

?????? ?????????????? ?? ????????? RedCheck

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

???????? ?????????????????? ?? ?????????? RedCheck

В KUMA можно импортировать сведения об активах из отчетов о результатах сканирования сетевых устройств с помощью RedCheck, системы контроля защищенности и соответствия стандартам. Импорт происходит через API с помощью утилиты `redcheck-tool.py`. Импортированные активы отображаются в веб-интерфейсе KUMA в разделе Активы. При необходимости вы можете редактировать параметры активов.

Импорт поддерживается из RedCheck 2.6.8 и выше

Поддерживается импорт информации о хостах только под управлением ОС Windows

Для работы утилиты требуется python версии 3.6 или выше, а также библиотеки: csv, re, json, requests, argparse, sys

Чтобы импортировать данные об активах из отчета RedCheck:

1. Сформируйте в RedCheck отчет сканирования сетевых активов в формате CSV и скопируйте файл отчета на сервер со скриптом. Подробнее о задачах на сканирование и форматах выходных файлов см. в документации RedCheck.

Импорт доступен из "Простых" отчетов "**Уязвимости**" и "**Инвентаризация**" сгруппированных по хостам в формате CSV. Подробнее на сайте RedCheck:
<https://docs.redcheck.ru/articles/#!redcheck-user-269/reports>

2. Создайте токен для доступа к KUMA REST API.

Требования к учетным записям, для которых генерируется API-токен:

- Роль Администратора или Аналитика.
- Доступ к тенанту, в который будут импортированы активы.
- Настроены права на использование API-запросов GET /assets, GET /tenants, POST /assets/import

3. Скопируйте утилиту redcheck-tool.py на сервер ядра KUMA и сделайте файл утилиты исполняемым с помощью команды:

```
chmod +x <путь до файла redcheck-tool.py>
```

4. Запустите утилиту redcheck-tool.py:

```
python3 redcheck-tool.py --kuma-rest <адрес и порт сервера KUMA REST API> --token <API-токен>
--tenant <название тенанта, куда будут помещены активы> --vuln-report <Полный путь к файлу
отчета "Уязвимости"> --inventory-report <Полный путь к файлу с отчета "Инвентаризация">
```

Пример:

```
python3 --kuma-rest example.kuma.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant
Main --vuln-report /home/user/vuln.csv --inventory-report /home/user/inventory.csv
```

Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения расширенного отчета о полученных активах `-v`. Подробное описание доступных флагов и команд приведено в таблице Флаги и команды утилиты redcheck-tool.py. Также для просмотра информации о доступных флагах и командах вы можете использовать команду `--help`.

Информация об активах будет импортирована из отчета RedCheck в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

Пример:

```
inventory has been imported for 2 host(s)
software has been imported for 5 host(s)
vulnerabilities has been imported for 4 host(s)
```

Пример расширенного вывода информации об импорте:

```
[inventory import]           Host: localhost           Code: 200  Response: {'insertedIDs': {'0':
'52ca11c6-a0e6-4dfd-8ef9-bf58189340f8'}, 'updatedCount': 0, 'errors': []}
[inventory import]           Host: 10.0.0.2            Code: 200  Response: {'insertedIDs': {'0':
'1583e552-5137-4164-92e0-01e60fb6edb0'}, 'updatedCount': 0, 'errors': []}
[software import][error]     Host: localhost          Skipped asset with FQDN localhost or IP
```

```

127.0.0.1
[software import]           Host: 10.0.0.2           Code: 200  Response: {'insertedIDs': {},
'updatedCount': 1, 'errors': []}
[vulnerabilities import]   Host: 10.0.0.2           Code: 200  Response: {'insertedIDs': {},
'updatedCount': 1, 'errors': []}
[vulnerabilities import]   Host: 10.0.0.1           Code: 200  Response: {'insertedIDs': {'0':
'0628f683-c20c-4107-abf3-d837b3dbbf01'}, 'updatedCount': 0, 'errors': []}
[vulnerabilities import]   Host: localhost          Code: 200  Response: {'insertedIDs': {},
'updatedCount': 1, 'errors': []}
[vulnerabilities import]   Host: 10.0.0.3           Code: 200  Response: {'insertedIDs': {'0':
'ed01e0a8-dcb0-4609-ab2b-91e50092555d'}, 'updatedCount': 0, 'errors': []}
inventory has been imported for 2 host(s)
software has been imported for 1 host(s)
vulnerabilities has been imported for 4 host(s)

```

Поведение утилиты при импорте активов:

- Данные импортированных в KUMA через API активов перезаписываются, а сведения об их устаревших уязвимостях удаляются.
- Активы с недействительными данными пропускаются.

????? ? ????????? ???????? redcheck-tool.py

Флаги и команды	Обязательный	Описание
--kuma-rest <адрес и порт сервера ядра KUMA>	Да	По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
--token <токен>	Да	Значение в параметре должно содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Администратора или Аналитика.
--tenant <название тенанта>	Да	Название тенанта KUMA, в который будут импортированы активы из отчета RedCheck
--vuln-report <полный путь к файлу отчета "Уязвимости">	Да	Файл должен содержать отчет "Уязвимости" в формате CSV
--inventory-report <полный путь к файлу отчета "Инвентаризация">	Нет	Файл должен содержать отчет "Инвентаризация" в формате CSV
-v	Нет	Выведение расширенной информации об импорте активов

?????????? ???????

Сообщение об ошибке	Описание
Tenant %w not found	Имя тенанта не найдено
Tenant search error: Unexpected status Code: %d	При поиске тенанта был получен неожиданный код ответа HTTP
Asset search error: Unexpected status Code: %d	При поиске актива был получен неожиданный код ответа HTTP
[%w import][error] Host: %w Skipped asset with FQDN localhost or IP 127.0.0.1	При импорте информации инвентаризации/уязвимостей был пропущен хост с fqdn=localhost или ip=127.0.0.1

Revision #6

Created 2023-08-22 10:47:27 UTC by Koala

Updated 2025-02-03 07:59:53 UTC by Koala