

# Содержание

<b>Обнаружение SSH брутфорс атак с использованием триггеров в QoE</b>	3
<i>Системный триггер на обнаружение SSH брутфорс атак</i>	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
- HTTP действие
- отправка email

Необходимые опции СКАТ DPI:

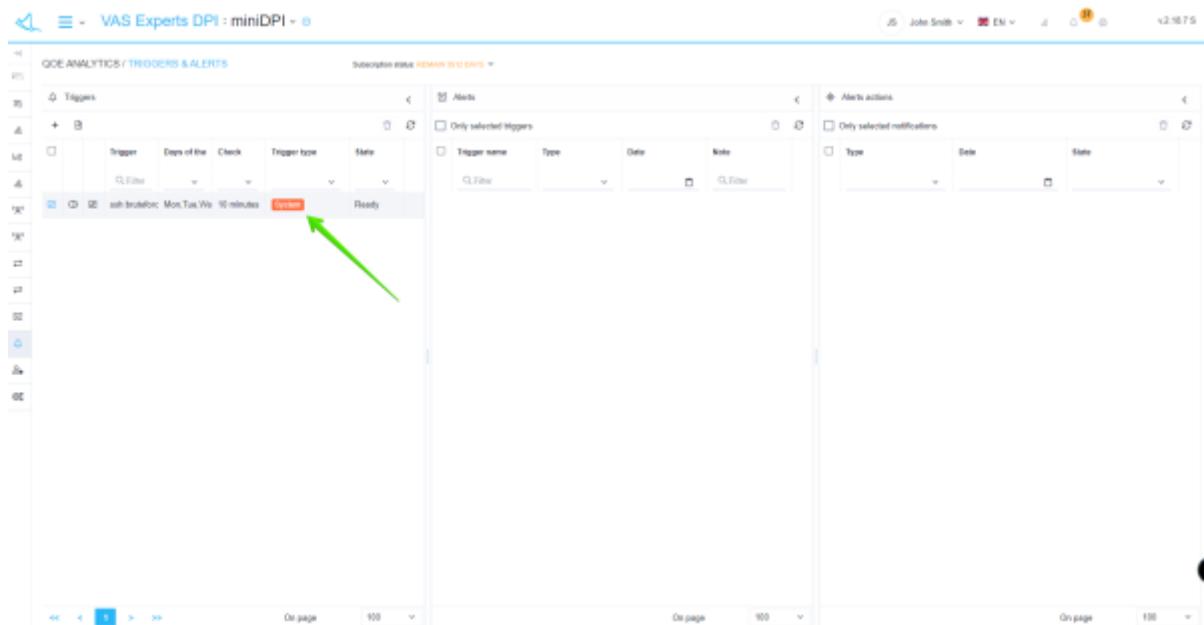
- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

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).



The screenshot shows the 'QOE ANALYTICS / TRIGGERS & ALERTS' page. The 'Triggers' section is active, displaying a table with columns: Trigger, Days of the week, Check, Trigger type, and Name. A single row is visible, representing the 'ssh-bruteforce' trigger, which is set to run 'Mon, Tue, Wed' at '10 minutes' and is currently in a 'Ready' state. The 'System' status indicator is highlighted with a green arrow. The 'Alerts' and 'Alerts actions' sections are also visible but empty.

### Общая информация триггера

Общее			
Название триггера *	ssh bruteforce	Важность	Высокая важность
Триггер	<input checked="" type="radio"/> Выключен		
Дни недели *	Пн, Вт, Ср, Чт, Пт, Сб, Вс	Частота проверки *	10 минут
		Количество срабатываний	
		0	
Дата начала	01.12.2024	Дата окончания	31.12.2099
Время начала	00:00	Время окончания	23:55

- 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

Запросы							
+		Название		Отчет		Период с	Период по
<input checked="" type="checkbox"/> Вкл.	A	SSH брутфорс		▼	сейчас - 30 минут	сейчас - 20 минут	

Для данного триггера 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

Условия							
+							
<input checked="" type="checkbox"/> Вкл.	Связь	И	Название	avg	Комбинатор	Серия	Оператор
						Время жизни <=	20
<input checked="" type="checkbox"/> Вкл.			A	max		Сессий на ас >=	1500

- Добавить "+" 2 поля

- Связка – И
- Функция – avg
- Серия в 1 поле – время жизни сессии к абоненту  $\leq 20$ (мс)
- Серия во 2 поле – количество сессий на абонента  $\geq 1500$



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 отсутствии 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

Alerts				
<input type="checkbox"/> Only selected triggers				
Trigger name	Type	Date	Note	
ssh bruteforce	<span style="color: red;">⚠ Alerting</span>	20.05.2021 14:45:24	count(sess_subscrib	<span style="color: red;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:31:43		<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:13:24	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:12:03	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:10:42	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:09:24	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:08:03	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:06:42	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:05:23	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:04:04	count(sess_subscrib	<span style="color: green;">X</span>
ssh bruteforce	<span style="color: green;">OK</span>	20.05.2021 14:02:43	count(sess_subscrib	<span style="color: green;">X</span>

Alerts actions				
<input type="checkbox"/> Only selected notifications				
Type	Date	Note	State	
notification	20.05.2021 14:45:44		<span style="color: green;">Complete</span>	<span style="color: green;">X</span>

Получить ссылку на отчет можно через меню нотификаций

Notifications

Triggers 20.05.2021 02:45  
ssh bruteforce (1)

Id: 1 Details

Subscribers synchronization Mark as read

Hardware: miniDPI Delete

Success >

Subscribers synchronization 20.05.2021 02:44

Hardware: centos8 >

Subscribers synchronization 20.05.2021 02:42

Hardware: miniDPI >

Subscribers synchronization 20.05.2021 02:42

Hardware: centos8 >

Subscribers synchronization 20.05.2021 02:40

Hardware: miniDPI >

Subscribers synchronization 20.05.2021 02:40

Hardware: centos8 >

<< < 1 2 3 4 5 > >>

Выбрать нотификацию Выбрать — "Детали"

Notifications

Triggers

Status	New
Notification date	20.05.2021 02:45
Notify type	⚠ Warning

Notification content

ssh bruteforce (1)

Id: 1

Trigger: ssh bruteforce

Status: firing

Severity: hight

Queries:

A: QoETableFullnetflowRawSshBruteForceWidget

Reasons for the occurrence of notification:

count(sess\_subscribers) > 0 is true in query A

Links to reports:

A: [https://localhost/#QoEAnyReport/report\\_id=896Fj5ZLpG8WenE](https://localhost/#QoEAnyReport/report_id=896Fj5ZLpG8WenE)

---

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