ThreatQuotient

Cisco Threat Response Enrichment Guide

Version 1.0.0

Thursday, June 4, 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: `1.0.0`
- ThreatQ Version: `4.20.0 or greater`

Introduction

The Cisco Threat Response Enrichment Integration for ThreatQ allows a user to bulk enrich indicators from ThreatQ using context from Cisco Threat Response.

Notes:

- The first run will enrich all indicators found in the saved search. Each consecutive run will only enrich newly created/updated indicators found in the saved search.
- Not all indicators will be enriched. Some indicators may not have context found for it in Cisco Threat Response.
- The default status will be applied to any indicator that enrichment context is found for.

Prerequisites

The Cisco Threat Response Python Module requires requests>=2.22.0. Due to this requirement, a virtual environment must be created before this integration to be installed.

Perform the following steps:

- Install python 2.7 virtual environment

```
pip install virtualenv==16.7.10
```

- Create a virtual environment for this integration

```
mkdir -p /etc/tq_labs/ctr-enrichment-env/
```

```
virtualenv --no-setuptools -p /usr/bin/python2.7

/etc/tq_labs/ctr-enrichment-env/
```

- Activate the virtual environment

```
source /etc/tq_labs/ctr-enrichment-env/bin/activate


pip install setuptools==44.0.0
```

- Continue with installation via the .whl file or repository

Installation

Confirm that you have completed the steps listed in the Prerequisites section before attempting to install the connector,

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 tq-conn-ctr-enrichment
```

via .whl File

1. Run the following command:

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

First Run

After installing the connector, you will need to run it for the first time, manually. This will install the connector into the ThreatQ UI so it can be configured.

- Create a directory for the integration

```
mkdir -p /etc/tq_labs/
```

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

- Run the Integration:

```
/etc/tq_labs/ctr-enrichment-env/bin/tq-conn-ctr-enrichment -v 3

-ll /var/log/tq_labs/ -c /etc/tq_labs/
```

- Enter the following information when prompted:

Field	Description
ThreatQ Host	The hostname or IP of your ThreatQ instance.
E-Mail Address	The email address you use to login to ThreatQ.
Password	The password used with the email address.
Status	The default status for the indicators brought in by the connector. The status selected here for all indicators with enrichment context.

The connector will now appear in the ThreatQ UI under the **Labs** tab for Incoming Feeds. Proceed to the Configuration section.

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:

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

Parameter	Description
Region	The region of the API you will be using.
Client ID	Your Cisco Threat Response API Client ID
Client Password	Your Cisco Threat Response API Client Password.
Saved Search Name (Threat Library)	The name for a saved search from your Threat Library. The indicators from this search will be sent to Cisco Threat Response for enrichment.

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

Usage

The connector has CLI argument that can be included for historical imports.

```
/etc/tq_labs/ctr-enrichment-env/bin/tq-conn-ctr-enrichment -v 3

-ll /var/log/tq_labs/ -c /etc/tq_labs/
```

Advanced Usage

For the integration's first run, all indicators in the saved search will be sent to Cisco Threat Response for enrichment. Each consecutive run will then only send updated indicators since the last time the integration ran. If you want to send indicators that have been created/updated since an earlier date, you can use the `--historical` CLI flag.

With this option, you can specify a date to download reports since. It must be in the 'YYYY-MM-DD' format. The below example will import all reports since January 1st, 2019.

```
etc/tq_labs/ctr-enrichment-env/bin/tq-conn-ctr-enrichment -v 3 -

ll /var/log/tq_labs/ -c /etc/tq_labs/ --historical 2020-01-01
```

CRON

Since the connector was installed in a separate virtual environment from the base python environment, the CRON-job must be configured to use that path.

Use the following path: `/etc/tq_labs/ctr-enrichment-env/bin/tq-conn-ctr-enrichment` as the executable path. Then configure the schedule and CLI parameters as needed.

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. Save and exit cron.

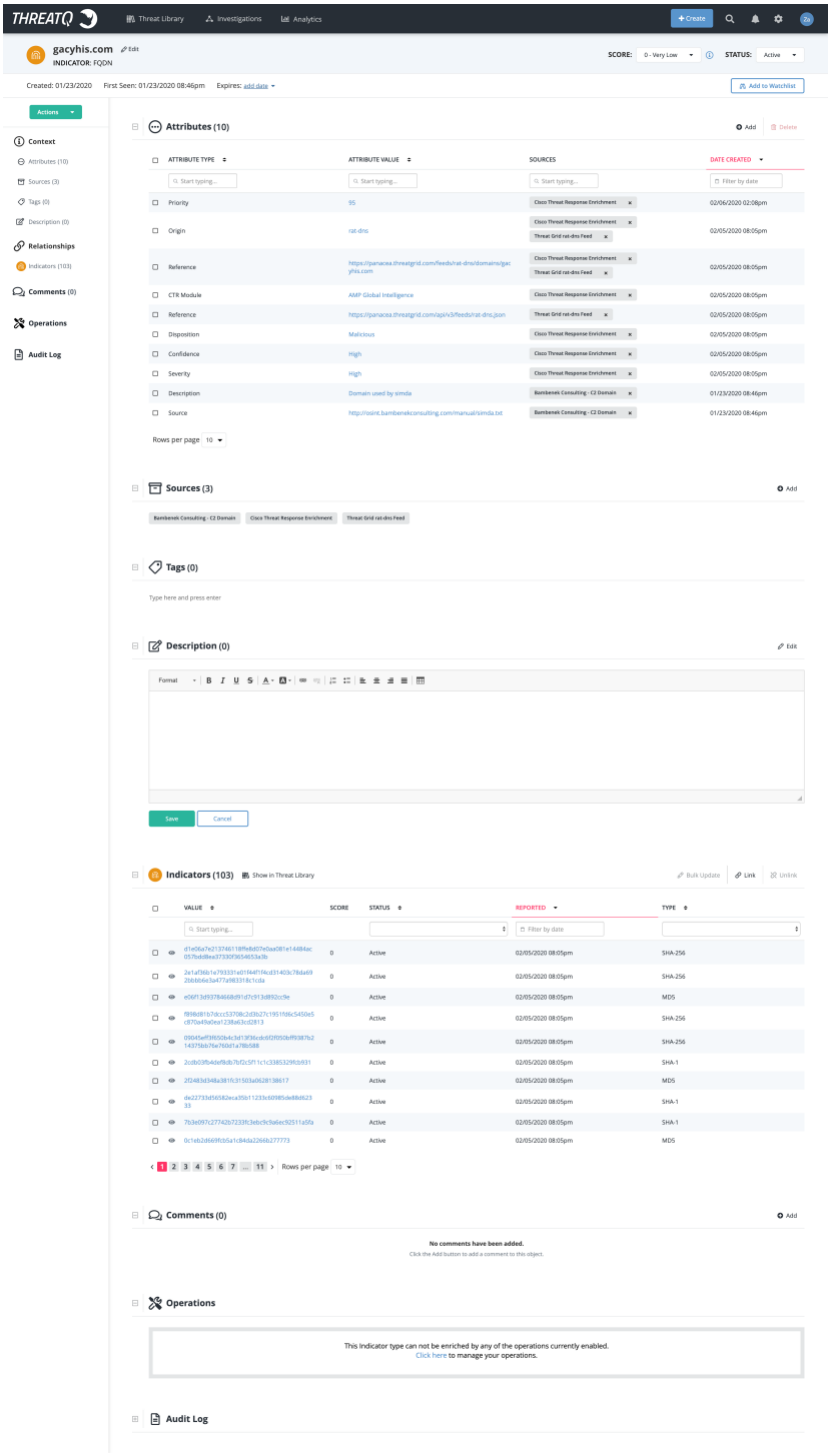
Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
`-v` (Required)	Sets the log verbsity (3 means everything).
`-c` (Required)	The path to the directory where you want to store your config file.
`-ll` (Required)	The path to the directory where you want to store your logs.
`-hist, --historical [date]`	This argument will allow you to run a "historical" export. It will look for updated incidents after the supplied date. **Example:** [-hist [YYYY-MM-DD]]
`-n --name [connector name]`	This argument allows you to install the connector with a custom name This argument is mainly used when you want to install multiple instances of the connector. For instance, if you have multiple saved searches that you want exported. You can simply setup a new instance of this connector with a new name, for a new saved search

Usage Example

Enrichment result examples in ThreatQ.



Change Log

Version	Details
1.0.0	Initial Release