ThreatQuotient for Snort Community Rules Application

October 11, 2019

Version 1.0.5

11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
https://www.threatq.com/
Support: support@threatq.com
Sales: sales@threatq.com

Contents

CONTENTS **2**

LIST OF FIGURES AND TABLES **3**

1 INTRODUCTION **4**

1.1 APPLICATION FUNCTION 4
1.2 PREFACE 4
1.3 AUDIENCE 4
1.4 SCOPE 4
1.5 ASSUMPTIONS 4

2 IMPLEMENTATION OVERVIEW **5**

2.1 PREREQUISITES 5
2.2 SECURITY AND PRIVACY 5

3 THREATQUOTIENT FOR SNORT COMMUNITY RULES APPLICATION APPLICATION INSTALLATION **6**

3.1 SETTING UP THE INTEGRATION 6
3.2 CONFIGURING THE CONNECTOR 8
3.3 CRON 9
3.3.1 Setting Up the CRONJOB *9*

APPENDIX A: SUPPLEMENTARY INFORMATION **10**

UNINSTALLING THE CONNECTOR 10
TQSNORTCOMMRULES COMMAND LINE OPTIONS 10

TRADEMARKS AND DISCLAIMERS **11**

List of Figures and Tables

Figure 1: Time Zone List Example 5
Figure 2: Time Zone Change Example 5
Figure 3: Installing From The ThreatQuotient Repository (Example Output) 6
Figure 4: Installing .whl File (Inc Example Output) 6
Figure 5: Creating Integration Directories (Example) 7
Figure 6: Running the Integration 7
Figure 7: ThreatQ UI Configuration 8
Figure 8: Command Line Crontab Command 9
Figure 9: Command Line Crontab tqSnortCommRules Command 9

Table 1: ThreatQuotient Software & App Version Information 4

1 Introduction

1.1 Application Function

The ThreatQuotient for Snort Community Rules Application downloads and ingests the Snort community rules into the ThreatQ platform. Versions of the Snort rules that can be downloaded and ingested can include both versions or split into versions 2 or 3.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Snort Community Rules Application. This document is not specifically intended as a site reference guide.
It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Snort Engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

1.4 Scope

This document covers the implementation of the ThreatQuotient for Snort Community Rules Application only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Snort Community Rules Application	1.0.5	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for Snort Community Rules Application into the managed estate:

- All ThreatQuotient equipment is online and in service.

2 Implementation Overview

This document will show how to install the ThreatQuotient for Snort Community Rules Application .

2.1 Prerequisites

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time (UTC recommended), time zone and date, 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, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

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

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

2.2 Security and Privacy

For ThreatQuotient Professional Services Engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is strictly confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

3 ThreatQuotient for Snort Community Rules Application Installation

3.1 Setting up the Integration

From the ThreatQuotient Repository

To install the ThreatQuotient for Snort Community Rules Application from the ThreatQuotient repository with YUM credentials, complete the following steps:

1. Install the ThreatQuotient for Snort Community Rules Application by using the following commands.

Figure 3: Installing From The ThreatQuotient Repository (Example Output)

```
sudo pip install -i
https://<USERNAME>:<PASSWORD>@extensions.threatq.com/threatq/integrations
tqSnortCommRules
Downloading https://extensions.threatq.com/threatq/integrations-
dev/+f/9c2/131c319f2bb32/tqSnortCommRules-1.0.3-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): threatqsdk>=1.6.2 in
/usr/lib/python2.7/site-packages (from tqSnortCommRules)
Requirement already satisfied (use --upgrade to upgrade): threatqcc>=1.1.2 in
/usr/lib/python2.7/site-packages (from tqSnortCommRules)
Collecting PySocks==1.6.7 (from tqSnortCommRules)
  Downloading
https://extensions.threatq.com/root/pypi/+f/d00/329f27efa157d/PySocks-1.6.7.tar.gz
(282kB)
    100% |████████████████████████████████| 286kB 4.3MB/s
Requirement already satisfied (use --upgrade to upgrade): requests>=2.9.1 in
/usr/lib/python2.7/site-packages (from threatqsdk>=1.6.2->tqSnortCommRules)
Requirement already satisfied (use --upgrade to upgrade): six>=1.5 in
/usr/lib/python2.7/site-packages (from python-dateutil>=2.6.1->tqSnortCommRules)
Requirement already satisfied (use --upgrade to upgrade): MarkupSafe in
/usr/lib64/python2.7/site-packages (from jinja2==2.8->threatqcc>=1.1.2-
>tqSnortCommRules)
Installing collected packages: PySocks, python-dateutil, tqSnortCommRules
Successfully installed PySocks-1.6.7 python-dateutil-2.7.3 tqSnortCommRules-1.0.5
```

Offline From The .whl File

To install the ThreatQuotient for Snort Community Rules Application from a wheel file, the wheel (.whl) file `tqSnortCommRules-1.0.3-py2-none-any.whl` will need to be copied via SCP into your ThreatQ instance.

1. Install the .whl file using the following command.

Figure 4: Installing .whl File (Inc Example Output)

```
$> sudo pip install /file/path/to/app/tqSnortCommRules-1.0.3-py2-none-any.whl
You are using pip version 7.1.0, however version 9.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Processing ./tqSnortCommRules-1.0.3-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): threatqsdk>=1.6.2 in
/usr/lib/python2.7/site-packages (from tqSnortCommRules==2.0.1)
Requirement already satisfied (use --upgrade to upgrade): threatqcc>=1.1.2 in
Installing collected packages: python-dateutil, tqSnortCommRules
      Successfully uninstalled python-dateutil-2.6.0
Successfully installed python-dateutil-2.7.0 tqSnortCommRules-1.0.5
```

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

Figure 5: Creating Integration Directories (Example)

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

A driver which will be called `tqSnortCommRules` is installed.

2. Issue the following commands to initialize the integration.

   You will be asked the following questions:

   a. **ThreatQ Host:** This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
   b. **Client ID:** This is the OAuth id that can be found at **Gear** > **OAuth Management**.
   c. **E-mail Address:** This is the *user in the ThreatQ System* for integrations.
   d. **Password:** The password for the above ThreatQ account
   e. **Status:** This is the default status for IoCs that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

Figure 6: Running the Integration

```
$>tqSnortCommRules -c /file/path/to/config/ -ll /file/path/to/logs/ -v3
ThreatQ Host: <IP ADDRESS>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured.  Set information in UI.please use UI for final configuration
```

The driver will run once, where it will connect to the TQ instance and install the user interface component of the connector.

3.2 Configuring the connector

Once the steps from the previous section are complete, access the ThreatQ user interface and navigate to **Settings > Incoming Feeds** > **ThreatQ Labs** and find the *Snort Community Rules* feed. The configuration is auto-completed but can be changed if required.

The following information will need to be entered as described below.

1. **Feed Name**: This is the name of the feed.
2. **Base URL**: This is the base URL for snort community downloads.

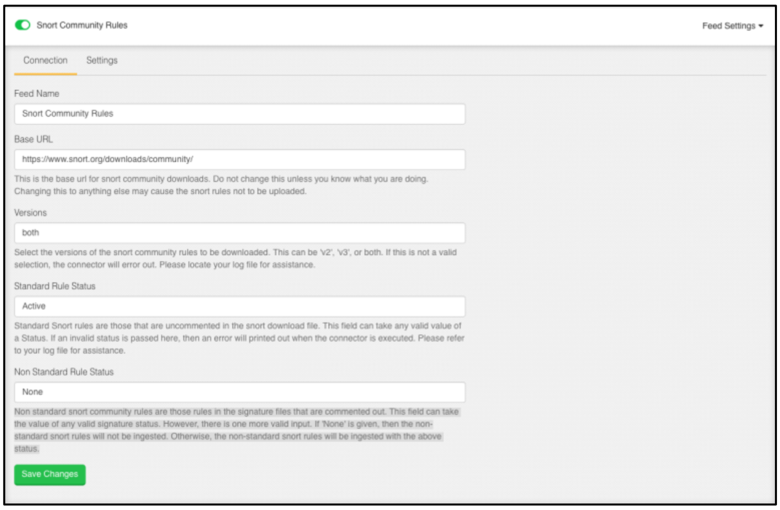
   ⚠ Do not change the base URL unless you know what you are doing. Changing this to anything else may cause the snort rules not to be uploaded.
3. **Versions**: **Both** is Default. Select the versions of the snort community rules to be downloaded. This can be 'v2', 'v3', or both.

   If this is not a valid selection, the connector will error out. Please locate your log file for assistance.
4. **Standard Rule Status**: Standard Snort rules are those that are uncommented in the snort download file. This field can take any valid value of a Status.

   If an invalid status is passed here, then an error will be printed out when the connector is executed. Please refer to your log file for assistance.
5. **Non-Standard Rule Status**: Non-standard snort community rules are those rules in the signature files that are commented out. This field can take the value of any valid signature status. However, there is one more valid input.

   If 'None' is given, then the non-standard snort rules will not be ingested. Otherwise, the non-standard snort rules will be ingested with the above status.
6. Click the **Save Changes** and ensure that the toggle next to the name of the integration is enabled (Showing Green).

Figure 7: ThreatQ UI Configuration



Feed Name
Snort Community Rules

Base URL
https://www.snort.org/downloads/community/
This is the base url for snort community downloads. Do not change this unless you know what you are doing. Changing this to anything else may cause the snort rules not to be uploaded.

Versions
both
Select the versions of the snort community rules to be downloaded. This can be 'v2', 'v3', or both. If this is not a valid selection, the connector will error out. Please locate your log file for assistance.

Standard Rule Status
Active
Standard Snort rules are those that are uncommented in the snort download file. This field can take any valid value of a Status. If an invalid status is passed here, then an error will printed out when the connector is executed. Please refer to your log file for assistance.

Non Standard Rule Status
None
Non standard snort community rules are those rules in the signature files that are commented out. This field can take the value of any valid signature status. However, there is one more valid input. If 'None' is given, then the non-standard snort rules will not be ingested. Otherwise, the non-standard snort rules will be ingested with the above status.

Once completed, the integration is ready for operation.

3.3 CRON

To run this script on a reoccurring basis use CRON or some other system schedule. The argument in the cron script ***must*** specify the config and log locations.

This can be run multiple times a day and should not be run more often than once per hour.

3.3.1 Setting Up the CRONJOB

1. Login via a CLI terminal session to your ThreatQ host.
2. Input the commands below.

   Figure 8: Command Line Crontab 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. Input the commands below – this example shows every **4 Hours.**

   Figure 9: Command Line Crontab tqSnortCommRules Command

   ```
   0 */4 * * * $> tqSnortCommRules -c /path/to/config/directory/ -ll
   /path/to/log/directory/ -f /path/to/files/directory --files files/
   ```

   To run this script on a reoccurring basis use CRON or some other on system schedule. Here is shown CRON.

   The argument in the cron script ***must*** specify the config and log locations.

   This can be run multiple times a day and should **not** be run more often than once per hour.

For further reference, see the ThreatQ Help Center.

Appendix A: Supplementary Information

Uninstalling the Connector

```
sudo pip uninstall tqSnortCommRules
```

tqSnortCommRules command line options

The `tqSnortCommRules` Driver has several command line arguments that will help you and your customers execute this. They are listed below. You can see these by executing `/usr/bin/tqSnortCommRules --help.`

```
usage: tqSnortCommRules Connector [-h] [-ll LOGLOCATION][-c CONFIG] [-v VERBOSITY]
```

```
tqSnortCommRules
```

optional arguments:

```
  -h, --help
```

Shows the help message and exit

```
  -ll LOGLOCATION, --loglocation LOGLOCATION
```

This sets the logging location for this connector. The location should exist and be writable by the current user. 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 have read and write permissions for the current user. If no config file is given, the current directory will be used. This file is also where some information from each run of the connector may be put (e.g. 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).

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.