

Содержание

Обнаружение SSH брутфорс атак с использованием триггеров в QoE	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 SKAT 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

Общее			
Название триггера *	Важность	Триггер	<input type="checkbox"/> Выключен
ssh bruteforce	Высокая важность		
Дни недели *	Частота проверки *	Количество срабатываний	
Пн, Вт, Ср, Чт, Пт, Сб, Вс	10 минут	0	
Дата начала	Дата окончания	Время начала	Время окончания
01.12.2024	31.12.2099	00:00	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: Сырой полный нетфлоу → Таблицы → Обнаружение атак → SSH брутфорс;
- Период с: сейчас - 30 минут
- Период по: сейчас - 20 минут

Условия

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

- Добавить "+" 2 поля
- Связка - И
- Функция - avg для 1 поля, max для 2 поля
- Серия в 1 поле - Время жизни сессии к абоненту, мс <= 20
- Серия во 2 поле - 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

Обработка ошибок	
Если нет данных *	Если ошибка выполнения или тайм-аут *
Нет данных	Сохранить последнее состояние

- В поле "Если нет данных" — Нет данных
- В поле "Если ошибка выполнения или тайм-аут" — 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

Действия

- E-mail

Кому Вкл.

your@email.com

Тема

Trigger fired: {trigger.name}

Сообщение 📎 </>

B / I / U / / Font Size... / Font Family... / Font Format... /

Id: {trigger.id}

Trigger: {trigger.name}

Status: {trigger.state}

Severity: {trigger.severity}

Queries:

{trigger.queries}

- 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

Действия

E-mail × Нотификация ×

Заголовок нотификации
{trigger.name} Вкл.

Подзаголовок нотификации Тип нотификации
{trigger.id} Предупреждение

Сообщение

В / Font Size... Font Family... Font Format...

Ид: {trigger.id}
 Триггер: {trigger.name}
 Статус: {trigger.state}
 Важность: {trigger.severity}

Запросы:
{trigger.queries}

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

Alerts					Alerts actions			
Only selected triggers					Only selected notifications			
<input type="checkbox"/>	Trigger name	Type	Date	Note	<input type="checkbox"/>	Type	Date	State
<input type="checkbox"/>	ssh bruteforce	Alerting	20.05.2021 14:45:24	count(sess_subscrib	<input checked="" type="checkbox"/>	notification	20.05.2021 14:45:44	Complete
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:31:43		<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:13:24	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:12:03	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:10:42	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:09:24	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:08:03	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:06:42	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:05:23	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:04:04	count(sess_subscrib	<input type="checkbox"/>			
<input type="checkbox"/>	ssh bruteforce	OK	20.05.2021 14:02:43	count(sess_subscrib	<input type="checkbox"/>			

Получить ссылку на отчет можно через меню нотификаций

Notifications ×

📖 🗑️

🔔 **Triggers** 20.05.2021 02:45
ssh bruteforce (1)
Id: 1

✅ **Subscribers synchronization**
Hardware: miniDPI
Success ➤

✅ **Subscribers synchronization** 20.05.2021 02:44
Hardware: centos8
Success ➤

✅ **Subscribers synchronization** 20.05.2021 02:42
Hardware: miniDPI
Success ➤

✅ **Subscribers synchronization** 20.05.2021 02:42
Hardware: centos8
Success ➤

✅ **Subscribers synchronization** 20.05.2021 02:40
Hardware: miniDPI
Success ➤

✅ **Subscribers synchronization** 20.05.2021 02:40
Hardware: centos8
Success ➤

⏪ ⏴ 1 2 3 4 5 ⏵ ⏩

Details
Mark as read
Delete

Выбрать нотификацию Выбрать — "Детали"

← 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

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

HTTP действие


Действия

E-mail × Нотификация × Http ×

Метод: POST
Урл: https://your_redmine_host/issues.xml?key=your_redmine_api_key Вкл.

Заголовки		Тело
+		
Имя	Значение	<pre><?xml version="1.0"?> <issue> <project_id>1</project_id> <subject>Trigger fired: {trigger.name}</subject> <priority_id>1</priority_id> <description>Id: {trigger.id}\nTrigger: {trigger.name}\nStatus: {trigger.state}\nSeverity: {trigger.severity}\nQueries: {trigger.queries}\nReasons for the occurrence of notification: {trigger.notification.notes}\nLinks to reports:\n{trigger.report.link}\n\nLinks to files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report .xlsx}\n\n{trigger.report.xlsx}</description> </issue></pre>

json Шаблон по умолчанию
xml Шаблон по умолчанию

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