ThreatQuotient

Proofpoint TAP Connector Guide

Version 1.2.0

Friday, January 15, 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: 1.2.0
- Supported on ThreatQ versions: 4.3 or greater

Support Matrix

Operating System	OS Version	Python Version	Notes
RedHat/CentOS	7	2.7.12	N/A
Ubuntu	16.04	2.7.12	This has not been tested.
Windows	2012R2/10	2.7.12	This has not been tested.

Introduction

Proofpoint TAP is a service that analyzes, detects and helps mitigate attacks that target people via email. The analysis data for each email that has been flagged as malicious by TAP is available via their API. The API provides multiple endpoints, of which we use the following:

SIEM

The SIEM endpoint allows integration with these solutions by giving administrators the ability to periodically download detailed information about several types of TAP events in a SIEM-compatible, vendor-neutral format. Currently, the following event types are exposed:

- Blocked or permitted clicks to threats recognized by URL Defense
- Blocked or delivered messages that contain threats recognized by URL Defense or Attachment Defense

Campaign

The Campaign endpoint allows administrators to pull specific details about campaigns, including:

- Their description
- The actor, malware family, and techniques associated with the campaign
- The threat variants which have been associated with the campaign

Forensics

The Forensics endpoint allows administrators to pull detailed forensic evidences about individual threats or campaigns observed in their environment. These evidences could be used as indicators of compromise to confirm infection on a host, as supplementary data to enrich and correlate against other security intelligence sources, or to orchestrate updates to security endpoints to prevent exposure and infection.

Installation

The connector can be installed from the ThreatQ integrations repository.

Perform the following steps to install the connector:

1. Install the connector using the following command:

```
pip install tq-conn-proofpoint-tap
```

   To install the connector from a .whl file, download the connector, and all of its dependencies, using the following command

```
pip download tq_conn_proofpoint_tap -d /tmp/distro/
```

   Copy the downloaded files, via SCP, to your ThreatQ instance. After completing that step, run the following command:

```
pip install tq_conn_proofpoint_tap-*-py2-none-any.whl
```

Once the connector is installed, a directory structure must be created for configuration, logs, and files.

   A driver called `tq-conn-proofpoint-tap` is installed.

2. Perform the following commands:

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

3. Perform the initial run using the following command:

```
tq-conn-proofpoint-tap -v3 -ll /etc/tq_labs -c /var/log/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. The recommended entry is **127.0.0.1.**
ThreatQ CID (Client ID)	This is the OAuth ID that can be found under a user's ThreatQ profile by navigating to the Systems gear icon > User Management and clicking on the user.
Email Address	The username that you use to login to ThreatQ.

Parameter	Description
Password	The password associated with the username above.
Status	The default status for IoCs that are created by this integration. It is common to set this to **Active** but organization SOPs should be respected when setting this field.

The connector will now appear on the integrations page in your ThreatQ instance. You will still need to configure and enable the connector.

Configuration

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

To configure the feed:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the Category dropdown (optional).
3. Click on the connector to open its details page.
4. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
API Host	The hostname or IP address of the Proofpoint TAP API.
API Principal	The principal provided for the API.
API Secret	The secret provided for the API.
Number of hours to pull data from history	An integer representing a historical time window, in hours, to pull data from the SIEM all endpoint. ***Note:*** *The max historical timeframe is 24 hours.*

5. Click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Usage

Once the connector is installed to the ThreatQ UI and enabled, you will re-run the Initial Configuration command in order to kick off the integration.

Note: *Once the integration successfully completes, you will need to setup a CRON-job for it so it can run on a schedule.*

```
tq-conn-proofpoint_tap -ll /etc/tq_labs/ -c /var/log/tq_labs/ -v
<verbosity_level>
```

Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
`-h`, `--help`	Shoes the help message and exits.
`-v`	Sets the log verbosity (3 means everything).
`-c`	The path to the directory where you want to store your config file.
`-ll`	The path to the directory where you want to store your logs.
`-ep`, `--external-proxy`	This allows you to use the proxy that is specified in the ThreatQ UI.
`-ds`, `--disable-ssl`	Adding this flag will disable SSL verification when contacting the Metron API.

Note: *All location-based options default to the current working directory if they are not provided. To find additional options and option descriptions, simply 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 at the top of every hour.

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. To execute the connector at a scheduled frequency, you can configure a CRON entry to run the connector. Depending on how quickly you want updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

   Hourly Example

```
0 * * * * tq-conn-proofpoint_tap -c /etc/tq_labs/ -ll
/var/log.tq_labs/ -v VERBOSITY_LEVEL
```

4. Save and exit cron..

Uninstalling the Connector

Run the following command to uninstall the connector:

```
sudo pip uninstall tq-conn-proofpoint-tap
```

Change Log

Version	Details
1.2.0	• Added the ability to open incident response tickets if the user has requested it via the ThreatQ UI.
1.1.0	• Improved exception handling • Optimized API calls to Proofpoint TAP
1.0.0	Initial Release