Содержание

QoE Триггеры и Нотификация	3
Назначение	. 3
Создание и настройка триггеров	3
Шаг 1. Расписание работы	3
Шаг 2. Выбор источника данных и метрики	4
Шаг З. Условия	7
Шаг 4. Обработка ошибок	8
Шаг 5. Действия	8
Описание элементов страницы "Триггеры и Нотификация"	12

QoE Триггеры и Нотификация

Назначение

В разделе "Триггеры и Нотификация" Вы сможете настроить отправление периодических отчетов и оперативных алертов в Telegram или на E-mail с отображением их в самом GUI. При срабатывании триггера будет приходить сообщение с информацией о заданном событии и ссылками на соответствующие отчеты. По умолчанию это 4 отчета в форматах csv, tsv, xlsx, pdf, но шаблон сообщения можно редактировать.



Для работы раздела "Триггеры и Нотификация" требуется активация подписки — лицензия Standard для GUI.

Сделаем настройки на примере двух сценариев:

- Периодический отчет для отслеживания задержки RTT от абонента.
 В отчете будут отображаться абоненты, у которых значение "RTT от абонента" больше либо равно 150000 мс. Он будет приходить по понедельникам и четвергам в Telegram.
- Алерт об абонентах-участниках ботнета.
 Настроим проверку таблицы раз в минуту каждый день. На почту будет приходить нотификация как только в таблице будет замечен хотя бы один зараженный абонент.

Создание и настройка триггеров

- 1. В GUI перейти в раздел QoE аналитика → Триггеры и Нотификация.
- 2. Нажать на + на дашборде "Триггеры" для добавления триггера. Откроется окно настройки.

Создание нового триггера происходит в 5 шагов. Настройки триггеров разделены на блоки, необходимо заполнить все из них.

Шаг 1. Расписание работы

Заполните обязательные поля:

- Название любое уникальное имя для триггера.
- Важность выбор степени важности: информация, предупреждение, средняя/высокая важность. Например, степень "Информация" можно задать для отчета, а все остальные разным нотификациям по вашему усмотрению. **Необязательное поле.**
- Дни недели проверки в какие дни недели будет работать триггер.
- Частота проверки как часто будет запускаться скрипт проверки. Например, если выставлено значение "1 минута" скрипт проверки будет запускаться в заданные дни недели раз в минуту.
- Дату и время начала и окончания работы триггера. Необязательные поля.

Также в этом блоке расположен переключатель для включения/выключения триггера, **после** окончания настройки не забудьте его включить.

Общее				
Название триггера *		Важность	Триггер	Выклю
Задержка RTT		Информация	v	
Дни недели *	Частота пр	оверки *	Количество срабатываний	
Пн, Чт	✓ 24 часа		~ 0	
Дата начала	Дата окончания	Время начала	Время окончания	я
		*	0	
3 этом случае ск аса — один раз Іример заполнен	рипт проверки бу в понедельник и о иия блока для ноти	/дет запускаться дин раз в четверн ификации об абон	а по заданным дня г. нентах с киберугро	ім ра зами
3 этом случае си аса — один раз Іример заполнен общее	рипт проверки бу в понедельник и о иия блока для ноти	/дет запускаться дин раз в четверн ификации об абон	а по заданным дня г. чентах с киберугро	ім ра зами:
3 этом случае си аса — один раз Іример заполнен общее	рипт проверки бу в понедельник и о иия блока для ноти	/дет запускаться дин раз в четверн афикации об абон	о я по заданным дня г. нентах с киберугро	ім ра: зами:
3 этом случае си аса — один раз ример заполнен общее название триггера • зараженные абоненты	рипт проверки бу в понедельник и о иия блока для ноти	/дет запускаться дин раз в четверн ификации об абон Вожность Предупреждение	а по заданным дня г. нентах с киберугро	ам ра: зами: выклю
В этом случае си аса — один раз Іример заполнен Общее Название триггера • Зараженные абоненты Дни недели •	срипт проверки бу в понедельник и о ния блока для ноти	/дет запускаться дин раз в четверн фикации об абон Важность Предупреждение	а по заданным дня г. нентах с киберугро Триггер	ам ра: зами: Выклю
В этом случае си аса — один раз Іример заполнен Общее Название триггера * Зараженные абоненты Дни недели * Пн. Вт. Ср. Чт. Пт. Сб. Во	срипт проверки бу в понедельник и о иия блока для ноти частота при частота при	/дет запускаться дин раз в четверн фикации об абон Важность Предупреждение	а по заданным дня г. нентах с киберугро триггер Количество срабатываний о	ам раз зами: Выклю
В этом случае си аса — один раз Іример заполнен Общее Название триггера • Зараженные абоненты Дни недели • Пн, Вт, Ср, Чт, Пт, Сб, Во Дата начала	срипт проверки бу в понедельник и о иия блока для ноти частота при частота при частота при зата окончания	/дет запускаться дин раз в четверн пфикации об абон Важность Предупреждение оверки	а по заданным дня г. нентах с киберугро триггер Количество срабатываний о Время окончания	ам ра: зами: выклю

Шаг 2. Выбор источника данных и метрики

Выбрать метрику и таблицу данных. Триггеры работают только с готовыми таблицами, которые находятся в разделах "Нетфлоу" и "Кликстрим", для начала настройки нужно найти таблицу, где есть необходимая метрика.





Для создания запроса нажать на + под названием блока.

- Отчет выбор таблицы с данными из готовых отчетов системы, по которым производится поиск.
- "Период с" и "-по". Например, если нужно анализировать данные за последние сутки, задайте "Период с" 24 часа, "Период по" сейчас.



"Сейчас" в периоде с/по в запросе означает момент запуска триггера. Он складывается из дней недели работы триггера и верхней границы частоты проверки (из блока настроек "Общее").

Для каждого запроса можно создать фильтр, где можно задать значение IP хоста, логина абонента и т.д. Например, можно настроить формирование отчета или нотификации по одному конкретному хосту, если задать такой фильтр:

Запросы																
+																
	Название	Отчет			Перис	одо		Период по								
🗹 Вкл.	А	Топ хостов	с высоким тра	фиком 71	8	≣	Фильт	к								
					Coxpo	+							Истор			
Условия					ненн			Фильтр	Оператор	Значение			RMG			
+					ыe фr		Вкл.	Хост	=	google.com		Û	1			
	Связь	Название	Функция	Комбинатор	ивтрь		Выкл.	Абонент	like		T	Û	1			
🗹 Вкл.	и	A	max	если не NaN			Выкл.	Логин	like		1	Û				
Ofeefer	n ourse ou						Выкл.	IP хоста	like		Ð	Û				
Copulotik	O OLDHOOK						Выкл.	Протокол	like		۲	Û				
Если нет Нотифия	аданных • кация			⊻ Нот	n v		Выкл.	Группы прикладных протоколов	in			Û				
							Выкл.	Прикладной протокол	like		1	Û				
Roŭernuo							Выкл.	Номер АС источника	like		٢	Û				
деиствия							Выкл.	Номер АС получателя	like		1	Û				
Нотификация ×							Выкл.	Категория хоста	in			Û				
Заголова {trigger.r	ок нотификац name}	ии			•		Выкл.	Категория зараженного трафика	in			Û	4			
Подзагол	ловок нотифи	кации		Тип	ŀ	Отменить При										

Пример заполнения блока для отчета для отслеживания задержки RTT от абонента. Здесь нужно выбрать отчет "Топ абонентов с высоким RTT", в нем есть нужные метрики для данного триггера. Так как нужно, чтобы отчет приходил по понедельникам и четвергам, "Период с" выставить равным промежутку между этими днями — "Сейчас - 4 дня", будут анализироваться данные за последние 4 дня.

3ar	просы						*
+							
		Название	Отчет		Период с	Период по	
	Вкл.	A	Топ абонентов с высоким RTT	7	сейчас - 4 дня	сейчас	Û

Пример заполнения блока для нотификации об абонентах с киберугрозами. Здесь нужно выбрать отчет "Топ зараженных абонентов с ботнет трафиком", в нем есть нужные метрики для данного триггера. В данном случае будут анализироваться данные за последние 24 часа.

Запросы												
+												
	Название	Отчет		Период с	Период по							
🗹 Вкл.	А	Топ зараженных абонентов с ботнет трафиком	7	сейчас - 24 часа	сейчас	Ċ						

Шаг З. Условия

Задать условия — что должно произойти с метрикой для срабатывания триггера. Для создания условия нажать на + под названием блока.

Для каждого условия нужно настроить следующие параметры:

- Связь И/ИЛИ сопоставить с названиями запросов на предмет выполнения либо сразу нескольких условий, либо хотя бы одного из заданных.
- Название выбрать один из созданных запросов.
- Функция выбрать тип агрегатной функции, которая будет применена к значениям в условии:
 - "count" считает количество элементов или записей в наборе данных,
 - "any" возвращает любое значение из доступных в наборе данных,
 - "anyLast" возвращает последнее значение из доступных в наборе данных,
 - "avg" вычисляет среднее значение числовых данных в наборе,
 - "min" возвращает минимальное значение из доступных в наборе данных,
 - "max" возвращает максимальное значение из доступных в наборе данных,
 - "sum" вычисляет сумму числовых данных в наборе,
 - "uniq" возвращает уникальные значения в наборе данных, удаляя дубликаты.
- Комбинатор выбрать нечисловое/ненулевое/числовое/нулевое значение или оставить пустым.
- Серия выбрать нужную метрику из отчета.
- Оператор выбрать: =, !=, >, >=, <, <=, between (будет возвращать записи, где выражение находится в диапазоне значений value1 и value2 включительно), not between (возвращает все записи, где выражение НЕ находится в диапазоне между value1 и value2 включительно).
- Значение присвоить необходимое значение для условия.

Ye	Условия													
+	+													
		Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение						
	Вкл	и	A	any	если не NaN	RTT от абонента, мс	>=	150000						
В з зна	этом ачени ример	случае ие RTT с заполн	триггер от абонент чения блон	будет ср га больш ка для ал	абатываты е либо рав тертов об а	, если в табли ное 150000 мс. бонентах с киб	це из ша еругроза	ага 2 поя ми:	16					
В з зна	этом ачени ример	случае ие RTT с заполн	триггер (от абонент чения блок	будет ср га больш ка для ал	абатываты е либо рав тертов об а	, если в табли ное 150000 мс. бонентах с киб	це из ша еругроза	ага 2 поя ми:	18					
В з зна Пр	этом ачени оимер	случае ие RTT с заполн	триггер (от абонент чения блок	будет ср га больш ка для ал	абатываты е либо рав тертов об а	, если в табли ное 150000 мс. бонентах с киб	це из ша еругроза	ага 2 поя ми:	ΪB					
В з зна Пр ж +	этом ачены оимер словия	случае ие RTT с заполн	триггер (от абонент чения блок	будет ср га больш ка для ал	абатываты е либо рав тертов об а	, если в табли ное 150000 мс. бонентах с киб	це из ша еругроза	ага 2 поя ми:	iΒ					
В з зна пр	этом ачени ример словия	случае ие RTT о заполн	триггер (от абонент чения блок	будет ср га больш ка для ал	абатываты е либо рав пертов об а Комбинатор	, если в табли ное 150000 мс. бонентах с киб Серия	це из ша еругроза Оперотор	ага 2 поя ми: значение	iΒ					

Шаг 4. Обработка ошибок

Задать поведение триггера при ошибках.

В полях "Если нет данных" и "Если есть ошибка выполнения или тайм-аут" выбрать одно из значений:

- "Нотификация" условие, заданное в триггере, выполнено.
- "Нет данных" при обработке отчетов, заданных в триггере, не найдено данных.
- "Сохранить последнее состояние" не нужно предпринимать никаких действий.
- "Ок" условия, заданные в триггере, не сработали, все в порядке и никаких действий выполнять не нужно.

	Пример заполнения блока	для отчета и для алертов:
	Обработка ошибок	*
\bigcirc	Если нет данных * Ok	Если ошибка выполнения или тайм-аут * ~ Нотификация ~
	В обоих случаях если нет, не будет приходить, если нотификация.	данных — триггер не будет срабатывать и сообщени 1 возникла ошибка или тайм-аут — будет приходит

Шаг 5. Действия

Настройка действия позволит в случае срабатывания триггера получать сообщение на E-mail или в Telegram.

Для создания действия нажать на + под названием блока.

Для удаления действия нажать на × напротив названия действия.

Telegram действие

Шаг 1. Регистрация своего бота через https://t.me/BotFather

- 1. Запустить BotFather командой /start.
- 2. Нажать / newbot для создания нового бота.



3. Ввести название бота.



		_		
По	исж	×	🗈 Сохранить 🖽	
	Управление DPI	~	86 Настройки	В Настройки Telegram
ác.m			Общие	Такен API Telegram бота (TELEGRAM_BOT_API_TOKEN)
200	Управление PCRF	Ť	Интервалы джобов	5975002635:AAGdSROudY9K9uxENaPu2HF4azmpsKQq98P
*	QoE аналитика	~	QoE Stor: Соединение с БД (Clickhouse)	T
0	Сервисы VAS cloud	~	QoE Stor: Ностройки времени жизни БД	
			QoE Stor: Настройки дисков	
යිම	Администратор	^	Настройки SMTP	
	Оборудование		Системные	
	Пользователи		Подключение к БД MySql	
	Роли		Настройки пуш-нотификаций	
	Kondbervoouws GUI		Настройки SSO-авторизации	
	Dorse GUII		Настрайки карты	
	Ofwormer GUI		Настрайки VasCloud	
			Настрайки кластера	
	Конфигурация QoE Stor		Настрайки резервного копиралания	
	Логи QoE Stor		Настройки авто восстановления из резервных копий	
	Конфигурация САРТСНА		Настройки Telegram	
	Темплейт САРТСНА		Настройки Триггеров	

Шаг 2. Получение id чата для своего персонального Telegram-аккаунта через https://t.me/RawDataBot



Для получения id чата у пользователя в Telegram-профиле должен быть задан username!

- 1. Запустить Telegram Bot Raw командой /start.
- 2. Скопировать id, выглядит так:



Шаг 3. Подключение Telegram к настроенному триггеру

Добавить id из шага 2 в Telegram действие в поле "Идентификатор чата".

Действия	*
Telegram ×	+
Идентификатор, ата 222455434	Вкл.

E-Mail действие

Создает уведомление и посылает его на выбранный адрес электронной почты.

- Если поле "Сообщение" не заполнено нажать на кнопку "Установить шаблон по умолчанию" (1) для заполнения полей действия значениями по умолчанию. При необходимости все значения можно отредактировать.
- 2. При нажатии на кнопку "Параметры шаблона" (2) Откроется меню с идентификаторами, которые можно использовать для составления сообщения.

Действия	
E-mail × Telegram ×	+
Кому	Вкл.
elena.krasnobryzh@vas.expert	
Тема	
Сработал триггер: {trigger.name} 2.	
1	
Сообщение	φ (h
B I U 書 書 書 目 日 Font Size マ Font Family. マ Font Format マ 運 運 夢 馬 吗 会 参 ② X x + + 小客 電 二	
Ид: {trigger.id}	Î
Триггер: {trigger.name}	
Ctatyc: (trigger.state)	- 11
Важность: {trigger.severity}	
Запросы:	
{trigger.queries}	-

Для работы E-mail действия нужно настроить SMTP. Перейти в раздел Администратор →

Конфигурация GUI, выбрать "Настройки SMTP".

Нотификация в GUI

Нотификацию можно использовать для проверки работоспособности триггеров.

- 1. Нажать на кнопку "Установить шаблон по умолчанию" (1) для заполнения полей действия значениями по умолчанию. При необходимости все значения можно отредактировать.
- 2. При нажатии на кнопку "Параметры шаблона" (2) Откроется меню с идентификаторами, которые можно использовать для составления сообщения.

Действия	*
E-mail × Telegram × Нотификация	× +
Заголовок нотификации	Вкл.
{trigger.name}	
Подзаголовок нотификации	Тип нотификации
{trigger.id}	Предупреждение 2
Сообщение	1
B I U II	L → ヨヨ夢馬 哟 ⊕ ● ⊇ X, x' S / 雪 = 四
Ид: {trigger.id}	Í.
Триггер: {trigger.name}	
Ctatyc: {trigger.state}	
Важность: {trigger.severity}	
Запросы:	
{trigger.queries}	*

После создания триггера нажать "Сохранить". На дашборде "Триггеры" включить необходимые триггеры. Если страница GUI не обновлялась — обновить страницу в браузере или нажать на кнопку "Обновить".

¢	Триг	геры						<	껑	ថ្លៃ Нотификации					٠	Ф Действия			
+	ł						Û	ø	Только выбранные триггеры						П Только выбранные нотификации				Ø
			Название	Дни	Частота	Тип триггера	Статус			Название	Тип	Дата	Заметка			Тип	Дата	Статуо	
			Q, $\phi_{RIBT]}$	v	~	×	~			Q Фильтр	×	Ö	Q Фильтр			~		~	
	Φ		Топ абонен	Пн,Вт,Ср,Ч	т 1 минута	Пользовательски	Готов	٥		Топ абонентов	🛕 Нотификация	14.06.2023 10:57:04	Error: Frozen job	٥		E-mail	14.06.2023 11:06:05	Мако, число попыток	٥
	Θ	2	Дельта пак	Πτ	1 минута	Пользовательски	Готов	Û		Топ абонентов	\Lambda Нотификация	14.06.2023 10:46:44	Error: Frozen job	Û		E-mail	14.06.2023 10:54:23	Мако, число попыток	Û
	Φ		test2	Пн	1 минута	Пользовательски	Готов	Û		Топ абонентов	\Lambda Нотификация	14.06.2023 10:36:24	Error: Frozen job	Û		E-mail	14.06.2023 10:44:03	Маке, число попыток	Û
	Θ	Z	test	Пн	1 минута	Пользовательски	Готов	٥		Топ абонентов	\Lambda Нотификация	14.06.2023 10:25:44	Error: Frozen job	۵		E-mail	14.06.2023 10:33:25	Мако, число попыток	٥
										Топ абонентов	\Lambda Нотификация	14.06.2023 10:15:43	Error: Frozen job	Û		E-mail	14.06.2023 10:23:44	Мако, число попыток	Û
										Топ абонентов	\Lambda Нотификация	14.06.2023 10:05:04	Error: Frozen job	Û		E-mail	14.06.2023 10:13:02	Мако, число попыток	Û
										Топ абонентов	\Lambda Нотификация	14.06.2023 09:54:43	Error: Frozen job	۵		E-mail	14.06.2023 10:02:23	Маке, число попыток	Û
										Топ абонентов	🛆 Нотификация	14.06.2023 09:44:28	Error: Frozen job	۵		E-mail	14.06.2023 09:52:02	Мако, число попыток	Û
										Топ абонентов	\Lambda Нотификация	14.06.2023 09:34:23	Error: Frozen job	Û		E-mail	14.06.2023 09:42:24	Мако, число попыток	Û
										топ абонентов	\Lambda Нотификация	14.06.2023 09:23:48	Error: Frozen job	Û		E-mail	14.06.2023 09:31:23	Маке, число попыток	Û
										Топ абонентов	\Lambda Нотификация	14.06.2023 09:13:43	Error: Frozen job	٥		E-mail	14.06.2023 09:21:02	Мако, число попыток	٥
										Топ абонентов	\Lambda Нотификация	14.06.2023 09:03:23	Error: Frozen job	Û		E-mail	14.06.2023 09:11:04	Мако, число попыток	Û
										Топ абонентов	\Lambda Нотификация	14.06.2023 08:53:23	Error: Frozen job	Û		E-mail	14.06.2023 09:00:44	Маке, число попыток	Û
										Топ абонентов	💧 Нотификация	14.06.2023 08:43:0	Error: Frozen job	٥		E-mail	14.06.2023 08:50:23	Мако, число попыток	٥
										Топ абонентов	🛆 Нотификация	14.06.2023 08:33:03	Error: Frozen job	Û		E-mail	14.06.2023 08:40:23	Макс, число попыток	Û

Описание элементов страницы "Триггеры и Нотификация"

Перейти в раздел QoE Аналитика → Триггеры и Нотификация. Откроется раздел как на картинке ниже.

=		QoE	аналитика	> Триггерь	ы и Нотифия	кация															" • •
Coc	гояна	е пор	писки: ОСТАЛС	ось 2741 дней	~	Состояние п	одписк	И							E E	сли Іоти	в триггер фикация	ое вы ″, она	брано действ хранится зде	зие есь	
Ф Триггеры Добавить триггер < 1							ថ	🖾 Нотификации <							Ф Действия						
+	Ð		H 00000				Ó	ø		Только выбранные т	риггеры				0 8		только выбран	ные ноты	ифика		0 0
			Название	Дни	Частота	Тип триггера	Статуо			Название триггера	Тип	д	στα	Заметка			Тип		Дата	Статуо	
			Q Фильтр		~	~	~			Q Фильтр		~		Q. Фильтр				~	0		~
	Ø	Ø	топ абонент	Пн,Вт,Ср,Чт	г, 1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотифика	ация 3	0.06.2023 17:31:43	maxIf(traffic,	isNaN 🖞		notification		30.06.2023 17:36:23	Завершено	Û
	Ø		Тест	Чт	1 минута	Пользовательский	Готов	٥		Топ абонентов	🛆 Нотифика	ация 2	9.06.2023 18:19:03	maxIf(traffic,	isNaN 🖞		telegram		29.06.2023 18:24:04	Завершено	Ċ
	Ø		Дельта паке	пт	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотифика	ация 2	9.06.2023 18:00:43	maxIf(traffic,	isNaN 🗊		С	писо	к действий п	о нотифик	сациям
	Ø	2	test2	Пн	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотифика	ация 2	9.06.2023 17:41:07	maxIf(traffic,	isNaN 🖞						
	Φ		test	Пн	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотифика	ация 2	9.06.2023 17:22:03	maxIf(traffic,	isNaN 🗊						
						Список	триггер	ров			Спис	ок но	тификаций	по тригі	ерам						
**	<		1 5 55			На странице	100	~	~~	< 1 2 3	3 4 5		На стр	ранице 10	o ~	~~	< 1		Ho	странице	100 ~

В данном разделе отображены три секции:

- Список триггеров.
- Список нотификаций по триггерам.
- Список действий, выполненных триггерами в результате возникших нотификаций.

Типы триггеров:

- Системные. Задаются вендором и их можно только включить/выключить.
- Пользовательские. Задаются пользователем и могут свободно настраиваться.

Подробное описание настройки триггера смотрите в разделе Создание и настройка триггеров.