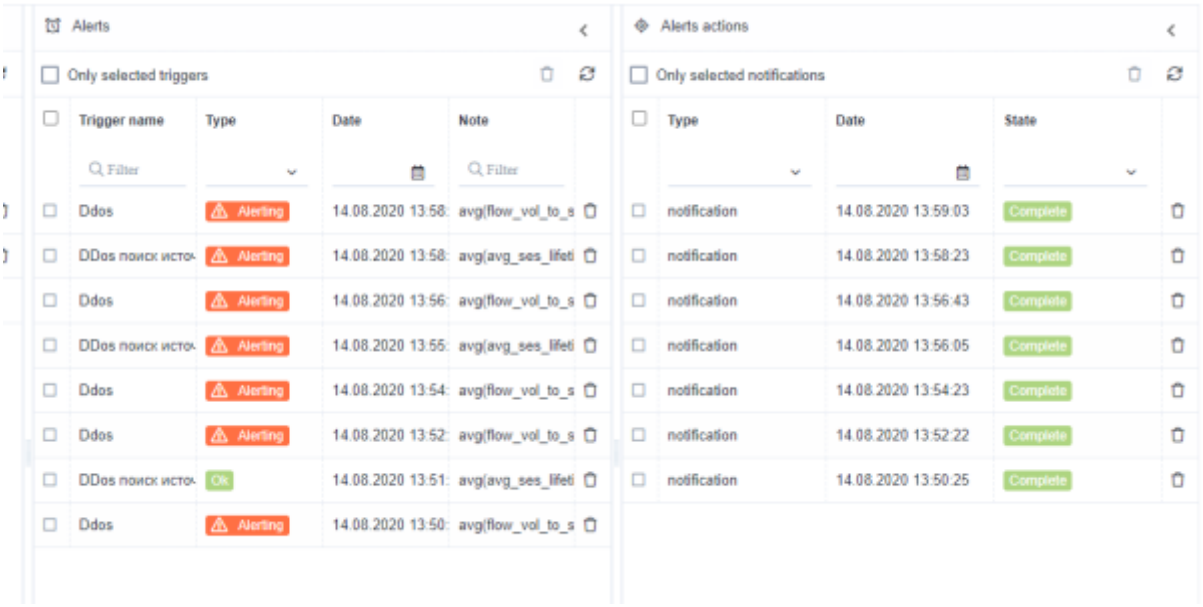
- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты

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).

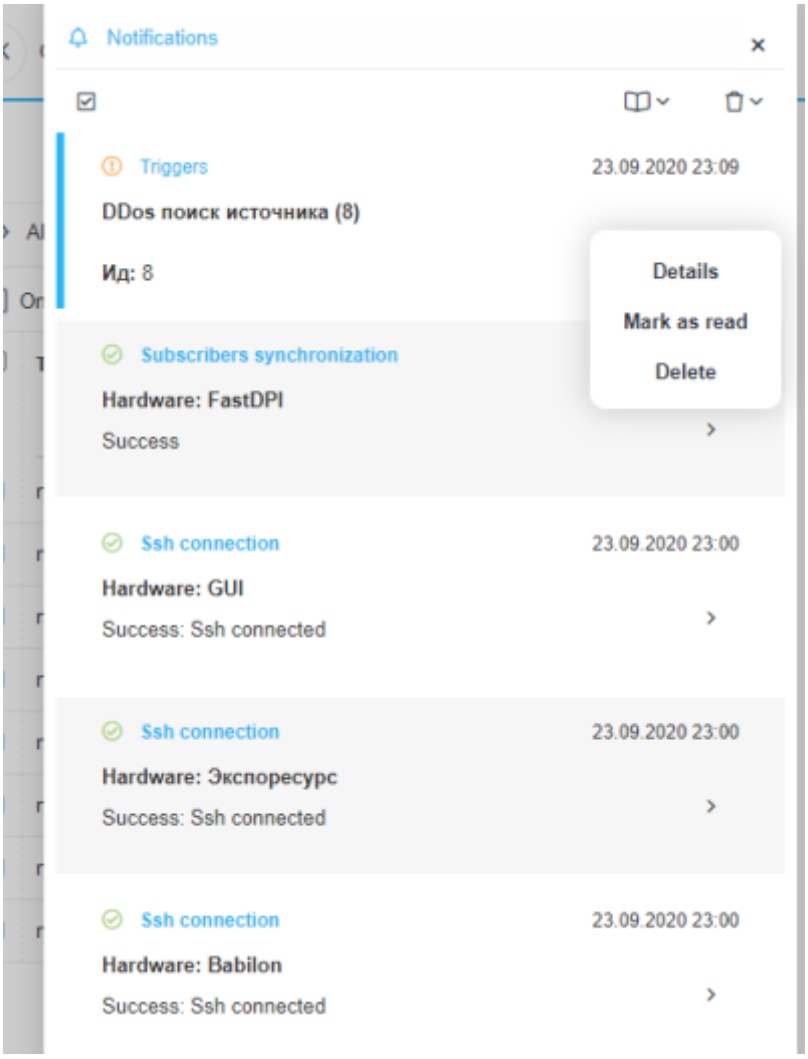
Нотификация



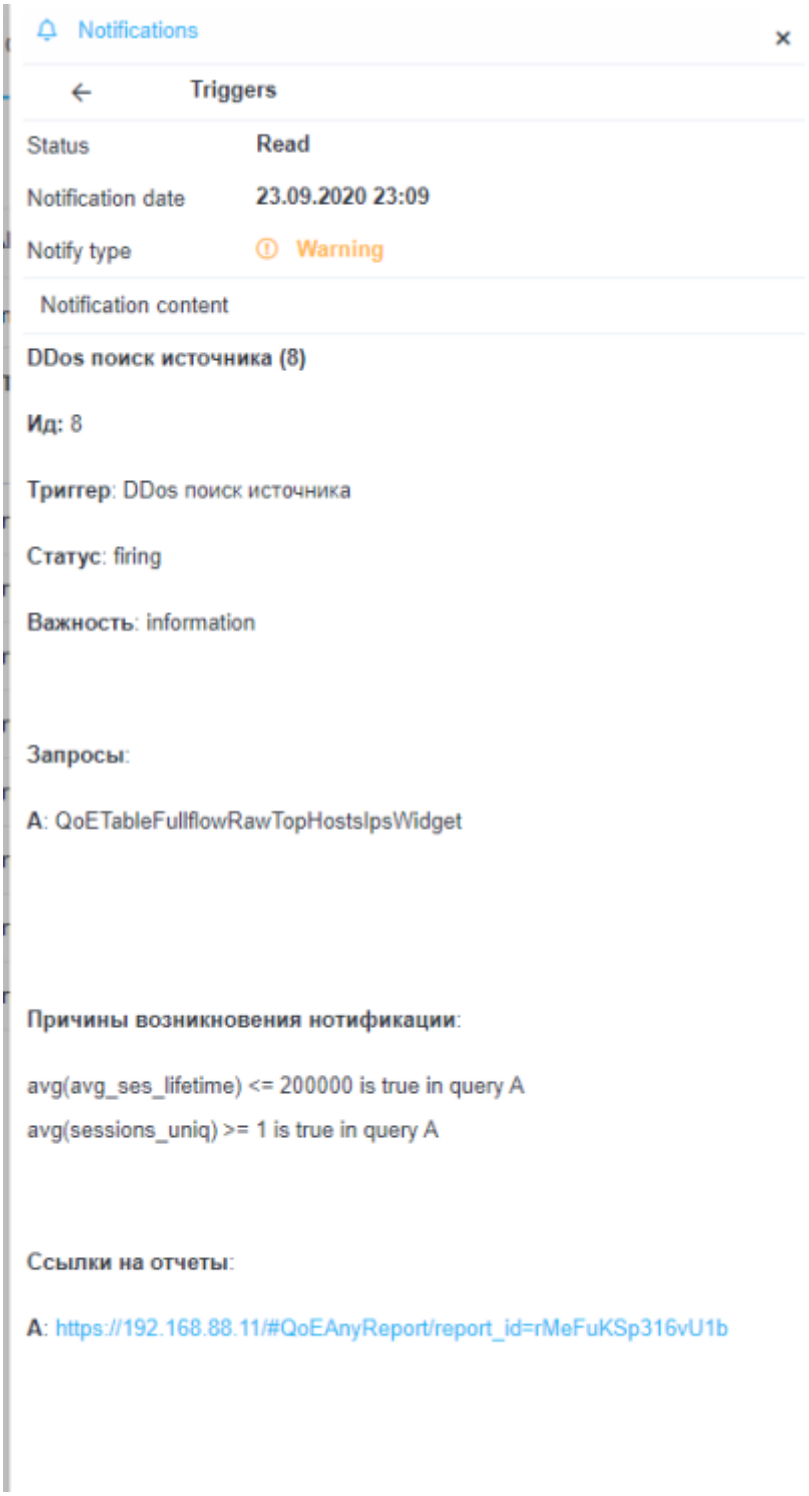
- Для автоматического заполнения — кликнуть (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ



Получить ссылку на отчет можно через меню нотификаций

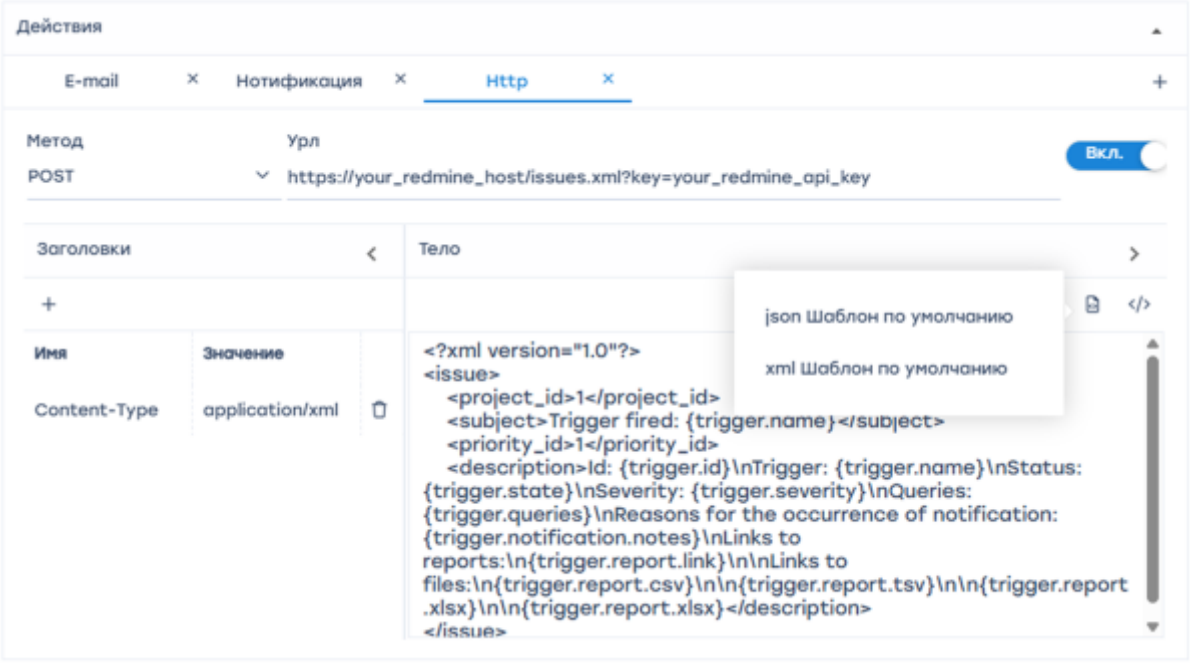


Выбрать нотификацию Выбрать — "Детали"



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

Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.