

Запуск скрипта коррелятором

Интерпретатор скрипта должен поддерживаться ОС на которой находится скрипт.

Для того чтобы коррелятор мог запускать скрипты. Зайти по ssh на сервер где находится служба коррелятора и поместите скрипт (можно сделать с помощью WinSCP или любым другим инструментом) в следующую папку коррелятора:

```
/opt/kaspersky/kuma/correlator/<id>/scripts/
```

<id> - идентификатор коррелятора, можно найти в веб-интерфейсе (подробнее как это сделать [ссылка](#))

Назначьте пользователя kuma владельцем файла и дайте файлу права на выполнение:

```
chown kuma:kuma /opt/kaspersky/kuma/correlator/<id>/scripts/my_script.sh  
chmod +x /opt/kaspersky/kuma/correlator/<id>/scripts/my_script.sh
```

■
В группирующем поле **правила корреляции** должны находиться целевые поля, которые используются в правилах реагирования, в нашем примере это **DestinationAddress**.

Общие

Селекторы

Действия

*Название

EICAR-Test-File

*Тенант

Main

*Тип

simple

*Группирующие поля

+ Добавить поле

DeviceCustomString1

DestinationHostName

DestinationAddress

✖ Сбросить

Частота срабатываний

0

?

Уровень важности

Низкий

Описание

В правиле реагирования рекомендуется добавить в условие (если необходимо) правило корреляции, на основе которого реагирование будет срабатывать:

*Название	<input type="text" value="[KEDR Response] Host Isolation"/>
*Тенант	<input type="text" value="Main"/>
*Тип	<input type="text" value="script"/>
Время ожидания	<input type="text" value="60"/> <small>Время ожидания в секундах</small>
*Название скрипта	<input type="text" value="kedr_response_universal.sh"/>
Аргументы скрипта	<input type="text" value="-kedr_isolate {{.DestinationAddress}} 180"/>
Рабочие процессы	<input type="text" value="0"/>
Описание	<input type="text" value="-kedr_isolate <KEDR_IP_ADDRESS> <HOURS>
-- isolating KEDR_IP_ADDRESS host from
network for <HOURS> hours"/>
Фильтр	<input type="text" value="Создать"/>
	<input type="checkbox"/> Сохранить фильтр
Условия	<div style="border: 2px solid red; padding: 5px;">И + Добавить условие + Добавить группу + Добавить фильтр Если поле события CorrelationRuleName = константа EICAR-Test-File x</div>

После внесения изменений в ресурсах (правила корреляции или реагирования) необходимо обновить параметры коррелятора в активных сервисах

Revision #2

Created 4 December 2023 11:03:13 by Boris RZR

Updated 7 July 2024 08:07:15 by Koala