ThreatQuotient

Proofpoint ET Signatures Connector Guide

Version 2.0.0

Friday, May 8, 2020

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

- Integration Version: 2.0.0
- ThreatQ Version: 4.16.0 or greater

Introduction

The ThreatQuotient for Proofpoint Signatures ET (Community) Application is a uni-directional connector that pulls information from the Emerging Threats rules base and then uploads the snort signatures into the ThreatQ instance.

Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for Emerging Threats Signatures (Community) Application into the managed estate:

- All ThreatQuotient equipment is online and in service.
- Infrastructure/transmission at all sites and between sites is in place to support the network traffic.
- All required firewall ports have been opened.
- All equipment is powered from permanent power supplies.
- A clock source of sufficient accuracy is connected to the network and the network and devices are using it as the primary clock source.

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.

Prerequisites

Throughout this implementation document, there will be referrals 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, time zone and date, and using a clock source available to all.

- ThreatQ version 4.16.0+
- EmergingThreats Pro Oinkcode for ETPro rules (https://etadmin.proofpoint.com/etpro)
- Ensure all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

An example of setting the ThreatQ device to the correct time is shown below.

```
sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

> ***Note:*** *The Emerging Threats Pro Oinkcode is only required to download pro rules. If you're not downloading pro rules, you can skip this prerequisite.*

Installation

> ***Note:*** *Users upgrading from version 1.0.0 should see the Upgrading from v1.0.0 section before attempting to upgrade the connector.*

Ensure the file tq_conn_emerging_threats-2.0.0-py2-none-any.whl has been added to the ThreatQ instance or that the ThreatQ instance has internet connectivity, where the yum credentials will need to be used as below.

Install Methods

The connector can be installed using the following methods:

- via ThreatQ Repository
- via .whl File

via ThreatQ Repository

1. Run the following command:

```
pip install -i

https://<USERNAME>:<PASSWORD>@extensions.threatq.com/threatq/integrati

ons tq_conn_emerging_threats
```

via .whl File

1. Run the following command:

```
pip install tq_conn_emerging_threats-2.0.0-py2-none-any.whl
```

Directory Structure

Once the application has been installed, a directory structure, using the `mkdir` command, must be created for all configurations, logs and files.

See example below:

```
mkdir -p /opt/tq-integrations/EmTS

mkdir -p /opt/tq-integrations/EmTS/config

mkdir -p /opt/tq-integrations/EmTS/logs

cd /opt/tq-integrations/EmTS/
```

A driver called **tq-conn-emerging-threats** is installed.

Initializing the Integration

Issue the following commands to initialize the integration:

```
tq-conn-emerging-threats -c /opt/tq-integrations/EmTS/config/ -ll


/opt/tq-integrations/EmTS/logs/ -v3
```

Enter the following information when prompted:

Parameter	Description
ThreatQ Host	ThreatQ Hostname or IP Address.
Connector Name	Emerging Threats ***Note:*** *This prompt is auto-filled.*
Client ID	The Client ID can be found within the ThreatQ instance, under **User Bubble > My Account > API Credentials**.
E-mail Address	ThreatQ account associated with the Emerging Threats integration.
Password	ThreatQ account password associated with the Emerging Threats integration.
Status	Active

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

Configuration

Note: *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.*

To configure the connector:

Note: *Confirm that you have completed the Initializing the Integration steps before proceeding.*

1. Log into your ThreatQ instance.
2. Click on the **Settings** icon and select **Incoming Feeds**.
3. Locate the connector under the **Labs** tab.
4. Click on the **Feed Settings** link for the connector.
5. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
ET Pro Oinkcode	This is the oinkcode provided by ETPro. You can get your key are: https://etadmin.proofpoint.com/etpro ***Note:*** *This is only required if you are downloading the ET Pro Ruleset.*
Rulesets	These are the rulesets that the connector will import. ***Note:*** *Hold shift and click to select multiple rules.*
Include Non-Standard Rules *(Yes/No radio options)*	This will import the non-standard rules as well as the standard ones that will be imported by default.
Standard Rule Status	This is the status that will be set for the standard rules when they get imported. Must be one of the following: • Active • Expired • Inactive • Non-Malicious

Parameter	Description
	• Review • Whitelisted
Non-Standard Rule Status	This is the status that will be set for the non-standard rules when they get imported. Must be one of the following: • Active • Expired • Inactive • Non-Malicious • Review • Whitelisted

6. Click on **Save Changes**.
7. Click on the toggle switch to the left of the connector name to enable the connector.

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 at the top of every 4 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 4 Hours Example

```
0 */4 * * * tq-emergingthreats -c /opt/tq-integrations/EmTS/config/ -

ll /opt/tqintegrations/EmTS/logs/ -v3
```

4. Save and exit cron.

Notes:

- Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.
- The argument in the cron script must specify the config and log locations.
- Cron can be run multiple times a day but should not run more frequently than once an hour.

Upgrading from v1.0.0

Upgrading the app from v1.0.0 to v2.0.0 requires additional steps as the package names have been updated.

1. Uninstall the app using the following command:

```
pip uninstall tqEmergingThreats
```

2. Remove the old configuration file.

   Note: Removing the old logs or renaming them are necessary to configure the new version of the connector.

3. Install version 2.0.0 as described in the Installation section of the guide.
4. Configure the connector using the steps described in the Configuration section.

Change Log

Version	Details
2.0.0	Updates: • Includes the option for standard and non-standard rules • Includes the ability to set a different status for standard and non-standard rules Includes the ability to download your choice of Open rules, block rules and/or ET Pro rules • Imports Suricata rules as well as snort
1.0.0	Initial Release