Автоматическое добавление активов

Описание

Данный скрипт и набор ресурсов позволяют автоматически на основании информации из событий (ip-адреса, доменные имена) создавать активы в KUMA

> Данный скрипт рекомендуется использовать только в тестовой или демонстрационной инсталляции

Требования

python 3.6+

- urllib
- argparse
- json
- requests
- os

KUMA 3.0.2

Подготовка скрипта

1. Поместите файлы `asset-import.py`, `kumaPublicApiV1.py`, `params.json` на сервер коррелятора в папку scripts: /opt/kaspersky/kuma/correlator/`id`/scripts

`id` коррелятора можно получить из веб-интерфейса KUMA: Ресурсы -> Активные сервисы -> Выбрать галочкой коррелятор и в верхнем меню `Копировать идентификатор сервиса`. Идентификатор будет скопирован в буфер обмена.

2. Внесите изменения в файл `params.json`:

- kumaAddress - укажите ip-адрес сервера ядра KUMA
- kumaAPIPort - укажите API-порт ядра KUMA (значение по умолчанию `7223`, если сомневаетесь - оставьте без изменений)
- kumaToken - токен для работы с API с правами `POST /assets/import`

3. Измените владельца файлов на kuma:

```
chown kuma:kuma asset-import.py kumaPublicApiV1.py params.json
```

4. Разрешите запуск файла `asset-import.py`:

```
chmod +x asset-import.py
```

Подготовка KUMA

1. Импортируйте все ресурсы из файла `auto_asset_add` (Пароль импорта: Qwerty123!)
2. Если нужно, внесите изменения в фильтры `org address filter` и `org hostname filter`, указав домены и подсети вашей организации, по ним отбираются активы из событий для импорта.
3. Привяжите все правила корреляции `Auto import asset info (src/dst/dvc)` к коррелятору
4. Привяжите правило реагирования `Auto asset import`
5. Обновите параметры сервиса коррелятора

Результат

В результате проделанных манипуляций в KUMA будут создаваться активы на основании информации, получаемой из событий.

Файлы

Все ресурсы доступны по ссылке: https://box.kaspersky.com/d/1eb25f174a3e44e2a1be/

Revision #2
Created 15 February 2024 13:05:06 by Koala
Updated 19 July 2024 14:37:44 by Koala