

Реагирование на KICS Networks с помощью скрипта

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

В связи с ограничениями коробочного реагирования с KICS Networks (возможность выбора полей только *AssetID) в KUMA 2.x версиях был разработан скрипт, который может использовать произвольное поле, где находится UUID актива в KUMA.

Скрипт реагирования можно загрузить из [Пресейл-Пак контент](#) из соответствующей папки.

Для попадания событий изменения категорий предварительно нужно **настроить аудит активов**, подробнее можно посмотреть [тут](#). Вот так выглядит аудита активов (при ручном или любом другом типе добавления в категорию):

TenantName	Main
Timestamp	05.12.2023 10:35:22:248
Name	3650
EndTime	05.12.2023 10:35:22:248
DeviceAction	asset added to category
DeviceEventCategory	Audit assets
DeviceExternalID	8d9f26da-41c9-4593-9087-32ac4585e5c4
DeviceHostName	3650
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
SourceHostName	10.68.85.138
DeviceCustomString1	Main/Categorized assets/KICS-NET/unwanted
DeviceCustomString1Label	category
DeviceCustomString2	manual
DeviceCustomString2Label	categorization type
EventOutcome	succeeded
Priority	Низкий
Type	Base

Далее необходимо создать правило корреляции, которое будет менять **статус KICS for Networks** на неразрешенное при добавлении в категорию, например *Main/Categorized assets/KICS-NET/unwanted*. Оно будет выглядеть так (необходимо пробросить поле *DeviceExternalID* в группирующие поля):

Общие

Селекторы

Действия

*Название

KICS_to_Unwanted

*Тенант

Общий

*Тип

simple

*Наследственные поля

+ Добавить поле

DeviceAction

DeviceCustomString1

DeviceExternalID

Частота срабатываний

0

Уровень важности

Низкий

Описание

Общие

Селекторы

Действия

Селектор №1

Параметры

Локальные переменные

*Филتر

Создать

Сохранить филтр

*Условия

И

+ Добавить условие

+ Добавить группу

+ Добавить филтр

Если

поле события

DeviceCustomString1

=

константа

Main/Categorized assets/KICS-N

И

Если

поле события

DeviceAction

=

константа

asset added to categor

Общие

Селекторы

Действия

Действия

На каждом событии

Отправить событие на дальнейшую обработку

Отправить событие снова в коррелятор

Не создавать алерт

Обогащение

+ Добавить обогащение

Обновление активных листов

+ Добавить действие с активным листом

Изменение категорий

+ Добавить категоризацию


Пример сработки правила корреляции:

Информация о корреляционном событии



TenantName	Main
Timestamp	05.12.2023 10:35:24:719
Name	KICS_to_Unwanted
StartTime	05.12.2023 10:35:22:248
EndTime	05.12.2023 10:35:22:248
DeviceAction	asset added to category
DeviceExternalID	8d9f26da-41c9-4593-9087-32ac4585e5c4
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
DeviceCustomString1	Main/Categorized assets/KICS-NET/unwanted
CorrelationRule	KICS to Unwanted
Service	[Example] Correlator
BaseEventCount	1

Далее нужно создать (либо загрузить из Пресейл-Пака) правило реагирования которое будет запускать скрипт из Пресейл-Пака, правило должно выглядеть следующим образом:

*Название	<input type="text" value="[KICS Response] Asset to Unwanted"/>
*Тенант	<div>Общий</div>
*Тип	<div>Запуск скрипта</div> 
Время ожидания	<div>0</div> <div>Время ожидания в секундах</div>
*Название скрипта	<input type="text" value="kics_response.sh"/>
Аргументы скрипта	<div>{{.DeviceExternalID}}</div>

Скрипт необходимо загрузить и выгрузить на коррелятор и выполнить действия по **этой статье**.

В результате правило корреляции и реагирование нужно добавить в коррелятор и обновить его параметры. Таким образом получим, что при перемещении актива в определенную категорию (например Активным способом по подсети), автоматом эти активы будут помечаться недоверенными.

Revision #3

Created 4 December 2023 10:37:39 by Boris RZR

Updated 19 July 2024 14:37:44 by Koala