

ThreatQuotient



Tenable.sc Connector Guide

Version 1.5.0

March 18, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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 © 2021 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.

Contents

Versioning.....	4
Introduction.....	5
Installation	6
Configuration.....	9
Usage.....	11
Command Line Arguments	11
Adding Assets Object to ThreatQ	12
CRON	15
Change Log.....	16

Versioning

- Current integration version: 1.5.0
- Supported on ThreatQ versions $\geq 4.40.0$

OPERATION SYSTEM	OS VERSION	PYTHON VERSION	NOTES
Redhat/CentOS	7	3.6.12	N/A
Ubuntu	16.04	3.6.12	This has not been tested.
Windows	2012R2/10	3.6.12	This has not been tested.

Introduction

The Tenable.sc Connector captures vulnerability data from Tenable.sc and adds it to ThreatQ.

This data can be found on your Tenable.sc account under **Analysis > Vulnerabilities**, with each vulnerability providing more information such as CVEs and IP Addresses when clicked on.

Vulnerabilities are stored within the Vulnerabilities object and CVEs are stored as Indicators and related back to the Vulnerability in ThreatQ. If selected, the connector can also add IP Addresses from Tenable.sc as **Assets** in ThreatQ and relate them back to the relevant CVEs and Vulnerabilities - simply make sure to have the Asset custom object installed on your ThreatQ instance.

Installation

The connector can be installed from the ThreatQuotient repository with YUM credentials or offline via a .whl file.

⚠ 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. Failure to delete the previous configuration file will result in the connector failing.

1. Install the connector using one of the following methods:

ThreatQ Repository

- a. Run the following command:

```
< > pip install tq_conn_tenable_sc
```

Offline via .whl file

To install this connector from a wheel file, the wheel file (.whl) will need to be copied via SCP into your ThreatQ instance.

- a. Download the connector whl file with its dependencies:

```
< > mkdir /tmp/tq_conn_tenable_sc
      pip download tq_conn_tenable_sc -d
      /tmp/tq_conn_tenable_sc/
```

- b. Archive the folder with the .whl files:

```
< > tar -czvf tq_conn_tenable_sc.tgz /tmp/tq_conn_tenable_sc/
```

- c. Transfer all the whl files, the connector and all the dependencies, to the ThreatQ instance.
- d. Open the archive on ThreatQ:

```
< > tar -xvf tq_conn_tenable_sc.tgz
```

- e. Install the connector on the ThreatQ instance.



The example assumes that all the whl files are copied to /tmp/conn on the ThreatQ instance.

```
< > pip install /tmp/conn/tq-conn-tenable-sc.whl --no-index --find-links /tmp/conn/
```



A driver called tq-conn-tenable-sc is installed. After installing with pip or setup.py, a script stub will appear in /usr/bin/tq-conn-tenable-sc.

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the mkdir -p command. See example below:

Creating Integration Directories Example

```
< > mkdir -p /etc/tq_labs/  
mkdir -p /var/log/tq_labs/
```

3. Perform an initial run using the following command:

```
< > tq-conn-tenable-sc -c /path/to/config/directory/ -ll /path/to/log/directory/ -v  
VERBOSITY_LEVEL
```

Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
Email Address	This is the User in the ThreatQ System for integrations.
Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

Example Output

```
tq-conn-tenable-sc -c /path/to/config/directory/ -l /path/to/log/directory/ -v VERBOSITY_LEVEL
```

ThreatQ Host: <ThreatQ Host IP or Hostname>

Client ID: <ClientID>

E-Mail Address: <EMAIL ADDRESS>

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).



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

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Tenable.sc Host	This is the hostname or IP address for the Tenable.sc server. <div> The scheme is not required.</div>
Tenable.sc Port	The port that is used to connect to Tenable.sc.
Tenable.sc API User Name	A Tenable.sc user that has privileges to access scan result and vulnerability data.
Tenable.sc API User Password	The password for the Tenable.sc user.
Capture Assests (checkbox)	(Optional) Enables the capture of Asset Information.
Severity Selection	Choose the minimum severity level from which to capture vulnerability data.

PARAMETER	DESCRIPTION
Exploitability Selection	Narrow down results from Tenable.sc based on exploitability of a vulnerability.
Number of Search Hours	Number of hours to search back for results.

5. Review the **Settings** configuration, 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

You can execute the integration using the following command:

```
< > tq-conn-tenable-sc -c /path/to/config/directory/ -ll /path/to/log/directory/
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
-h, --help	Shows this help message and exits.
-n, --name	Change the name of the connector.
-d, --no-differential	If exports are used in this connector, this will turn 'off' the differential flag for the execution. This allows debugging and testing to be done on export endpoints without having to rebuild the exports after the test. <div> This should never be used in production.</div>
-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. The default is 1 (Warning). Recommended value is 3 (Debug).

ARGUMENT	DESCRIPTION
-ep, --external-proxy	This allows you to use the proxy that is specified in the ThreatQ UI.
-ds, --disasble-ssl	Adding this flag will disable verification of SSL certificates in tenable.sc API.

Adding Assets Object to ThreatQ

The following are the steps to install a custom object, called Assets in ThreatQ. The object is not mandatory for the operation. However, it enables the functionality to add IP Addresses related to vulnerabilities in Tenable.sc as assets to ThreatQ. If you would like to add an icon, select an SVG file and upload it to ThreatQ. If you don't need one, ThreatQ will use a star for the icon.

To install the custom object:

1. Create a custom object definition

Create a JSON file with the content below either locally, or directly on the ThreatQ instance in the custom objects folder shown below.

```
[
  {
    "code": "asset",
    "name": "Assets",
    "description": "ASSET",
    "icon": "/var/www/api/database/seeds/data/icons/images/custom_objects/asset.svg",
    "fg_color": "#ffffff",
    "bg_color": "#db4e4e",
    "fields": [
      {
        "field": "value",
        "name": "Title",
        "definition": "varchar(128) NOT NULL",
        "required": "Yes"
      },
      {
        "field": "description",
        "name": "Description",
        "definition": "text",
        "required": "No"
      },
      {
        "field": "published_at",
        "name": "Published At",
```

```
    "definition": "datetime(3) DEFAULT NULL",
    "required": "Yes"
  }
}
}
```

2. Create a ThreatQ icon for the custom object

The icon should be a file in SVG format and placed on the ThreatQ instance. We recommend using the following definition for the custom object icon. Create a file locally or directly on the ThreatQ instance in the folder `/var/www/api/database/seeds/data/icons/images/custom_objects/asset.svg`

```
<?xml version="1.0" encoding="utf-8"?>
<svg enable-background="new 0 0 1000 1000" id="Layer_1" version="1.1" viewBox="0 0 1000 1000" x="0px" xml:space="preserve"
xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" y="0px">
<style type="text/css">
    .st0{fill:#FFFFFF;}
</style>
<g><g transform="translate(150.000000,511.000000) scale(0.0700000,-0.0700000)"><path class="st0"
d="M4651,4707.5c-626.6-13.4-1379.7-82.4-1946.9-178.2c1251.7,4284.1,356.8,3864.4,134.5,3320.2c101.9,3239.7,100,3073,100,93.3v-3142.6l55
.
6-113.1c295.1-601.7,1485.1-1063.5,3240.3-1255.1c550-61.3,954.3-80.5,1600-80.5c1076.9,0,2044.6,97.7,2882,289.3c996.4,230,1680.5,578.7,192
2,977.3c107.3,178.2,103.5,7.7,97.7,3384l-5.7,3104.3l-65.2,126.5c-67.1,136-229.9,312.3-394.7,429.2c-567.2,402.4-1711.2,712.8-3104.3,839.3c-31
2.3,28.7-1249.4,72.8-1389.3,65.2c4902.1,4715.2,4771.7,4711.4,4651,4707.5z
M6174.4,4320.4c726.3-70.9,1243.6-151.4,1724.6-270.2c879.6-216.5,1469.7-521.2,1619.2-833.6c47.9-99.6,47.9-151.4-5.7-268.3c-218.5-467.6-14
58.3-900.6-3041.1-1063.5c-2222.8-226.1-4696.7,95.8-5658.6,733.9c544.6,2799,414.3,2981,443,3138.1c99.6,527,1621.1,1053.9,3403.2,1180.4c1
62.9,11.5,335.3,23,383.2,26.8c4407.7,4360.7,5971.3,4339.6,6174.4,4320.4z
M592.5,2341c138-92,433.1-239.5,661.1-327.7c624.7-247.2,1554-425.4,2659.7-515.5c404.3-32.6,1761-32.6,2165.3,0c1546.4,124.6,2682.7,415.8,
3338.1,856.6l130.3,86.2l5.8-691.8c3.8-640,1.9-697.5-30.7-772.2c-80.5-178.2-272.1-333.4-618.9-498.2c7249.4-313,3591.4-403,1527.6,298.3c-29
5.1,99.6-689.8,297-843.1,423.5c-67.1,55.6-149.5,143.7-182,193.5l-57.5,93.9l-5.7,718.6c-3.8,578.7,0,712.8,19.2,701.3c471.7,2421.5,533.1,2381.2,
592.5,2341z
M617.4,334.7c1855.3-456.7,4888.6-759.4,7362.5-336c850.8,145.6,1548.3,381.3,2031.2,684.1l1153.3,95.8l5.8-672.6c3.8-438.8-1.9-699.4-15.3-745
.
4c-46-161-274-364.1-584.5-517.4c-666.8-333.4-1768.7-567.2-3050.6-649.6c-475.2-28.7-1785.9-13.4-2219,28.7c-1510,147.6-2652.1,488.6-3087,9
21.7c-161,162.9-161,153.3-161,944.7c0,551.9,5.7,693.7,24.9,682.2c471.7,428.6,544.6,382.6,617.4,334.7z
M565.6-1619.8c672.6-454.1,1860.7-753.1,3443.5-866.1c419.6-30.7,1554-30.7,1973.7,0c1556,111.2,2734.5,402.4,3407,843.1c82.4,53.7,153.3,97.
7,157.1,97.7c5.8,0,9.6-312.3,9.6-693.7c0-801,3.8-779.9-178.2-956.2c-325.8-320-1115.3-611.3-2121.3-781.8c-766.5-130.3-1243.6-164.8-2261.1-1
64.8c-1017.5,0-1492.7,34.5-2261.1,164.8c-1015.6,170.6-1808.9,467.6-2140.4,801c-161,159-159,147.5-159,937c0,381.3,3.8,693.7,11.5,693.7c45
2.6-1545.1,506.2-1577.7,565.6-1619.8z"/></g></g>
</svg>
```

3. Copy the custom object to ThreatQ and install it.

< > # Copy the icon and the JSON for the custom object to the ThreatQ instance

```
scp /path/to/asset.svg root@<THREATQ HOST>:/var/www/api/database/seeds/
data/icons/images/custom_objects/asset.svg
```

```
scp /path/to/asset.json root@<THREATQ HOST>:/var/www/api/database/seeds/
data/custom_objects/asset.json
```

```
# Install the custom object
cd /var/www/api
```

```
sudo php artisan threatq:make-object-set --file=/var/www/api/database/seeds/
data/custom_objects/asset.json
```

```
# Start up ThreatQ  
sudo php artisan up
```

After the object is installed, it will appear in the ThreatQ Threat Library under Adversaries.

CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis, use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector every hour.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

```
< > crontab -e
```

This will enable the editing of the crontab, using vi. Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Enter the commands below:

Every Hour Example

```
< > 0 * * * * /usr/bin/tq-conn-tenable-sc -c /path/to/config/directory/ -ll /path/to/log/directory/ -ll /path/to/config/directory/ -v VERBOSITY_LEVEL
```

4. Save and exit CRON.

Change Log

- Version 1.5.0
 - Added asset custom object existence verification functionality.
 - Integration moved to the ThreatQ Integration Repository.
 - Removed requests from requirements.