Table of Contents

Поиск DDoS атак с использованием триггеров в QoE 3
Пример настройки триггера на поиск источника DDOS-атаки типа Flood 3
Пример настройки триггера на поиск цели DDOS-атаки типа Flood 9
Анализ BotNet 10
Фиксация перехода абонента на ресурс конкурента 11

Поиск DDoS 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:

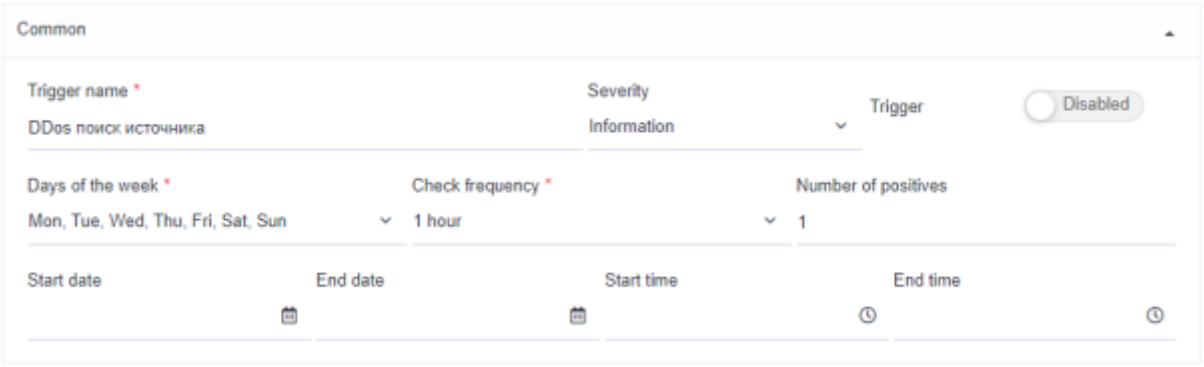
- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

- DPIUI2 (GUI - Графический интерфейс управления)
- QoE Stor (Модуль сбора статистики)

Пример настройки триггера на поиск источника DDOS-атаки типа Flood

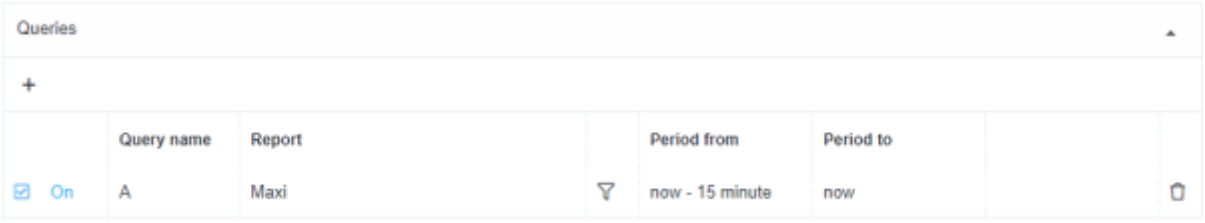
Общая информация триггера



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.

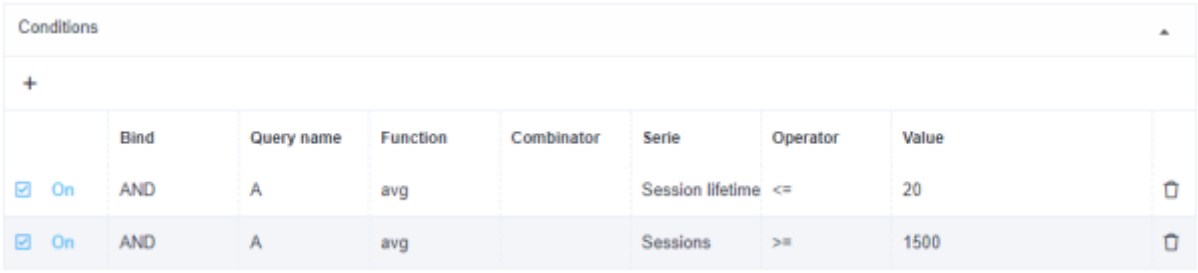
Запросы



- Добавить поле
- Название A
- Выбрать таблицу для сканирования: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Выбрать период с: «now – 15minute», период по : «now»

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

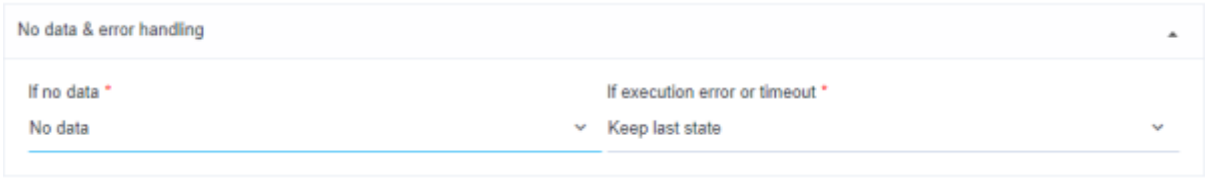
Условия



- Добавить "+" 2 поля
- Связка – И
- Функция – avg
- Серия в 1 поле – время жизни сессии <= 20(мс)
- Серия во 2 поле – количество сессий >= 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

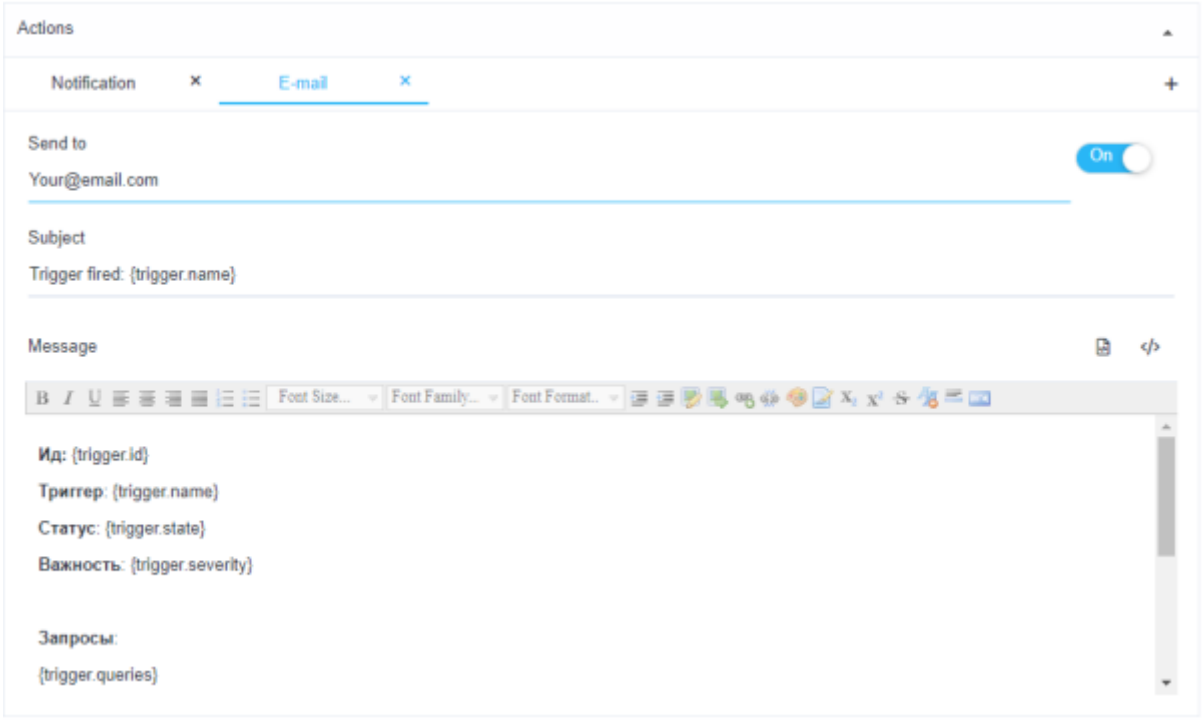


- В поле "Если нет ошибок" — нет данных
- В поле "Если есть ошибка или таймаут" — сохранить последнее состояние

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

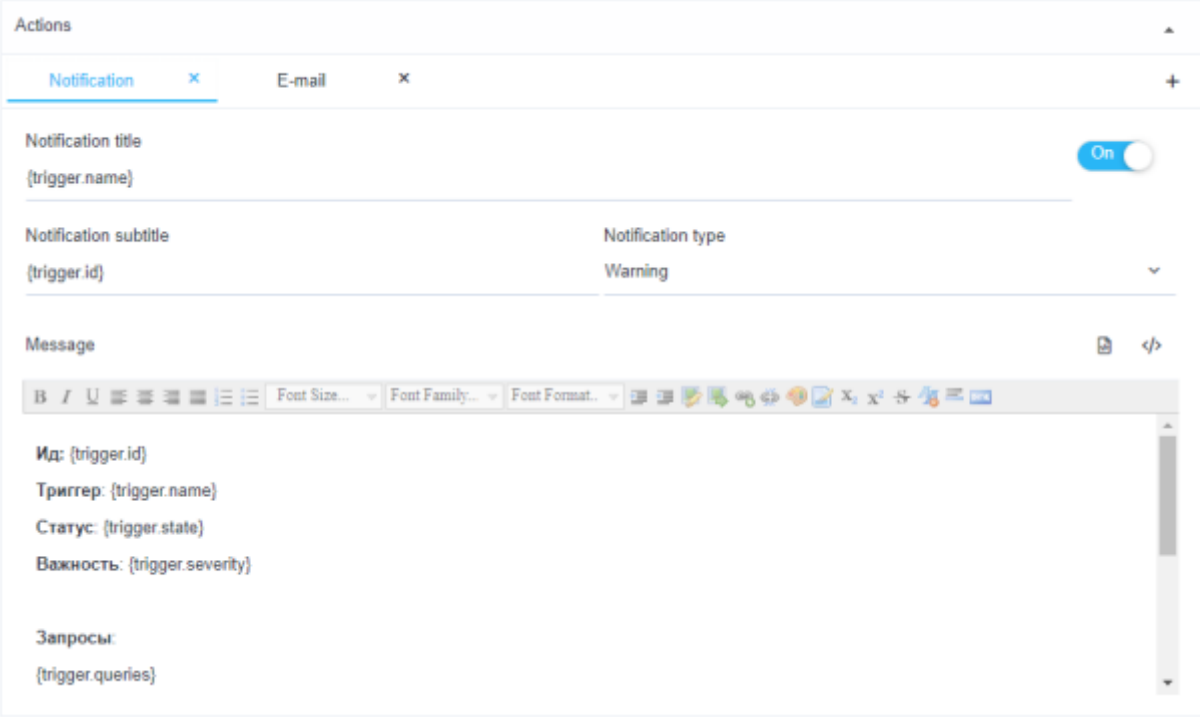
Действия

E-mail действие

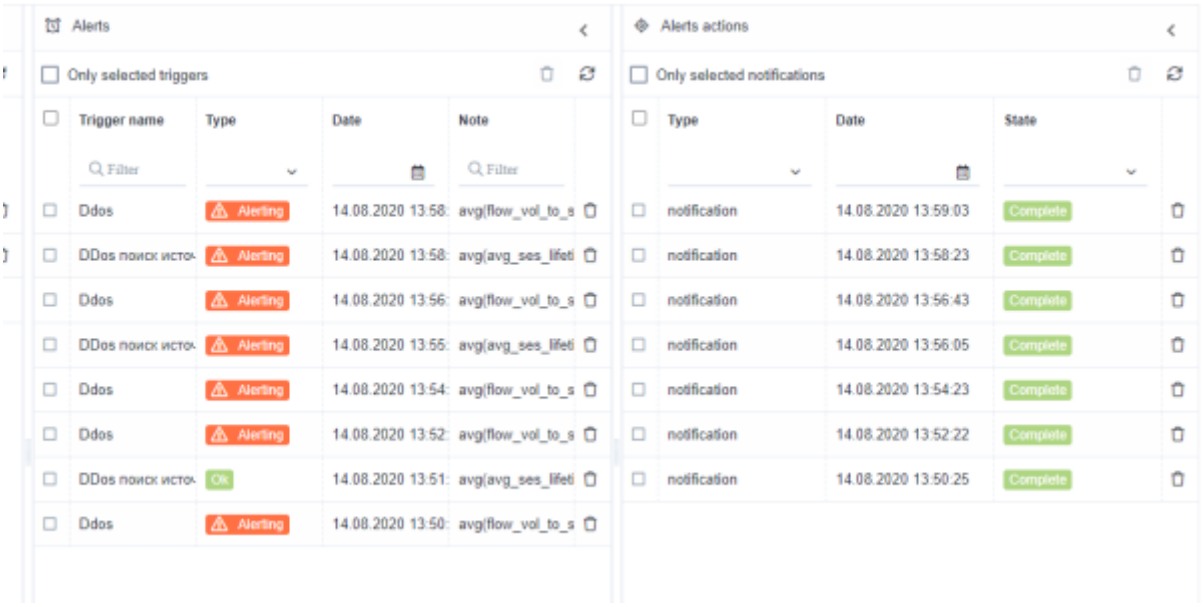


- Для автоматического заполнения — кликнуть по иконке "</>" (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты
- При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус,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

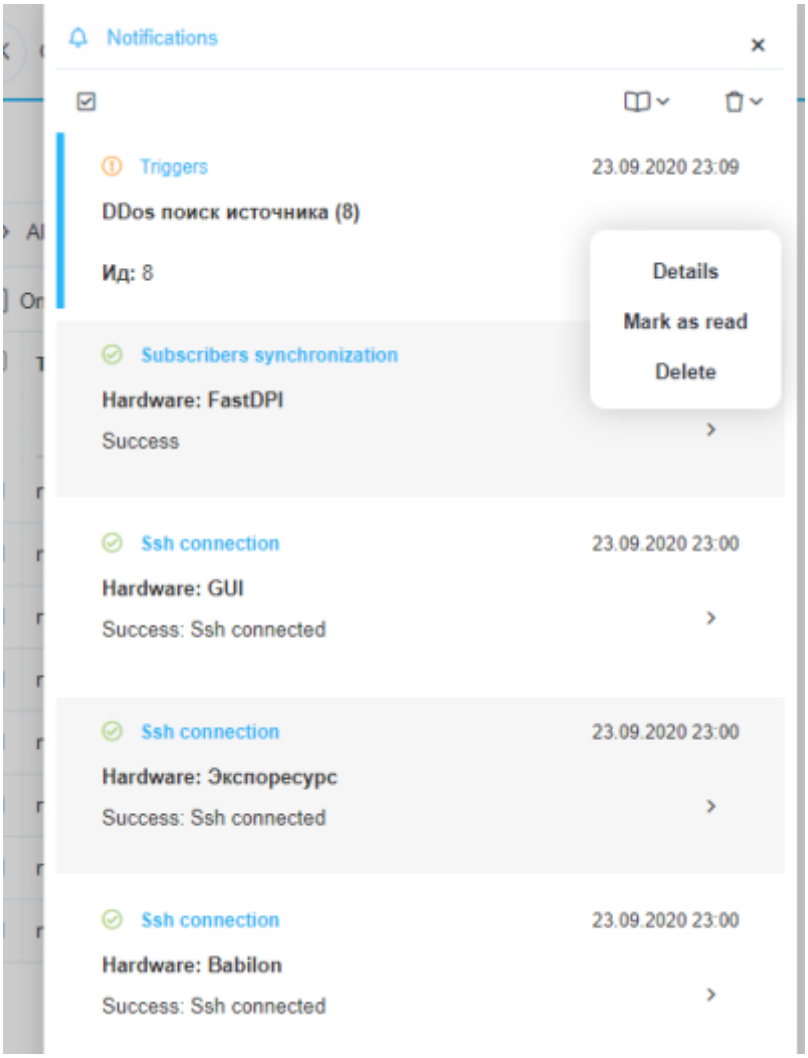
Нотификация



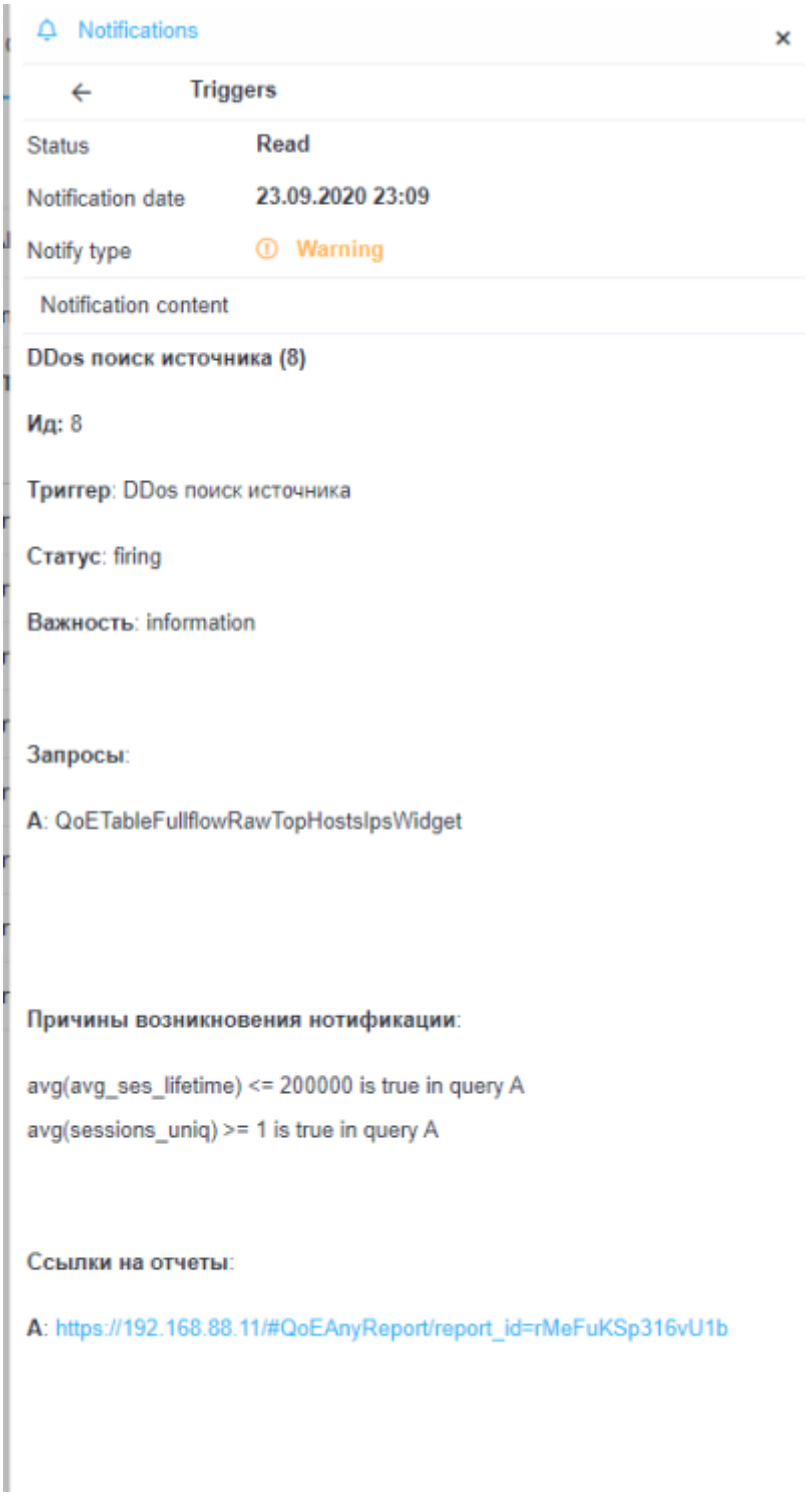
- Для автоматического заполнения — кликнуть "</>" (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ



Получить ссылку на отчет можно через меню нотификаций

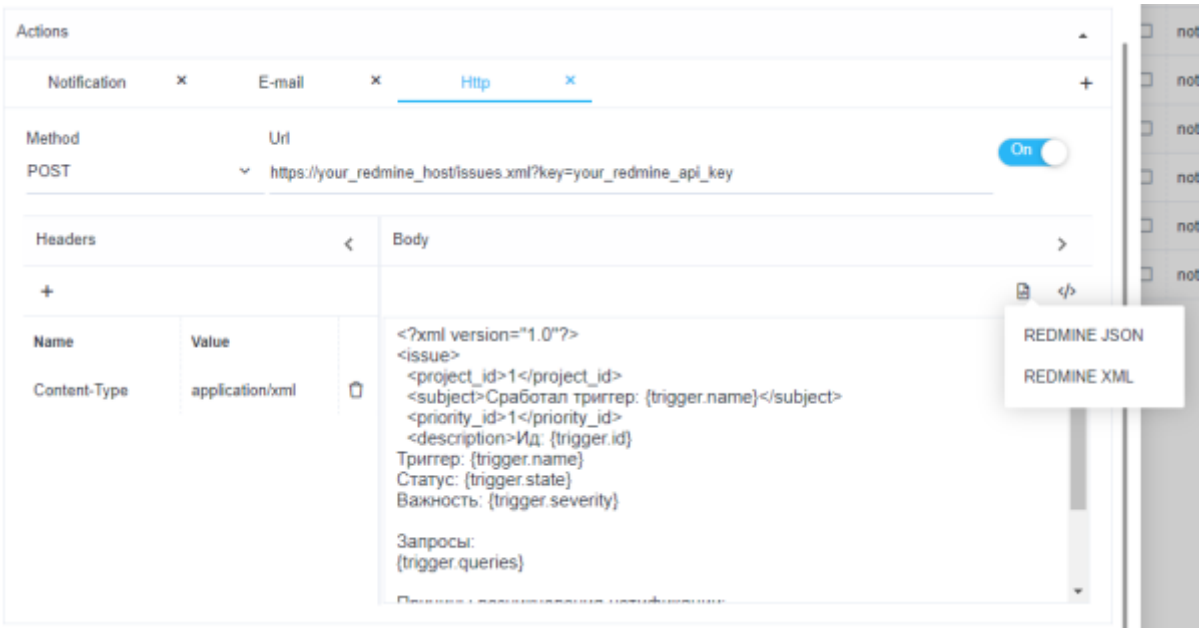


Выбрать нотификацию Выбрать — "Детали"



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

HTTP действие



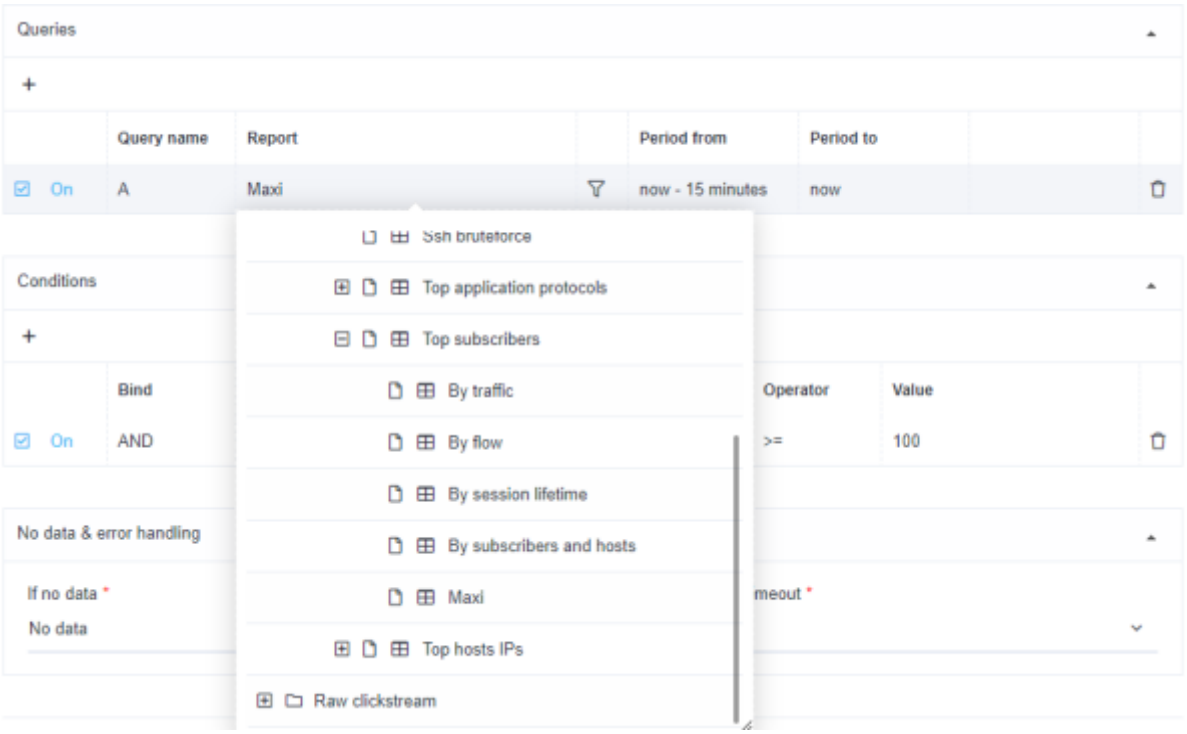
Для автоматического заполнения — кликнуть "</>" (автоматическое заполнение формы)
Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес

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 Raw full netflow → Tables → Attacks detection → Top subscribers → 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

Queries

	Query name	Report		Period from	Period to		
On	A	Maxi		now - 15 minute	now		
On	B	Full raw log		now - 15 minute	now		

- Выбрать Raw full netflow → Tables → Attacks detection → Top application protocols → Maxi для значения "A"
- Raw full network → Tables → Raw log → Full raw log для значения "B"

Условия

Conditions

	Bind	Query name	Function	Combinator	Serie	Operator	Value	
On	OR	B	avg		Destination port	=	6667	
On	OR	B	avg		Source port	=	6667	
On	OR	B	avg		Destination port	=	1080	
On	OR	B	avg		Source port	=	1080	
On	AND	A	avg		Flow, Pkts/s	>=	2000	

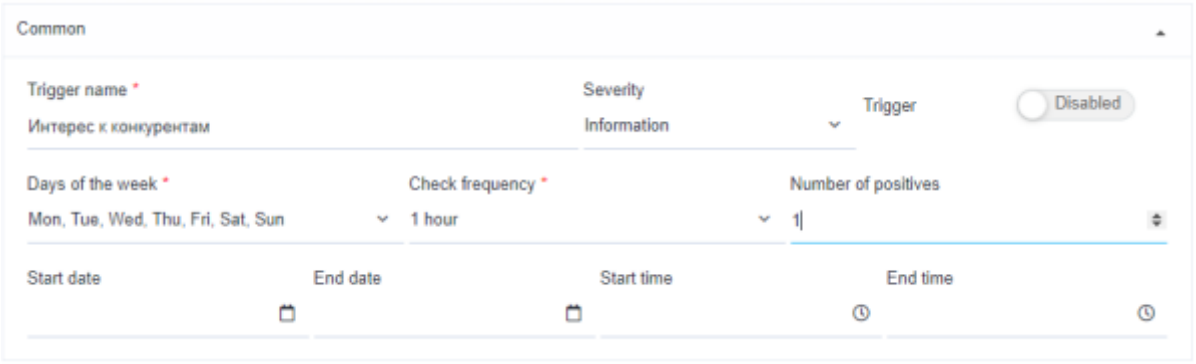
Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "B" со значением "ИЛИ", и Flow Pcts/s больше или равно 2000.

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

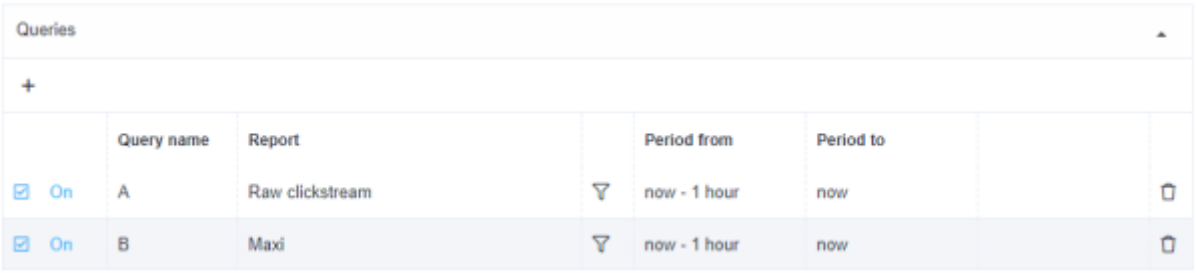
Общая информация триггера



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

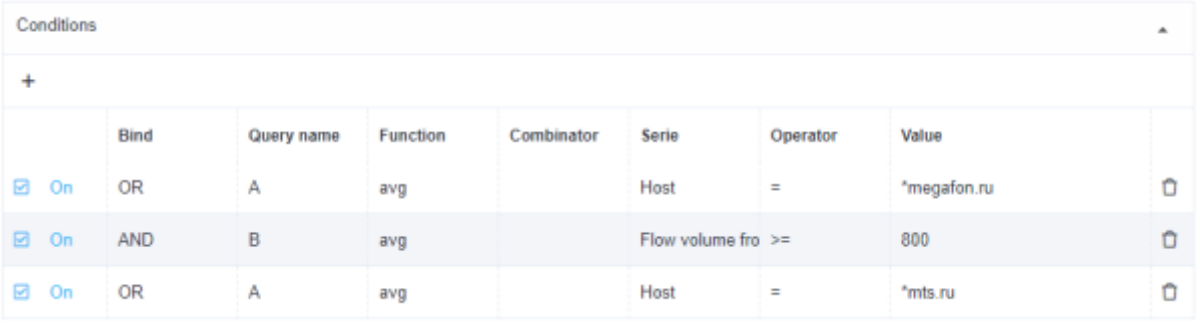
Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

Запросы



- Добавить "+" поле
- Название A
  Выбрать таблицу для сканирования: Raw clickstream → Tables → Raw clickstream
- Название B
  Выбрать таблицу для сканирования: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Выбрать период с: «now – 1 hour», период по : «now»
- В этом случае будет происходит анализ трафика каждый час по выбранным таблицам.

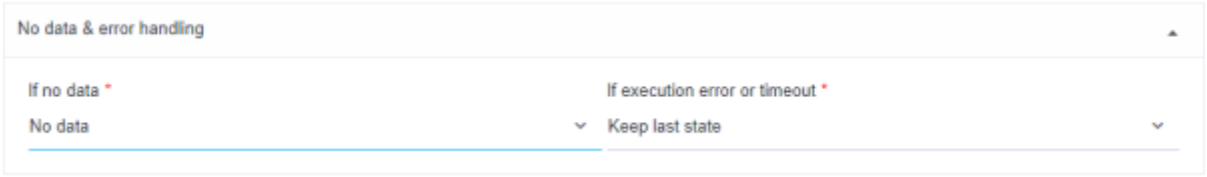
Условия



- Добавить "+" поле 3 поля
- Первое поле — выбрать таблицу "А"; Связка – "Или"; Функция – "avg";Серия Host = *megafon.ru(или ваш любимый конкурент)
- Второе поле — выбрать таблицу "Б"; связка "И"; Функция – "avg";Серия Flow volume from subscriber, Pct/s >= 800

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

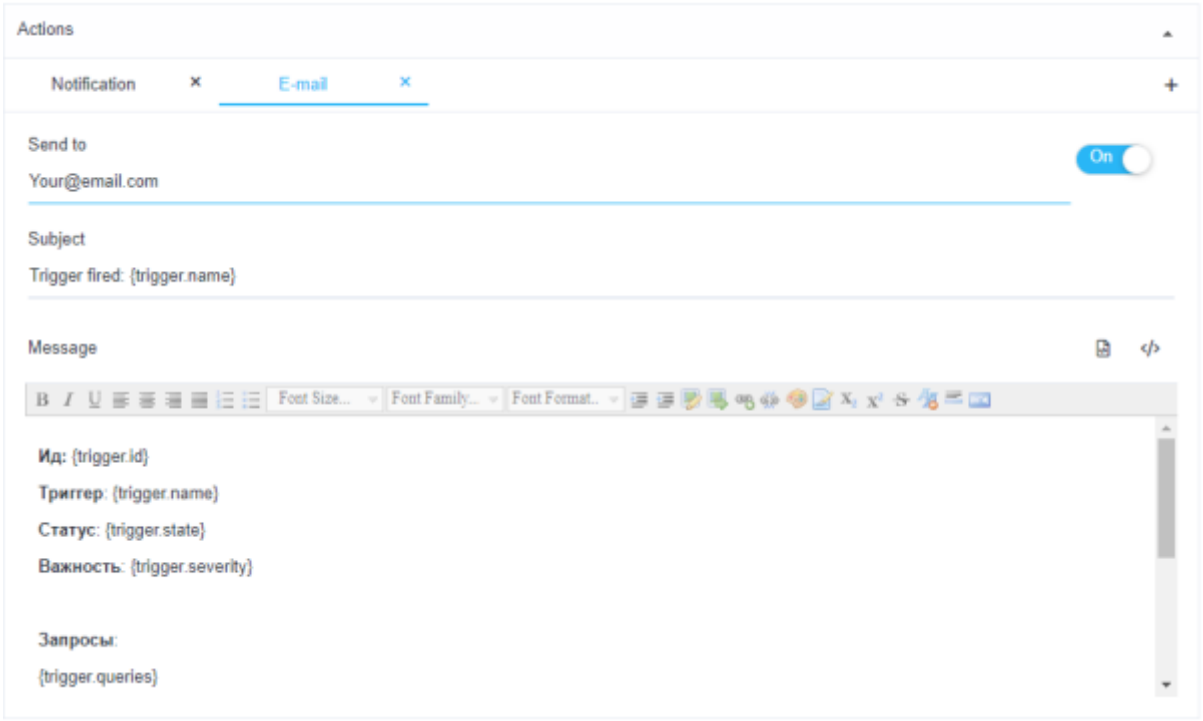


- В поле "Если нет ошибок" — нет данных
- В поле "Если есть ошибка или таймаут" — сохранить последнее состояние.

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

Действия

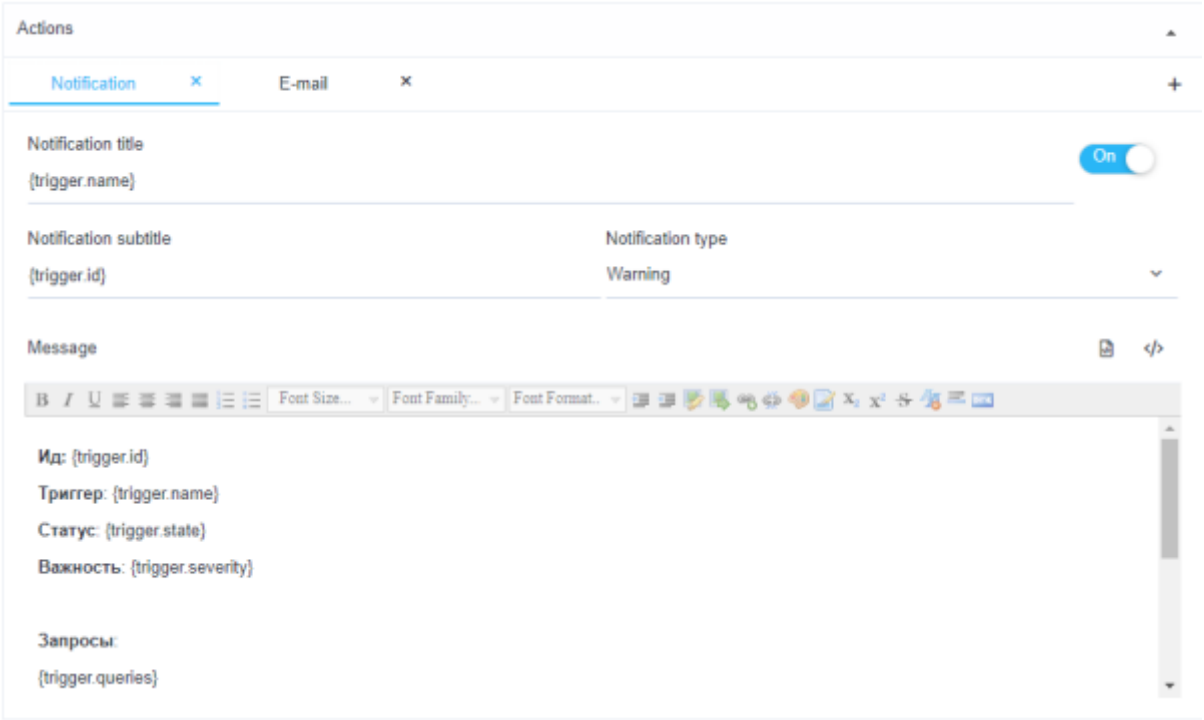
E-mail действие



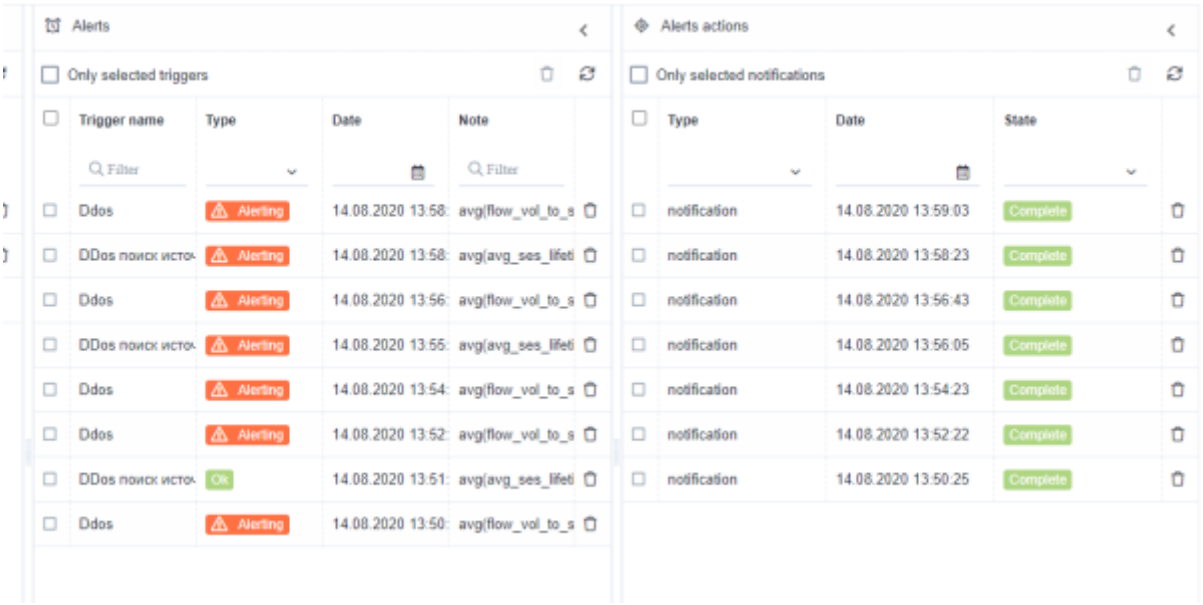
- Для автоматического заполнения — кликнуть (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты

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).

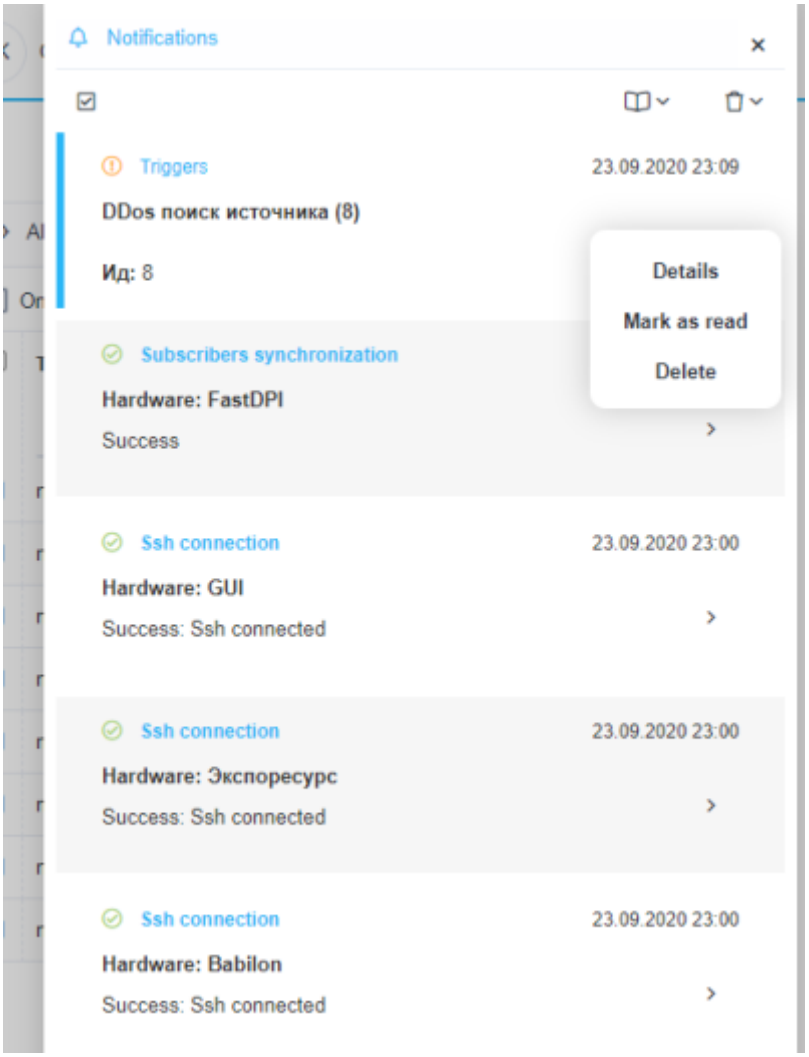
Нотификация



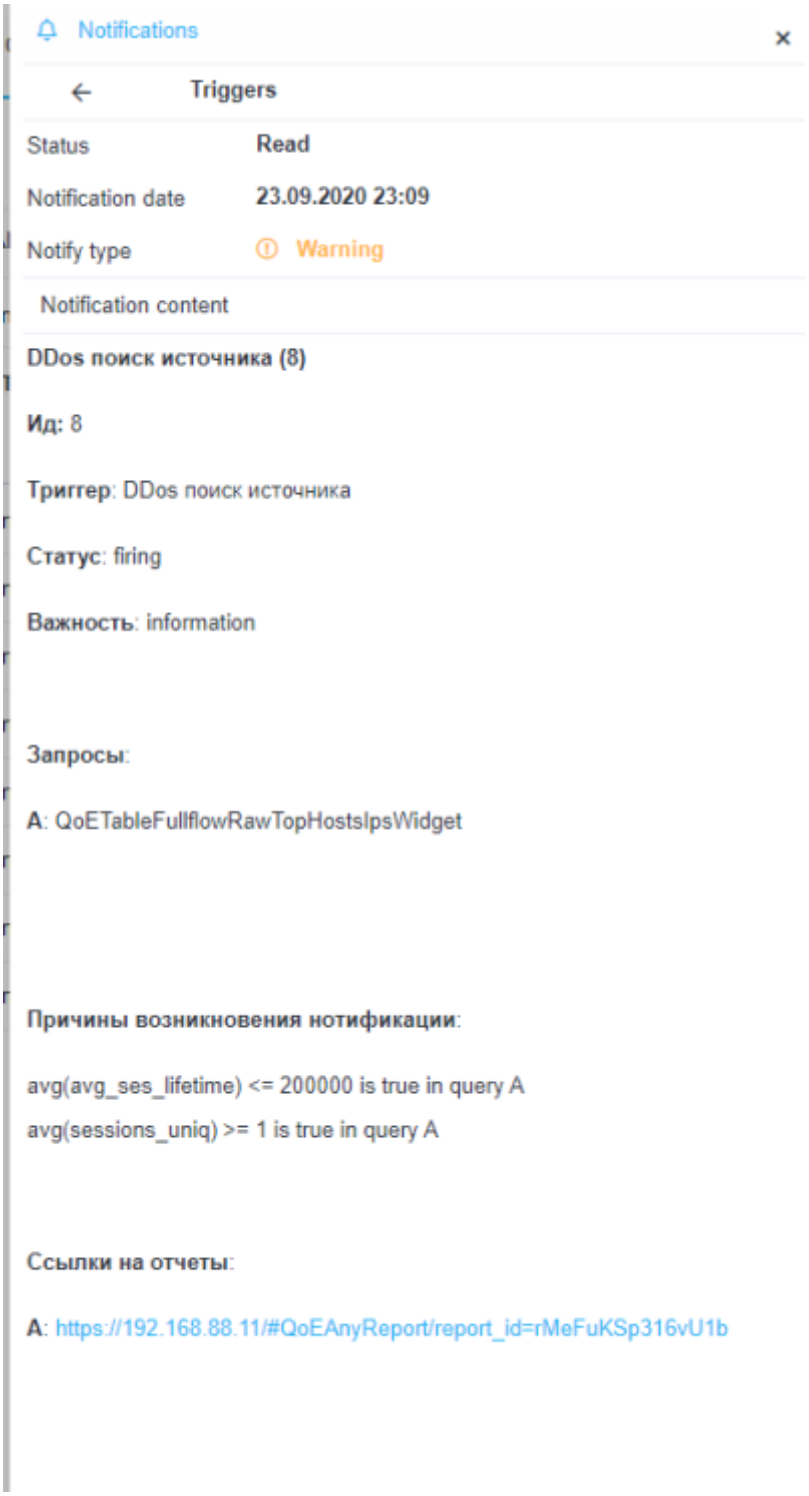
- Для автоматического заполнения — кликнуть "</>" (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ



Получить ссылку на отчет можно через меню нотификаций

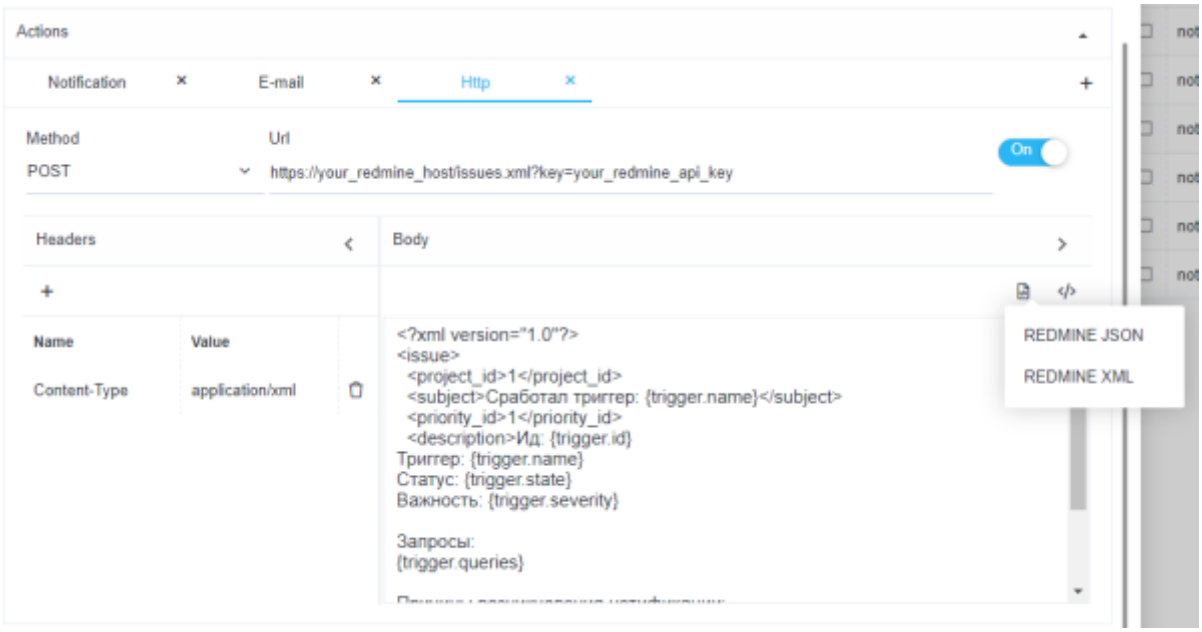


Выбрать нотификацию Выбрать — "Детали"



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.