ThreatQuotient

Cisco Threat Response Exporter 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 or greater`

Introduction

The Cisco Threat Response Exporter for ThreatQ allows a ThreatQ user to export indicator/observable judgements from ThreatQ to Cisco Threat Response via the Cisco Threat Intelligence API (CTIA)

Notes:

- Due to an API limitation, the CTIA (Cisco Threat Intelligence API) will only allow TLP amber and/or red. As a result, all indicators being sent over to Cisco AMP will receive an Amber TLP (unless TLP red is applied in ThreatQ)
- This integration will push judgements to your organization's private instance. This will not publish information to Cisco's public sources

Installation

The Cisco Threat Response Exporter must be installed using one of the two methods listed below and then run manually in order for the integration to be accessible via the ThreatQ UI.

Install Methods

The integration 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-exporter
```

via .whl File

1. Run the following command:

```
pip install tq_conn_ctr_exporter-*-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.

```
tq-conn-ctr-exporter  -v 3 -ll stdout
```

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 (generated via your profile).
API Password	Y our Cisco Threat Response API Client Secret associated with your Client ID.
Saved Search Name (Threat Library)	The name of the saved search from the Threat Library. **Note:** The indicators found in this saved search will have their context sent to Cisco AMP Threat Response.
Default Disposition	The default disposition to give to observables/indicators added to Cisco AMP.
Default Confidence	The default confidence to give to observables/indicators added to Cisco AMP.
Default Severity	The default severity to give to observables/indicators added to Cisco AMP.
Default Priority	The default disposition to give to observables/indicators added to Cisco AMP **Note:** This must be a number in between 0 and 100
Default Expiration	The default expiration to give to observables/indicators added to Cisco AMP if they do not have one set by ThreatQ

Parameter	Description
	Options include: • 2 Weeks • 1 Month • 6 Months • 1 Year • 5 Years • Never
ThreatQ Hostname/IP Address	The hostname/IP of the ThreatQ instance so that we can link back to it in the Cisco AMP UI.

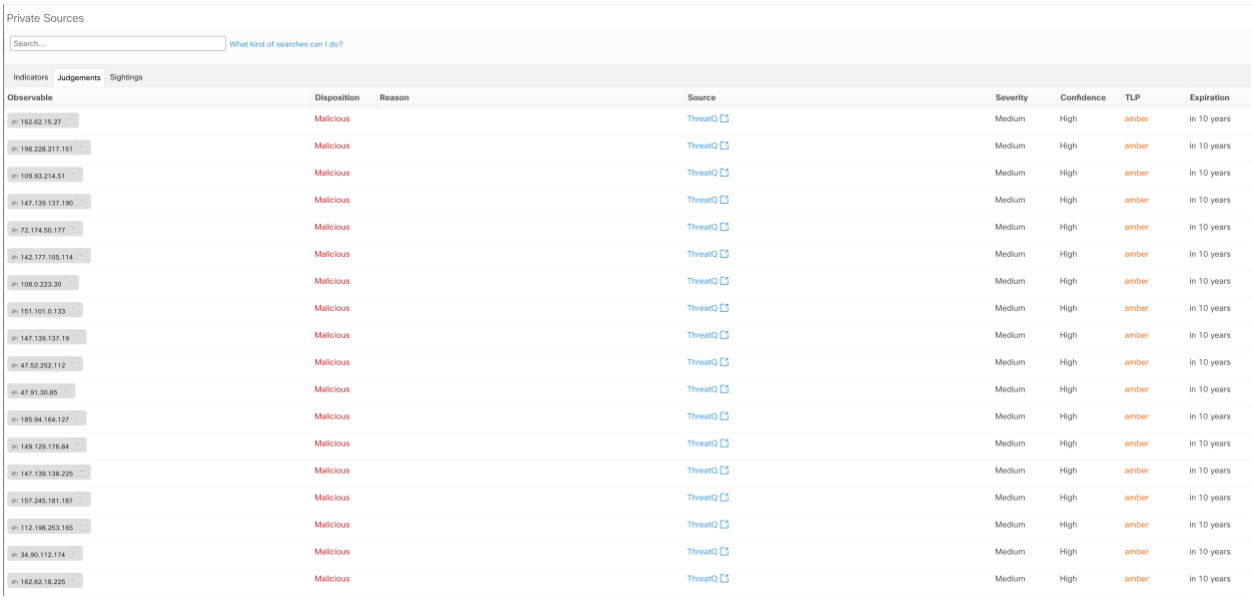
5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the connector name to enable the connector.

Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
`-hist, --historical [date]`	This argument will allow you to run a "historical" export. It will look for updated incidents after the supplied date.
`-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



Change Log

Version	Details
1.0.0	Initial Release