ThreatQuotient

CrowdStrike Next-Gen SIEM Connector

Version 2.1.0

March 17, 2025

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

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.

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	2.1.0
Compatible with ThreatQ Versions	>= 6.3.0
Third-Party Application Hosting Type	On-Premise, Cloud
Python Version	3.6
Support Tier	ThreatQ Supported

Introduction

The CrowdStrike Next-Gen SIEM Connector for ThreatQ enables the automatic dissemination of IOCs from a ThreatQ data collection to a CrowdStrike Next-Gen SIEM Lookup File.

The integration will convert IOC results from the Threat Library into CSV files to be uploaded to CrowdStrike Next-Gen SIEM. Separate CSV files will be created based on type and uploaded to CrowdStrike Next-Gen SIEM. The files can then be used to add contextual information to log data using the match search function. The added contextual information such as score, related malware, related adversaries, and tags can be used to create alert policies.

The integration utilizes the following endpoint:

- **{CROWDSTRIKE_HOST}/humio/api/v1/repositories/{REPOSITORY}/files**

> This connector does not ingest any data back into ThreatQ.

Prerequisites

Review the following requirements before attempting to install the connector.

Third-Party Credentials/Scope

The following is required by the integration:

- CrowdStrike Next-Gen SIEM API URL.
- CrowdStrike Client ID with **NGSIEM** scope.
- CrowdStrike Client Secret with **NGSIEM** scope.
- CrowdStrike Repository to receive exported IOCs.

Integration Dependencies

> ⚠ The integration must be installed in a python 3.6 environment.

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you will need to download and install these dependencies separately as the integration will not be able to download them during the install process.

> Items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

DEPENDENCY	VERSION	NOTES
threatqsdk	>= 1.8.10	N/A
threatqcc	>= 1.4.4	N/A
python-dateutil	>= 2.8.2	N/A
pytz	>= 2022.4	N/A
requests	>= 2.21.0	N/A

Installation

Use the following steps to install the connector.

> ⚠ **Upgrading Users -** Review the Change Log for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. The location of this file will differ between ThreatQ v6 and v5. Failure to delete the previous configuration file will result in the connector failing.

1. Download the connector integration file from the ThreatQ Marketplace.
2. Transfer the connector whl file to the `/tmp/` directory on your instance.
3. SSH into your instance.
4. Move the connector whl file from its `/tmp/` location to the following directory: `/opt/tqvenv`
5. Navigate to the custom connector container:

   ```
   kubectl exec -n threatq -it deployments/custom-connectors -- /bin/bash
   ```
6. Create your python 3 virtual environment:

   ```
   python3.6 -m venv /opt/tqvenv/<environment_name>
   ```
7. Active the new environment:

   ```
   source /opt/tqvenv/<environment_name>/bin/activate
   ```
8. Install the required dependencies:

   ```
   pip install --upgrade pip
   pip install setuptools==59.6.0
   pip install threatqsdk threatqcc python-dateutil pytz requests
   ```
9. Install the connector:

   ```
   pip install /opt/tqvenv/tq_conn_crowdstrike_next_gen_siem-<version>-
   py3-none-any.whl
   ```
10. Perform an initial run of the connector:

    ```
    /opt/tqvenv/<environment_name>/bin/tq-conn-crowdstrike-next-gen-siem
    --cron="0 */2 * * *"
    ```

    > The `--cron` argument above is used to generate a cron job for the connector. After running the command above, the cronjob will be created under the /etc/cron.d/ directory. This entry will initially be commented out upon creation - see the CRON section for more details.

11. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	**Leave this field blank as this field will be set dynamically.**
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user’s details.
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.
ThreatQ Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

Example Output

```
/opt/tqvenv/<environment_name>/bin/tq-conn-crowdstrike-next-gen-siem --cron="0
*/2 * * *"
ThreatQ Host:
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

You will still need to configure and then enable the connector.

Configuration

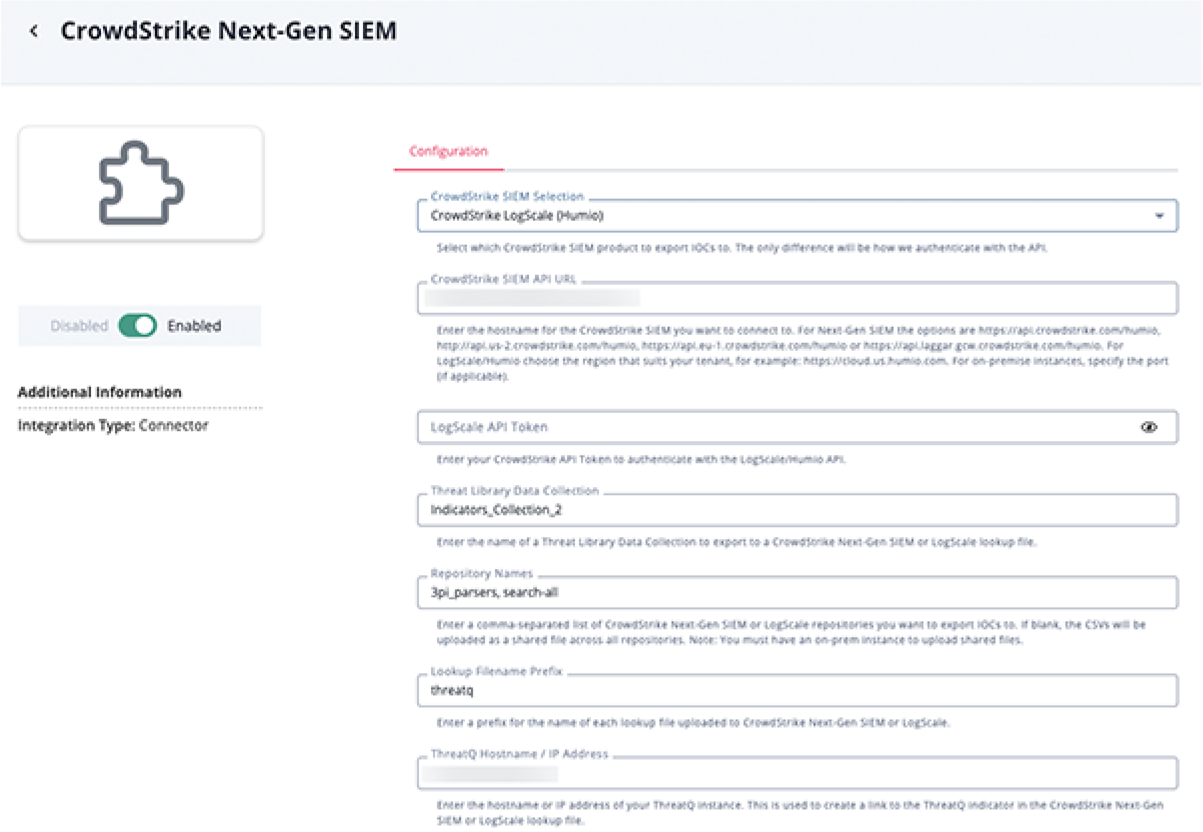
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the *Category* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
CrowdStrike SIEM Selection	Select the CrowdStrike SIEM product to export IOCs to via the connector. Options include: ◦ CrowdStrike Next-Gen SIEM ◦ CrowdStrike LogScale (Humio) Your selection here will only affect how the connector authenticates with the API.
CrowdStrike Next-Gen SIEM API URL	Enter the hostname for the CrowdStrike Next-Gen SIEM. The options for cloud instances are: ◦ https://api.crowdstrike.com/humio ◦ http://api.us-2.crowdstrike.com/humio ◦ https://api.eu-1.crowdstrike.com/humio ◦ https://api.laggar.gcw.crowdstrike.com/humio On-Premise instances are required to specify the port as well.
CrowdStrike Client ID	Enter your CrowdStrike Client ID to authenticate with the API. This parameter will be displayed if you have selected the `CrowdStrike Next-Gen SIEM` option for the **CrowdStrike Next-Gen SIEM API URL** configuration parameter.

PARAMETER	DESCRIPTION
CrowdStrike Client Secret	Enter your CrowdStrike Client Secret to authenticate with the API. This parameter will be displayed if you have selected the `CrowdStrike Next-Gen SIEM` option for the **CrowdStrike Next-Gen SIEM API URL** configuration parameter.
LogScale API Token	Enter your CrowdStrike API token used to authenticate with the LogScale/Humio API. This parameter will be displayed if you have selected the `CrowdStrike LogScale (Humio)` option for the **CrowdStrike Next-Gen SIEM API URL** configuration parameter.
Threat Library Data Collection	Enter the name of a Threat Library Data Collection to export to a CrowdStrike Next-Gen SIEM or LogScale (Humio) lookup file.
Repository Names	Enter a comma-separated list of CrowdStrike Next-Gen SIEM/ LogScale repository you want to export IOCs to. If this parameter is left blank, the CSVs will be uploaded as a shared file across all repositories. You must have an on-premise instance to upload shared files.
Lookup Filename Prefix	Enter a prefix for the name of each lookup file uploaded to CrowdStrike Next-Gen SIEM or LogScale (Humio).
ThreatQ Hostname / IP Address	Enter the hostname or IP address of your ThreatQ instance. This is used to create a link to the ThreatQ indicator in the CrowdStrike Next-Gen SIEM or LogScale (Humio)lookup file.



CrowdStrike Next-Gen SIEM

Disabled Enabled

Additional Information

Integration Type: Connector

CrowdStrike SIEM Selection: CrowdStrike LogScale (Humio)

Select which CrowdStrike SIEM product to export IOCs to. The only difference will be how we authenticate with the API.

CrowdStrike SIEM API URL

Enter the hostname for the CrowdStrike SIEM you want to connect to. For Next-Gen SIEM the options are https://api.crowdstrike.com/humio, http://api.us-2.crowdstrike.com/humio, https://api.eu-1.crowdstrike.com/humio or https://api.laggar.gcw.crowdstrike.com/humio. For LogScale/Humio choose the region that suits your tenant, for example: https://cloud.us.humio.com. For on-premise instances, specify the port (if applicable).

LogScale API Token

Enter your CrowdStrike API Token to authenticate with the LogScale/Humio API.

Threat Library Data Collection: Indicators_Collection_2

Enter the name of a Threat Library Data Collection to export to a CrowdStrike Next-Gen SIEM or LogScale lookup file.

Repository Names: 3pi_parsers, search-all

Enter a comma-separated list of CrowdStrike Next-Gen SIEM or LogScale repositories you want to export IOCs to. If blank, the CSVs will be uploaded as a shared file across all repositories. Note: You must have an on-prem instance to upload shared files.

Lookup Filename Prefix: threatq

Enter a prefix for the name of each lookup file uploaded to CrowdStrike Next-Gen SIEM or LogScale.

ThreatQ Hostname / IP Address

Enter the hostname or IP address of your ThreatQ instance. This is used to create a link to the ThreatQ indicator in the CrowdStrike Next-Gen SIEM or LogScale lookup file.

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

Usage

The following section include driver commands, CLI arguments, directory locations, and CRON steps.

Driver Command

```
/opt/tqvenv/<environment_name>/bin/tq-conn-bulk-csv-exporter
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
`-h`, `--help`	Review all additional options and their descriptions.
`-ll LOGLOCATION`, `--loglocation LOGLOCATION`	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).
`-c CONFIG`, `--config CONFIG`	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)
`-v {1,2,3}`, `--verbosity {1,2,3}`	This is the logging verbosity level where **3** means everything.
`-n, --name`	Optional - Name of the connector (Option used in order to allow users to configure multiple connector instances on the same TQ box).
--cron	Creates a CRON entry for the connector based on a pre-loaded ThreatQ template. See the CRON section for more details.

Accessing Connector Logs

ThreatQ version 6 aggregates the logs for all custom connectors to its output container. You can access the container's log using the following command:

```
kubectl logs -n threatq deployments/custom-connectors
```

Accessing Connector Configuration

The custom connector configuration file can be found in the following directory: `/etc/tq_labs/`.

CRON

The addition of the `--cron` argument in the initial run of connector, performed during the install process, resulted in the creation of a cron job file for the connector in the following directory: `/etc/cron.d/`. The contents of the file will resemble the following structure:

```
#{schedule} root /bin/bash -c "source /etc/env-vars.sh; {venv_path}/bin/
{executable} --config=/etc/tq_labs > /proc/1/fd/1 2>/proc/1/fd/2"
```

The `{schedule}` will be replaced with the cron settings you entered with the `--cron` flag and the `{executable}` will be replaced for with the connector's driver command.

You will also see a `#` at the beginning of the file. This comments out the job. This allows you to configure the custom connector in the ThreatQ UI first. After you have configured the connector in ThreatQ, you can remove the `#` from the file content's in order to activate the cron job.

To summarize this process:

1. Install the connector and perform an initial run using the `--cron` argument to create the cron job.
2. Complete the connector's configuration settings in the ThreatQ UI.
3. Access the connector's cron file in the `/etc/cron.d/` directory and remove the # from the beginning of the file.

Known Issues / Limitations

- The temporary CSV files are saved to `/etc/tq_lab` if the argument `--config` is not present.

Change Log

- **Version 2.1.0**
  - Added compatibility with CrowdStrike LogScale (Humio).
  - Added the following configuration parameters:
    - **CrowdStrike SIEM Selection -** allows you to select the CrowdStrike SIEM product to export IOCs to via the connector.
    - **LogScale API Token -** your CrowdStrike API Token to authenticate with the LogScale (Humio) API.
- **Version 2.0.0**
  - Initial release