

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	<input type="text" value="EICAR-Test-File"/>	
*Тенант	<div>Main</div>	
*Тип	<div>simple</div>	
*Группирующие поля	<div><div>+ Добавить поле</div><div>DeviceCustomString1</div><div>DestinationHostName</div><div>DestinationAddress</div><div>✕ Сбросить</div></div>	
Частота срабатываний	<div>0</div>	
Уровень важности	<div>Низкий</div>	
Описание	<div></div>	

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	<div>Main</div>
*Тип	<div>script</div>
Время ожидания	<div>60</div> <div>Время ожидания в секундах</div>
*Название скрипта	<input type="text" value="kedr_response_universal.sh"/>
Аргументы скрипта	<div><div>-kedr_isolate {{.DestinationAddress}} 180</div></div>
Рабочие процессы	<div>0</div>
Описание	<div><div>-kedr_isolate <KEDR_IP_ADDRESS> <HOURS> -- isolating KEDR_IP_ADDRESS host from network for <HOURS> hours</div></div>
Фильтр	<div>Создать</div>
	<input type="checkbox"/> Сохранить фильтр
Условия	<div><div>И</div><div>+ Добавить условие</div><div>+ Добавить группу</div><div>+ Добавить фильтр</div><div>Если поле события CorrelationRuleName = константа EICAR-Test-File</div></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