

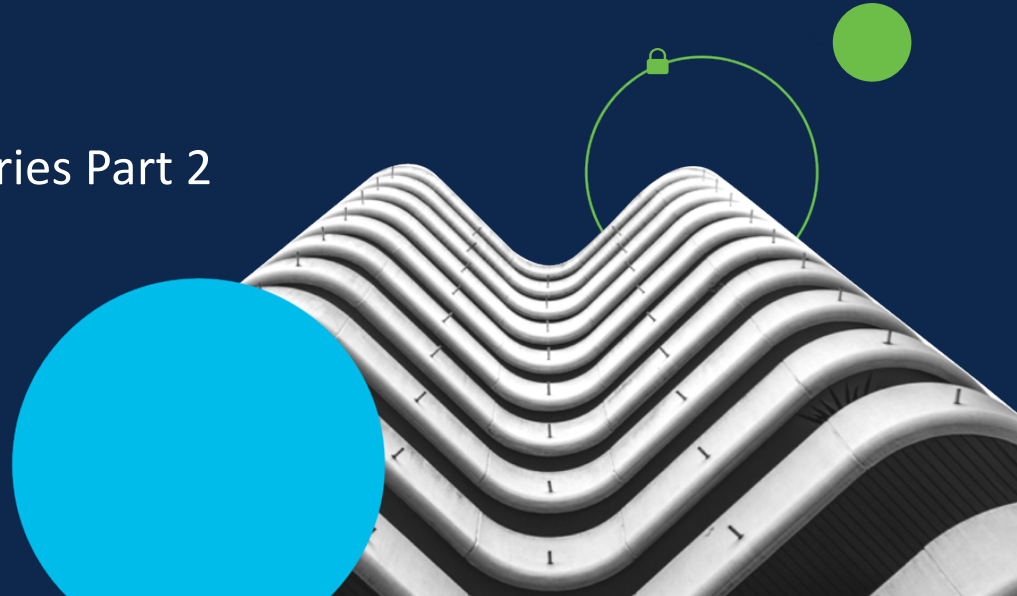
Power User Webinar



Getting dirty with Kenna's Super Clean API

API Series Part 2

01/21/2021



Kenna Security is
now part of Cisco.



Presenters:



Murillo Perrotti

Customer Success
Engineer



Lewis Onyejiaka

Customer Success
Engineer



Katie Kolon

Customer Success
Operations Manager

Agenda

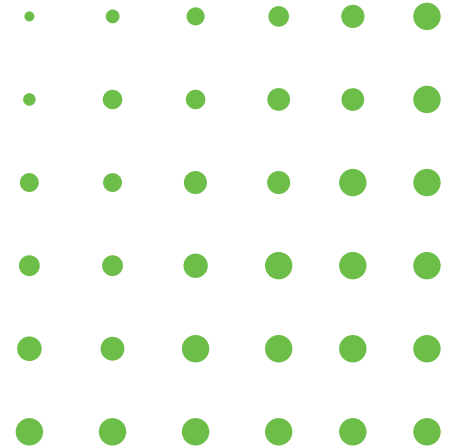


- ▶ Kenna's new API documentation
- ▶ Overview of some of our favorite endpoints
- ▶ From endpoints to scripts
- ▶ Kenna Public Script Repository
- ▶ Demos with some interesting scripts
- ▶ Q&A

To be
fair ...
we did
say it



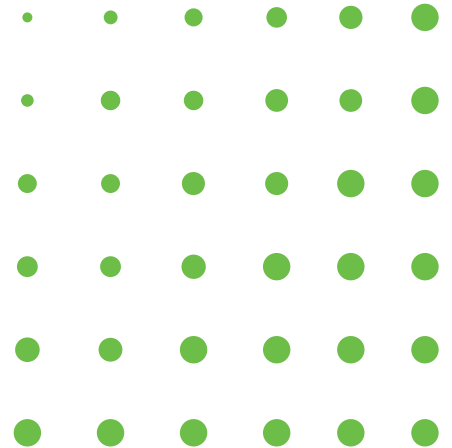
New API Documentation



- ✓ Several features improve navigation
 - Alphabetically ordered
 - Sub-sections are collapsible
 - Cleaner interface
- ✓ Many more language options for API calls
- ✓ Back-end redesign for accuracy and consistency



Some of our Favorite Endpoints



Getting Metrics

Under the “Asset Group Reporting” endpoint you can find nine (9) API calls that can be used to retrieve metrics information from your Kenna instance, such as:

- Average Days Open by Risk Level Over Time
- False Positive by Risk Level Over Time
- Historical Mean Time To Remediate by Risk Level
- Historical Vulnerability Risk Category Counts
- Past Due Vulnerabilities by Risk Level Over Time
- Historical Risk Meter Scores
- Risk Accepted by Risk Level Over Time
- Total Past Due Vulnerabilities by Risk Level
- Vulnerabilities by Due Date

```
RESPONSE 200 Try It
1 {
2   "id": 277286,
3   "name": "All",
4   "risk_meter_scores": {
5     "2021-12-12": 660,
6     "2021-12-13": 660,
7     "2021-12-14": 660,
8     "2021-12-15": 660,
9     "2021-12-16": 660,
10    "2021-12-17": 660,
11    "2021-12-18": 660,
12    "2021-12-19": 660,
13    "2021-12-20": 660,
14    "2021-12-21": 660,
15    "2021-12-22": 660,
16    "2021-12-23": 660,
17    "2021-12-24": 660,
18    "2021-12-25": 660,
19    "2021-12-26": 660,
20    "2021-12-27": 660,
21    "2021-12-28": 660,
22    "2021-12-29": 660,
23    "2021-12-30": 660,
24    "2021-12-31": 660,
25    "2022-01-01": 660,
26    "2022-01-02": 660,
27    "2022-01-03": 660,
28    "2022-01-04": 660,
29    "2022-01-05": 660,
30    "2022-01-06": 660,
31    "2022-01-07": 660,
32    "2022-01-08": 660,
33    "2022-01-09": 660,
34    "2022-01-10": 660,
35    "2022-01-11": 660
36  }
37 }
```

Show CVE History

Returns Kenna's CVE score history for one or more CVE identifiers.

- Customers who have purchased the Kenna.VI+ API may access any CVE.
- Customers who have not purchased Kenna.VI+ API may only access CVEs that correspond to vulnerabilities within their instance.

Use this endpoint to check when a specific CVE changed score and if that could be the reason why some Risk Meters' scores changed.

```
RESPONSE 200 Try It
1- {
2-   "CVE-2013-1710": {
3-     "id": 59209,
4-     "risk_meter_score": 100,
5-     "risk_meter_score_history": [
6-       {
7-         "changed_at": "2017-09-24T03:28:20.000Z",
8-         "from": 100,
9-         "to": 91
10-      },
11-      {
12-        "changed_at": "2017-12-31T03:19:53.000Z",
13-        "from": 91,
14-        "to": 92
15-      },
16-      {
17-        "changed_at": "2018-02-04T03:27:42.000Z",
18-        "from": 92,
19-        "to": 90
20-      },
21-      {
22-        "changed_at": "2018-04-12T03:15:52.000Z",
23-        "from": 90,
24-        "to": 100
25-      },
26-      {
27-        "changed_at": "2019-04-16T03:54:55.000Z",
28-        "from": 100,
29-        "to": 90
30-      },
31-      {
32-        "changed_at": "2019-05-12T03:42:18.000Z",
33-        "from": 90,
34-        "to": 100
35-      },
36-      {
37-        "changed_at": "2020-10-02T12:44:25.000Z",
38-        "from": 100,
39-        "to": 92
40-      },
41-      {
42-        "changed_at": "2020-11-08T12:25:51.000Z",
43-        "from": 92,
44-        "to": 100
45-      }
46-    ]
47-  }
48- }
```

Data Exports

Yes, even though we like data, we still share!

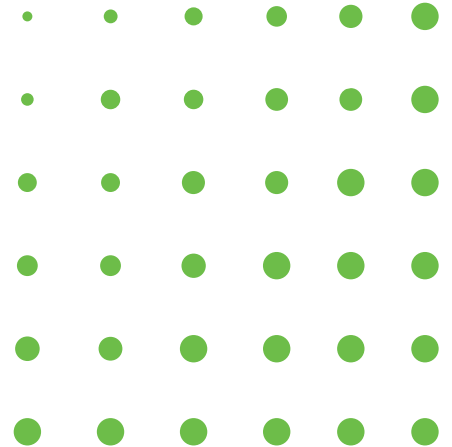
- ✓ Request Data Export (RDE)
- ✓ Check Data Export (CDE)
- ✓ Retrieve Data Export

There are some sample filter options in the Postman Collection

The screenshot displays a Postman interface with three API request details. The top request is a POST to `https://{{(API_URL)}}/data_exports...` with a body containing JSON: `{ "export_settings": { "format": "json", "model": "asset" } }`. The middle request is a GET to `https://{{(API_URL)}}/data_exports/status?search_id=1346955...` with query parameters `search_id=1346955` and `record_count=1003`. The bottom request is a GET to `https://{{(API_URL)}}/data_exports/status?search_id=1346955...` with a response body containing `"message": "Export ready for download"`.

KEY	VALUE
<input checked="" type="checkbox"/> search_id	1346955
Key	Value

From API endpoint(s) to Scripts



DO IT YOUR SELF THEY SAID



IT'S EASY THEY SAID

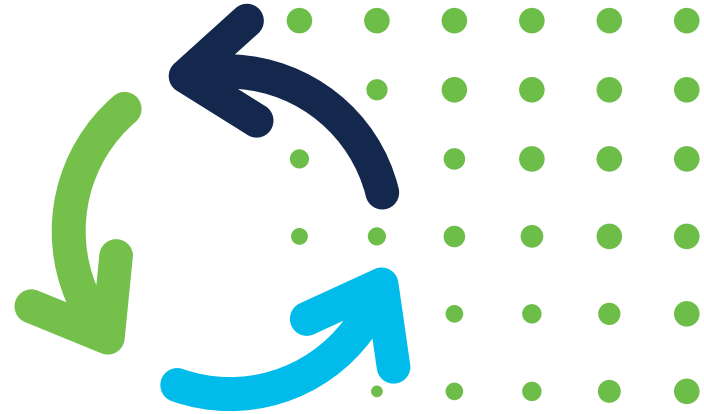
Sample script – Download all users

High-level design

- ✓ Prepare the API call
 - Token
 - Headers
 - Request Type (GET, PUT, POST, DELETE)
- ✓ Make the API call
- ✓ Get the response
- ✓ Format the response
- ✓ Save the response

```
1 $token = <token>
2 $headers = @{}
3 $headers["X-Risk-Token"] = [string]::Format($token)
4 $headers["Accept"] = "application/json"
5 $headers["Content-Type"] = "application/json"
6 $json_file = userlist.json
7 $csv_file = userlist.csv
8 $response = Invoke-RestMethod -Uri 'https://api.kennasecurity.com/users'
   -Method Get -Headers $headers
9 $response | ConvertTo-Json >> $json_file
10
11 ((Get-Content -Path $json_file) | ConvertFrom-Json).users | Export-Csv
   $csv_file -NoTypeInformation
```

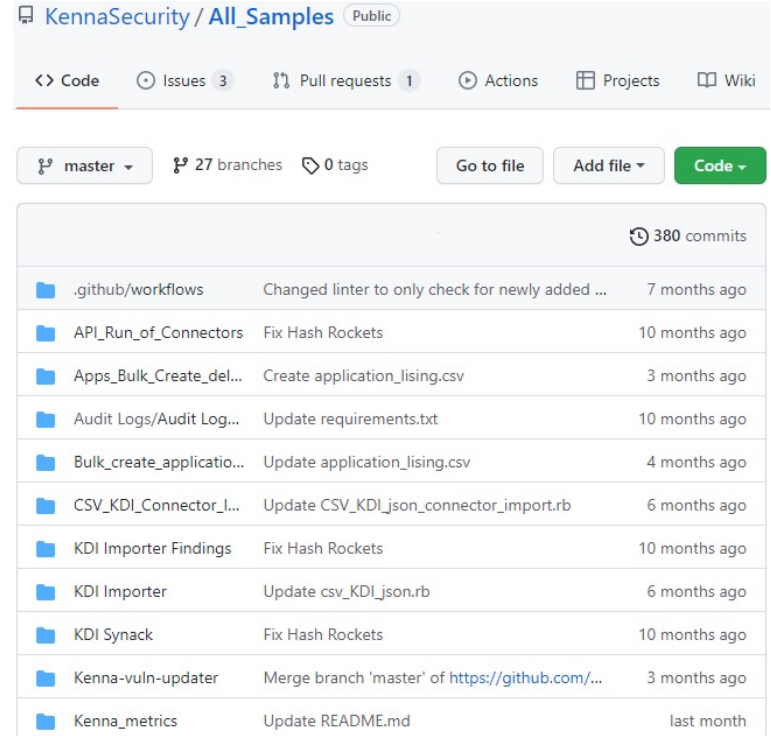
Kenna Public Script Repository



Kenna Public Script Repository

The scripts are written to assist customers in automating common functions on the Kenna Security Platform or to integrate data not natively support via Kenna Connectors.

- They are not part of the Kenna Engineering program and do not participate in a formal SDLC program.
- All the code samples in the All_Samples GitHub repository are **offered “as is”** and include no warranty of any kind.



KennaSecurity / All_Samples Public

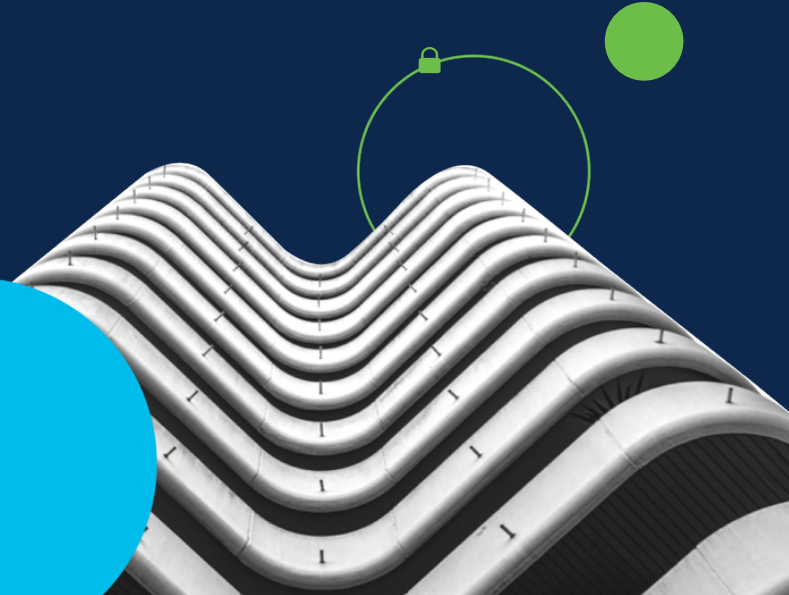
<> Code Issues 3 Pull requests 1 Actions Projects Wiki

master 27 branches 0 tags Go to file Add file Code

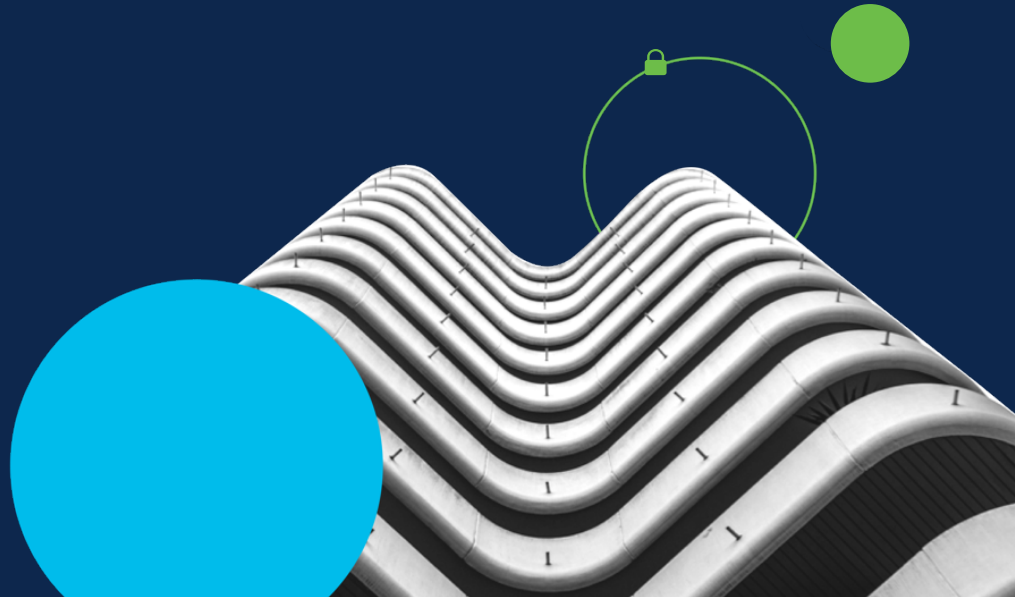
380 commits

.github/workflows	Changed linter to only check for newly added ...	7 months ago
API_Run_of_Connectors	Fix Hash Rockets	10 months ago
Apps_Bulk_Create_del...	Create application_lising.csv	3 months ago
Audit_Logs/Audit Log...	Update requirements.txt	10 months ago
Bulk_create_applicatio...	Update application_lising.csv	4 months ago
CSV_KDI_Connector_l...	Update CSV_KDI_json_connector_import.rb	6 months ago
KDI_Importer Findings	Fix Hash Rockets	10 months ago
KDI_Importer	Update csv_KDI_json.rb	6 months ago
KDI_Synack	Fix Hash Rockets	10 months ago
Kenna-vuln-updater	Merge branch 'master' of https://github.com/...	3 months ago
Kenna_metrics	Update README.md	last month

Demos with some
interesting scripts



API Links & Resources



API Documentation & Helpful Links

- API Documentation can be found here:
 - <https://apidocs.kennasecurity.com>
- Github – Kenna Toolkit:
 - <https://github.com/KennaSecurity/toolkit>
- Kenna Help Center:
 - <https://help.kennasecurity.com/hc/en-us>



Questions?



Thank You!

