

Содержание

Обнаружение SSH brutфорс атак с использованием триггеров в QoE 3

Системный триггер на обнаружение SSH brutфорс атак 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	
ssh bruteforce	Высокая важность		Выключен
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
your@email.com

Тема
Trigger fired: {trigger.name}

Сообщение

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

Notifications

ssh bruteforce (1)

Id: 1

Subscribers synchronization

Hardware: miniDPI

Success

Subscribers synchronization

Hardware: centos8

Success

Subscribers synchronization

Hardware: miniDPI

Success

Subscribers synchronization

Hardware: centos8

Success

Subscribers synchronization

Hardware: miniDPI

Success

Subscribers synchronization

Hardware: centos8

Success

Details

Mark as read

Delete

<<

<

1

2

3

4

5

>

>>

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

Урл

POST

▼

https://your_redmine_host/issues.xml?key=your_redmine_api_key

Вкл.

Заголовки

<

Тело

>

+

Имя

Значение

Content-Type

application/xml

🗑

json Шаблон по умолчанию

xml Шаблон по умолчанию

<?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>

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