ThreatQuotient

ThreatQuotient for Snort Subscription Rules

Version 1.0.0

Monday, July 9, 2019

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

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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.

Last Updated: Tuesday, July 9, 2019

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for Snort Subscription Rules Connector allows a ThreatQ and Snort user to import signatures and indicators from the Snort registered/subscription rulesets.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Snort Subscription 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 the ThreatQuotient Apps and integrations covered within the document, as well as the 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 Subscription Rules Connector only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Snort Subscription Rules Connector	1.0.0	

1.5 Assumptions

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

1. All ThreatQuotient equipment is online and in service.

2 Implementation Overview

This document explains how to install the ThreatQuotient for Snort Subscription Rules Connector.

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 Subscription Rules Application Installation

3.1 Setting up the Integration

From the ThreatQuotient Repository

To install the ThreatQuotient for Snort Subscription Rules Application from the ThreatQuotient repository with YUM credentials.

1. Install the ThreatQuotient for Snort Subscription Rules Connector by using the following commands:

Figure 3: Installing from the ThreatQuotient Repository (Example Output)

```
$> pip install tq-conn-snort-subscription-rules
Collecting tq-conn-snort-subscription-rules
  Downloading https://extensions.threatq.com/threatq/integrations-
dev/+f/e7b/7112897638161/ tq-conn-snort-subscription-rules-1.0.0-py2-none-any.whl
Requirement already satisfied: jinja2==2.8 in /usr/lib/python2.7/site-packages
(from threatqcc>=1.3.0-> tq-conn-snort-subscription-rules) (2.8)
Collecting pyasn1>=0.3.7 (from python-ldap==3.2.0-> tq-conn-snort-subscription-
rules)
  Downloading https://extensions.threatq.com/root/pypi/+f/da6/b43a8c9ae93bc/pyasn1-
0.4.5-py2.py3-none-any.whl (73kB)
    100% |████████████████████████████████| 81kB 1.0MB/s
Collecting pyasn1_modules>=0.1.5 (from python-ldap==3.2.0-> tq-conn-snort-
subscription-rules)
  Downloading
  Running setup.py install for python-ldap ... done
Successfully installed pyasn1-0.4.5 pyasn1-modules-0.2.5 python-ldap-3.2.0 tq-conn-
snort-subscription-rules-1.0.0
```

Offline from the .whl File

To install this ThreatQuotient for Snort Subscription Rules Connector from a wheel file, the wheel file (.whl) file `tq-conn-snort-subscription-rules-<version>-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/tq-conn-snort-subscription-rules-<version>-
py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): urllib3<1.25,>=1.21.1 in
/usr/lib/python2.7/site-packages (from requests>=2.9.1->threatqsdk>=1.6.7-> tq-conn-
snort-subscription-rules)
Requirement already satisfied (use --upgrade to upgrade): chardet<3.1.0,>=3.0.2 in
/usr/lib/python2.7/site-packages (from requests>=2.9.1->threatqsdk>=1.6.7-> tq-
conn-snort-subscription-rules)
Requirement already satisfied (use --upgrade to upgrade): idna<2.9,>=2.5 in
/usr/lib/python2.7/site-packages (from requests>=2.9.1->threatqsdk>=1.6.7-> tq-
conn-snort-subscription-rules)
Installing collected packages: tq-conn-snort-subscription-rules
Successfully installed tq-conn-snort-subscription-rules-1.0.0
```

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

Figure 5: Creating Integration Directories (Example)

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

A driver called `tq-conn-snort-subscription-rules` 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 refers to the API credentials that can be found at the **User icon** > **My Account**.
   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 status.

Figure 6: Running the Integration

```
$> tq-conn-snort-subscription-rules -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 ThreatQ instance and install the user interface component of the connector.

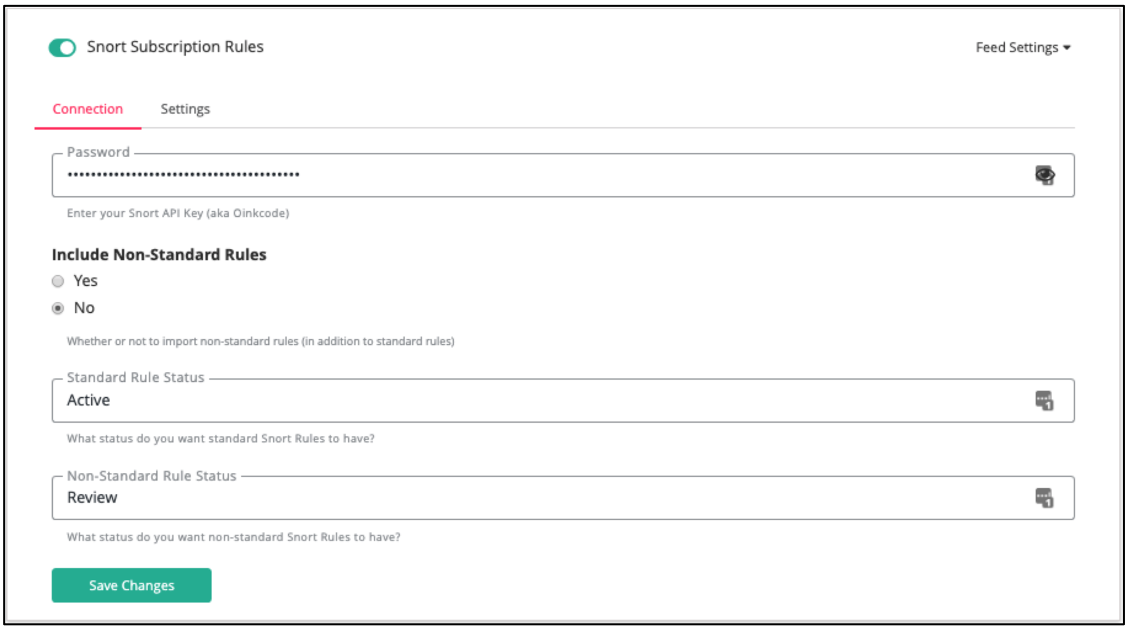
3.2 Configuring the Connector

Once the steps from the previous section are complete, access the ThreatQ user interface and navigate to the **Settings icon** > **Incoming Feeds** > **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. API Key (Oinkcode): Enter your Snort API Key (aka Oinkcode).
2. Include Non-Standard Rules: Whether or not to import non-standard rules
   - This is in addition to the standard rules
3. Standard Rule Status: The status you want to give to the Snort standard rules.
4. Non-Standard Rule Status: The status you want to give to the Snort non-standard rules.

Figure 7: ThreatQ UI Configuration



Snort Subscription Rules

Password: ••

Enter your Snort API Key (aka Oinkcode)

Include Non-Standard Rules

○ Yes

● No

Whether or not to import non-standard rules (in addition to standard rules)

Standard Rule Status: Active

What status do you want standard Snort Rules to have?

Non-Standard Rule Status: Review

What status do you want non-standard Snort Rules to have?

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 connector is slightly different from other connectors as it uses some custom command line arguments.

The connector 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 tq-conn-snort-subscription-rules Command

```
0 */4 * * * tq-conn-snort-subscription-rules -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. CRON is shown here.

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

The connector 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 tq-conn-snort-subscription-rules
```

Command line options

The `tq-conn-snort-subscription-rules` driver has several command line arguments that will help you and your customers execute it. They are listed below. You can see these by executing `/usr/bin/tq-conn-snort-subscription-rules --help.`

```
usage: tq-conn-snort-subscription-rules Connector [-h] [-ll LOGLOCATION][-c CONFIG]
[-v VERBOSITY]
```

`tq-conn-snort-subscription-rules`
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 SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING 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 TERMS AND CONDITIONS WHEN PURCHASED. 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.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

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.