

ThreatQuotient



SentinelOne Connector Guide

Version 1.0.0

August 31, 2021

ThreatQuotient

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

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Versioning.....	4
Prerequisites	5
Introduction.....	6
Installation	7
Configuration.....	10
Usage.....	12
Command Line Arguments	12
CRON.....	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 © 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.

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions \geq 4.30.0

There are two versions of this integration:

- Python 2 version
- Python 3 version

Prerequisites

You should ensure all ThreatQ devices are set to the correct time, time zone, and date (UTC is recommended), and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option.

For example, enter the following command to list all available time zones in Europe:

```
timedatectl list-timezones | grep Europe  
Europe/Amsterdam  
Europe/Athens  
Europe/Belgrade  
Europe/Berlin
```

Enter the following command, as root, to change the time zone to UTC:

```
timedatectl set-timezone UTC
```

Introduction

SentinelOne Connector enables users to block IP Addresses using SentinelOne's Network Control.

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_sentinelone
```

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_sentinelone  
  
pip download tq_conn_sentinelone -d  
  
/tmp/ tq_conn_sentinelone/
```

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

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

- 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_sentinelone.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_sentinelone-<version>-<python version>-none-any.whl --no-index --find-links /tmp/conn/
```



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

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. Use the commands below to create the required directories:

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

3. Perform an initial run using the following command:

```
<> tq-conn-sentinelone -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

4. 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.
ThreatQ Username	This is the User in the ThreatQ System for integrations.
ThreatQ Password	The password for the above ThreatQ account.

Example Output

```
tq-conn-sentinelone -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/  
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).
3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
SentinelOne Host	Your SentinelOne Hostname.
Username	Your Username to authenticate with SentinelOne.
Password	The password associated with the account referenced above.
Site Names	A comma-separated list of site names for this integration to execute on. You can use the wildcard "*" to specify all sites.
Data Collection (Threat Library)	Enter the number of Qualys IDs to search at a time. Consult the administrative setting in Qualys to determine this value. The default value is 1000. <div> Only IP Addresses will be exported to SentinelOne.</div>
Firewall Rule Direction	The network direction that should apply to the rule. Options include: <ul style="list-style-type: none">• Any (default)

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none">• Inbound• Outbound
Firewall Rule Operating System	<p>The operating systems that should apply to the rule.</p> <p>Options include:</p> <ul style="list-style-type: none">• Windows• Linux• macOS
Firewall Rule Enabled by Default	Enable the Firewall Rule by default option.

5. Review any additional settings available, 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

Use the following command to execute the driver:

```
<> tq-conn-sentinelone -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3  
VERBOSITY_LEVEL
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
<code>-h, --help</code>	Shows this help message and exits.
<code>-ll LOGLOCATION, --loglocation LOGLOCATION</code>	Sets the logging location for the connector. The location should exist and be writable by the current.
<code>-c CONFIG, --config CONFIG</code>	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 oath, etc.)
<code>-v {1,2,3}, --verbosity {1,2,3}</code>	This is the logging verbosity level where 3 means everything.
<code>-n, --name</code>	Optional - Name of the connector (Option used in order to allow users to configure multiple Cybereason connector instances on the same TQ box).



All location-based options default to the current working directory if they are not provided. To find additional options and option descriptions, invoke the program with `-h`.

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 two hours.

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 2 Hours Example

```
<> 0 */2 * * * tq-conn-sentinelone -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

4. Save and exit CRON.

Known Issues / Limitations

- Due to API limitations with SentinelOne, bulk blocking is only enabled for IP Addresses.
- Each Firewall rule is limited to a maximum of 5,000 IP Addresses. As a result, if your data collection has more than 5,000 items, they will be broken into multiple rules. Each rule will be marked with a (1), (2), (3), etc.

Change Log

- Version 1.0.0
 - Initial Release