Импорт информации об активах RedCheck

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

Импорт информации об активах RedCheck

? KUMA ????? ????????????? ???????? ?? ??????? ?? ??????? ? ??????????? ???????????? ??????? ????????? ? ??????? RedCheck, ??????? ???????? ???????????? ? ???????????? ?????????. ?????? ????????? ????? API ? ??????? ??????? `redcheck-tool.py`. ?????????????? ?????? ???????????? ? ???-?????????? KUMA ? ??????? ??????. ??? ????????????? ?? ?????? ????????????? ????????? ???????.

?????? ????????????? ?? RedCheck 2.6.8 ? ????

????????????? ?????? ????????? ? ?????? ?????? ??? ??????????? ?? Windows

??? ?????? ??????? ????????? python ????? 3.6 ??? ????, ? ????? ??????????: csv, re, json, requests, argparse, sys

????? ????????????? ?????? ?? ??????? ?? ?????? RedCheck:

1. ??????????? ? RedCheck ????? ???????????? ??????? ??????? ? ??????? CSV ? ?????????? ???? ?????? ?? ?????? ?? ????????. ????????? ? ??????? ?? ???????????? ? ???????? ???????? ?????? ??. ? ???????????? RedCheck.

?????? ???????? ?? "???????" ??????? "**Уязвимости**" ? "**Инвентаризация**" ?????????????? ?? ?????? ? ??????? CSV. ????????? ?? ????? RedCheck: https://docs.redcheck.ru/articles/#!redcheck-user-269/reports

2. ???????? ????? ??? ??????? ? KUMA REST API.

?????????? ? ??????? ???????, ??? ??????? ???????????? API-?????:

- ???? ????????????? ??? ?????????.
- ?????? ? ???????, ? ??????? ????? ????????????? ??????.

- ????????? ????? ?? ????????????? API-???????? GET /assets, GET /tenants, POST /assets/import

3. ?????????? ??????? redcheck-tool.py ?? ?????? ???? KUMA ? ???????? ???? ??????? ??????????? ? ??????? ???????:

```
chmod +x <???? ?? ????? redcheck-tool.py>
```

4. ????????? ??????? redcheck-tool.py:

```
python3 redcheck-tool.py --kuma-rest <????? ? ???? ??????? KUMA REST API> --token <API-?????> --tenant <
???????? ???????, ???? ????? ???????? ??????> --vuln-report <?????? ???? ? ????? ?????? "??????????"> --
inventory-report <?????? ???? ? ????? ? ?????? "??????????????">
```

??????:

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

?? ?????? ???????????? ?????????????? ????? ? ??????? ??? ???????. ????????, ??????? ??? ??????????? ???????????? ?????? ? ?????????? ??????? `-v`. ????????? ???????? ????????? ?????? ? ?????? ????????? ? ??????? ????? ? ??????? ??????? redcheck-tool.py. ????? ??? ????????? ?????????? ? ????????? ?????? ? ???????? ?? ?????? ???????????? ??????? `--help`.

?????????? ?? ??????? ????? ????????????? ?? ?????? RedCheck ? KUMA. ? ??????? ???????????? ???????? ? ?????????? ????? ? ??????????? ???????.

??????:

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

?????? ???????????? ?????? ?????????? ?? ???????:

```
[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)
```

????????? ??????? ??? ??????? ???????:

- ?????? ?????????????? ? KUMA ????? API ??????? ??????????????, ? ???????? ?? ?? ?????????? ?????????? ?????????.
- ?????? ? ???????????????? ??????? ???????????.

Флаги и команды утилиты redcheck-tool.py

Флаги и команды	Обязательный	Описание
--kuma-rest <????? ? ???? ??????? ???? KUMA>	??	?? ????????? ??? ????????? ?? API ???????????? ???? 7223. ??? ????????????? ??? ????? ????????.
--token <?????>	??	???????? ? ????????? ?????? ????????? ?????? ?????. ??????? ??????, ??? ??????? ???????????? API-?????, ?????? ???? ????????? ???? ????????????? ??? ????????? .
--tenant <???????? ???????>	??	???????? ??????? KUMA, ? ??????? ????? ????????????? ?????? ?? ?????? RedCheck
--vuln-report <?????? ???? ? ????? ?????? "??????????">	??	???? ?????? ????????? ????? " ??????????" ? ??????? CSV
--inventory-report <?????? ???? ? ????? ?????? " ??????????????">	???	???? ?????? ????????? ????? " ????????????????" ? ??????? CSV
-v	???	????????? ??????????? ?????????? ?? ??????? ???????

Возможные ошибки

Сообщение об ошибке	Описание
Tenant %w not found	??? ??????? ?? ???????

Tenant search error: Unexpected status Code: %d	??? ?????? ??????? ??? ??????? ??????????? ??? ?????? HTTP
Asset search error: Unexpected status Code: %d	??? ?????? ?????? ??? ??????? ??????????? ??? ?????? HTTP
[%w import][error] Host: %w Skipped asset with FQDN localhost or IP 127.0.0.1	??? ??????? ?????????? ?????????????? ??????????? ??? ???????? ???? ? fqdn=localhost ??? 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