

Содержание

Обнаружение SSH bruteforce атак с использованием триггеров в QoE	3
<i>Системный триггер на обнаружение SSH bruteforce 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:

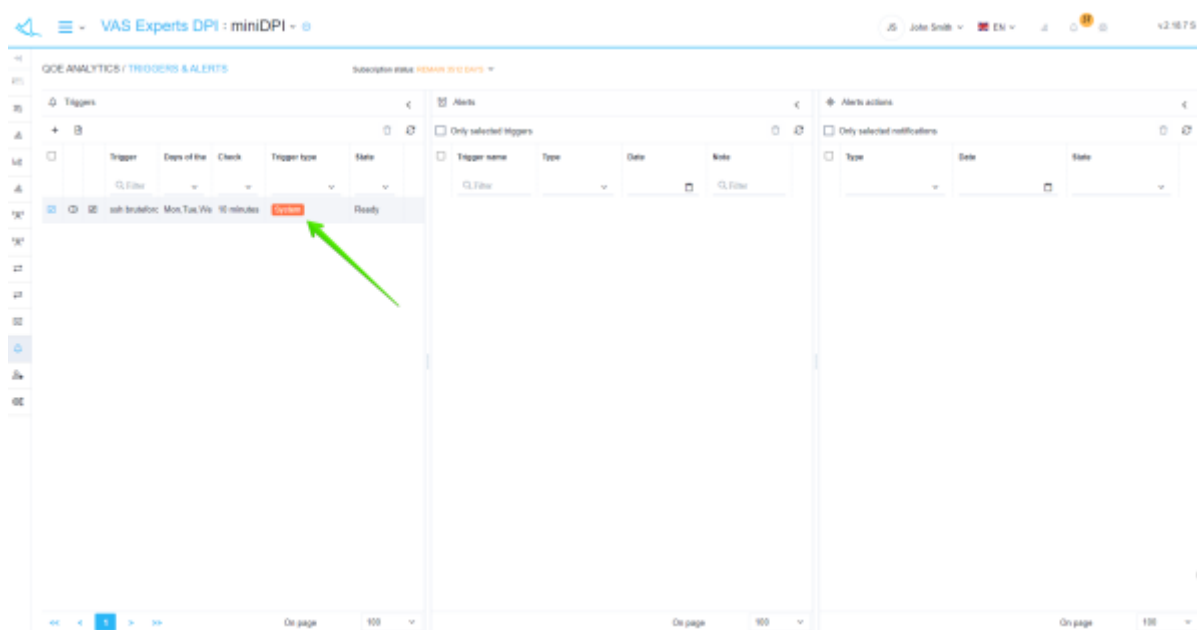
- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

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

Системный триггер на обнаружение SSH брутфорс атак

Триггер на обнаружение SSH брутфорс атак (Имя - "ssh brute force") является системным и доступен в разделе "QOE Аналитика"- "Триггеры и нотификации" (по-умолчанию выключен).



Общая информация триггера

Common

Trigger name * ssh bruteforce Severity Hight Trigger Disabled

Days of the week * Mon, Tue, Wed, Thu, Fri, Sat, Sun Check frequency * 10 minutes Number of positives 0

Start date 10/01/2019 End date 12/31/2099 Start time 00:00 End time 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

Queries						
+						
	Query name	Report		Period from	Period to	
☒ On	A	Ssh bruteforce		now - 30 minutes	now - 20 minutes	

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

Conditions							
+							
	Bind	Query name	Function	Combinator	Series	Operator	Value
☒ On	AND	A	avg		Session lifetime	<=	20
☒ On	AND	A	max		Sessions per su	>=	1500

- Добавить "+" 2 поля

- Связка - И
- Функция - avg
- Серия в 1 поле - время жизни сессии к абоненту ≤ 20 (мс)
- Серия во 2 поле - количество 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

No data & error handling	
If no data *	If execution error or timeout *
No data	Keep last state

- 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

Е-mail действие

Actions

Notification x E-mail x

Send to
Your@email.com

Subject
Trigger fired: {trigger.name}

Message

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

Запросы:
{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

Actions

Notification x E-mail x

Notification title
{trigger.name}

Notification subtitle
{trigger.id}

Notification type
Warning

Message

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			
☐	Trigger name	Type	Date	Note	☐	Type	Date	State
☐	ssh bruteforce	Alerting	20.05.2021 14:45:24	count(sess_subscrib	☒	notification	20.05.2021 14:45:44	Complete
☐	ssh bruteforce	Ok	20.05.2021 14:31:43					
☐	ssh bruteforce	Ok	20.05.2021 14:13:24	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:12:03	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:10:42	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:09:24	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:08:03	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:06:42	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:05:23	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:04:04	count(sess_subscrib				
☐	ssh bruteforce	Ok	20.05.2021 14:02:43	count(sess_subscrib				

Получить ссылку на отчет можно через меню нотификаций

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

Actions

Notification

E-mail

Http

Method

POST

Url

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

On

Headers

Body

+

Name

Value

Content-Type

application/xml

<?xml version="1.0"?>

<issue>

<project_id>1</project_id>

<subject>Сработал триггер: {trigger.name}</subject>

<priority_id>1</priority_id>

<description>Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

REDMINE JSON

REDMINE XML

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