ThreatQuotient

Snort Community Rules Connector Guide

Version 1.1.1

April 20, 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.

Contents

Versioning

- Current integration version: `1.1.1`
- Supported on ThreatQ versions >= `3.6.0`

There are two versions of this integration:

- Python 2 version
- Python 3 version

Introduction

The ThreatQuotient for Snort Community Rules Application downloads and ingests the Snort community rules into the ThreatQ platform.

The versions of Snort rules can be downloaded and ingested together (both versions included) or split into separte versions (versions 2 or 3). See the **Versions** parameter setting under Configuration for more information.

Notes

- The connector should take about 2-4 minutes to run (when downloading from both rulesets).
- Snort Community Rules are only updated every so often. To prevent the connector from re-downloading and re-uploading the same signatures, hashes of the rules are saved, and checked on each run.
- An attribute, **Snort Version,** is added to each signature so you will know which ruleset it came from.
- Many signatures contain CVE references. These CVE values are added to ThreatQ and related to the signature.

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-snort-comm-rules
   ```

   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-snort-comm-rules

      pip download tq-conn-snort-comm-rules -d

      /tmp/ tq-conn-snort-comm-rules/
   ```

   b. Archive the folder with the .whl files:

   ```
   <> tar -czvf tq-conn-snort-comm-rules.tgz /tmp/ tq-conn-
      snort-comm-rules/
   ```

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

pip install /tmp/conn/ tq-conn-snort-comm-rules-1.1.1-py2-none-any.whl --no-index --find-links /tmp/conn/

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

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-snort-comm-rules -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.
Email Address	This is the User in the ThreatQ System for integrations.
Password	The password for the above ThreatQ account.

PARAMETER	DESCRIPTION
Status	This is the default status for objects that are created by this Integration.

Example Output

```
tq-conn-snort-comm-rules v 3 -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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Feed Name	The name of the feed.
Base URL	This is the base URLfor snort community downloads. Do not change this field unless instructed to do so. Changing this parameter may result in SNORT rules not being uploaded.
Versions	This parameter tells the connector which community rules to download. You can set this to **v2**, **v3**, or **both**. Entering **both** will download both the v2 and v3 rules.
Standard Rule Status	This option will determine the status given to the rules that are **not** commented out. When downloaded, the community rules file contains a list of rules. Some of these rules are commented out while others are not.

PARAMETER	DESCRIPTION
Non-Standard Rule Status	This option determines the status given to the rules that **are** commented out. If set to **None**, the connector will not add these (commented out) rules to ThreatQ.

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

Use the following command to execute the driver:

```
<> tq-conn-snort-comm-rules -v3 -ll /var/log/tq_labs/ -c /etc/
   tq_labs/
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
`-h`, `--help`	Shows this help message and exits.
`-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. The default setting is **1** (Warning).
`-ep, --external-proxy`	This allows you to use the proxy that is specified in the ThreatQ UI.

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-snort-comm-rules -c /etc/tq_labs/ -ll /
      var/log/tq_labs/ -v3
   ```

4. Save and exit CRON.

Change Log

- **Version 1.1.1**
  - Added value parameter in order to allow users to default settings without explicitly submitting the form.
- **Version 1.1.0**
  - Added python 3 support.
- **Version 1.0.5**
  - Signatures now related to indicators (CVE).
- **Version 1.0.3**
  - Fixed an issue where bulk uploading of indicators (400+) would cause the connector to stop.
- **Version 1.0.2**
  - Added the ability to change indicator status from the ThreatQ UI.
- **Version 1.0.0**
  - Initial Release