

ThreatQuotient



GitHub Nomi Sec CVE PoCs CDF User Guide

Version 1.0.0

June 26, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
ThreatQ Mapping.....	9
Nomi Sec CVE PoCs.....	9
GitHub - Fetch JSON (Supplemental).....	11
Average Feed Run.....	13
Nomi Sec CVE PoCs.....	13
Known Issues / Limitations	14
Change Log	15

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.58.0
Support Tier	ThreatQ Supported

Introduction

The GitHub Nomi Sec CVE PoCs CDF can be used to automatically pull CVE PoC information from Nomi Sec's PoC-in-GitHub repository.

The integration provides the following feeds:

- **Nomi Sec CVE PoCs** - pulls CVE PoC information from Nomi Sec's PoC-in-GitHub repository.
- **GitHub - Fetch JSON(Supplemental)** - pulls CVE details from Nomi Sec's PoC-in-GitHub repository.

The integration ingests the following system objects:

- Indicators
 - Indicator Attributes

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.

4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Nomi Sec CVE PoCs

The Nomi Sec CVE PoCs feed pulls the PoC CVEs stored in GitHub.

GET <https://api.github.com/repos/nomi-sec/PoC-in-GitHub/contents/{since}>

Sample Response:

```
[
  {
    "name": "CVE-2023-0045.json",
    "path": "2023/CVE-2023-0045.json",
    "sha": "de58d4a0fa340554d6845ef9bc083f76d312918d",
    "size": 1893,
    "url": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/contents/2023/CVE-2023-0045.json?ref=master",
    "html_url": "https://github.com/nomi-sec/PoC-in-GitHub/blob/master/2023/CVE-2023-0045.json",
    "git_url": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/git/blobs/de58d4a0fa340554d6845ef9bc083f76d312918d",
    "download_url": "https://raw.githubusercontent.com/nomi-sec/PoC-in-GitHub/master/2023/CVE-2023-0045.json",
    "type": "file",
    "_links": {
      "self": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/contents/2023/CVE-2023-0045.json?ref=master",
      "git": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/git/blobs/de58d4a0fa340554d6845ef9bc083f76d312918d",
      "html": "https://github.com/nomi-sec/PoC-in-GitHub/blob/master/2023/CVE-2023-0045.json"
    }
  },
  {
    "name": "CVE-2023-0050.json",
    "path": "2023/CVE-2023-0050.json",
    "sha": "2115d1102696d48260d6887be3b8d169ce059c1e",
    "size": 961,
    "url": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/contents/2023/CVE-2023-0050.json?ref=master",
    "html_url": "https://github.com/nomi-sec/PoC-in-GitHub/blob/master/2023/CVE-2023-0050.json",
    "git_url": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/git/blobs/2115d1102696d48260d6887be3b8d169ce059c1e",
    "download_url": "https://raw.githubusercontent.com/nomi-sec/PoC-in-GitHub/master/2023/CVE-2023-0050.json",
    "type": "file",
    "_links": {
```

```
        "self": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/
contents/2023/CVE-2023-0050.json?ref=master",
        "git": "https://api.github.com/repos/nomi-sec/PoC-in-GitHub/git/
blobs/2115d1102696d48260d6887be3b8d169ce059c1e",
        "html": "https://github.com/nomi-sec/PoC-in-GitHub/blob/master/
2023/CVE-2023-0050.json"
    }
}
]
```

GitHub - Fetch JSON (Supplemental)

The GitHub - Fetch JSON supplemental feed pulls PoC information for CVEs stored in GitHub, based on the CVE's download_url.

<https://raw.githubusercontent.com/nomi-sec/PoC-in-GitHub/master/{year}/CVE-{cve-id}.json>

Sample Response:

```
[
  {
    "id": 597559046,
    "name": "CVE-2023-0045",
    "full_name": "ASkyeye/CVE-2023-0045",
    "owner": {
      "login": "ASkyeye",
      "id": 50972716,
      "avatar_url": "https://avatars.githubusercontent.com/u/50972716?v=4",
      "html_url": "https://github.com/ASkyeye"
    },
    "html_url": "https://github.com/ASkyeye/CVE-2023-0045",
    "description": null,
    "fork": false,
    "created_at": "2023-02-04T22:42:21Z",
    "updated_at": "2023-02-23T07:53:12Z",
    "pushed_at": "2023-02-03T22:22:52Z",
    "stargazers_count": 0,
    "watchers_count": 0,
    "has_discussions": false,
    "forks_count": 5,
    "allow_forking": true,
    "is_template": false,
    "web_commit_signoff_required": false,
    "topics": [],
    "visibility": "public",
    "forks": 5,
    "watchers": 0,
    "score": 0
  },
  {
    "id": 598766898,
    "name": "CVE-2023-0045",
    "full_name": "es0j/CVE-2023-0045",
    "owner": {
      "login": "es0j",
      "id": 37257235,
      "avatar_url": "https://avatars.githubusercontent.com/u/37257235?v=4",

```

```

      "html_url": "https://github.com/es0j"
    },
    "html_url": "https://github.com/es0j/CVE-2023-0045",
    "description": null,
    "fork": false,
    "created_at": "2023-02-07T19:12:41Z",
    "updated_at": "2023-04-17T04:45:09Z",
    "pushed_at": "2023-02-07T19:15:48Z",
    "stargazers_count": 11,
    "watchers_count": 11,
    "has_discussions": false,
    "forks_count": 1,
    "allow_forking": true,
    "is_template": false,
    "web_commit_signoff_required": false,
    "topics": [],
    "visibility": "public",
    "forks": 1,
    "watchers": 11,
    "score": 0
  }
]

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.name</code>	Indicator Value	CVE	N/A	N/A	N/A
<code>.owner.login</code>	Attribute	Publisher	<code>.created_at</code>	ASkyeye	N/A
<code>.html_url</code>	Attribute	Link	<code>.created_at</code>	https://github.com/ASkyeye/CVE-2023-0045	N/A
<code>.pushed_at</code>	Attribute	Pushed At	<code>.created_at</code>	2023-02-07T19:15:48Z	Timestamp
<code>.updated_at</code>	Attribute	Updated At	<code>.created_at</code>	2023-04-17T04:45:09Z	Timestamp. Field is updated at ingestion.
<code>.description</code>	Description	N/A	N/A	n/A	N/A
<code>.topics[]</code>	Tag	N/A	N/A	N/A	CVE ID topics are excluded

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Nomi Sec CVE PoCs

METRIC	RESULT
Run Time	5 minutes
Indicators	41
Indicator Attributes	212

Known Issues / Limitations

- The first run for this integration will only pull PoCs that have been updated within the past 24 hours.
- To ingest older PoC information, re-run the integration manually, setting the date timeframe back to when you want to start pulling PoC data.

Change Log

- Version 1.0.0
 - Initial release