ThreatQuotient

Extrahop Connector Guide

Version 1.0.0

Monday, November 9, 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

Warning and Disclaimer 2

Contents 3

Versioning..4

Introduction 5

Installation 6

Configuration 7

Usage...8

Command Line Arguments.. 8

CRON 9

Change Log 10

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions: 4.0.0 or greater

Introduction

The Extrahop Connector for ThreatQ integration allows a user to export indicators directly to Extrahop via Extrahop's REST API.

The indicator types pushed to Extrahop are:

- FQDN
- URL
- IP Address
- IPv6 Address

Installation

Perform the following steps to install the connector:

1. Modify the pip.conf file in your environment as follows:

```
[global]
   index-url = https://system-updates.threatq.com/pypi
   extra-index-url =
https://<username>:<password>@extensions.threatq.com/threatq/int
egrations

https://<username>:<password>@extensions.threatq.com/threatq/sdk
```

2. Install the connector using the following command:

```
pip install tq_conn_extrahop
```

Once the connector is installed, you will need to run the integration once in order to create the UI configuration within ThreatQ.

3. Perform the initial run using the following command:

```
tq-conn-extrahop -ll <log_location> -c <tq_config_location> -n
<connector_name> -v <verbosity_level>
```

Note: *See the Command Line Arguments chapter for command options.*

4. Enter the following parameters when prompted:

Parameter	Description
ThreatQ Host	The hostname or IP of your ThreatQ instance
ThreatQ CID (Client ID)	Your ThreatQ Client ID.
ThreatQ Username	The username that you use to login to ThreatQ.
ThreatQ Password	The password associated with the username above.

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. Click on the connector to open its details page.
3. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
Extrahop Hostname	The Extrahop instance hostname or IP address.
Extrahop API Key	The Extrahop API Key.
Saved Search Name (Threat Library)	The ThreatQ Threat Library saved search that you want IOCs to be exported from.

4. Click on **Save**.
5. Click on the toggle switch to the left of the integration name 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-extrahop -ll <log_location> -c <tq_config_location> -n
<connector_name> -v <verbosity_level>
```

Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
`-v` (optional)	Sets the log verbosity (3 means everything).
`-c` (optional)	The path to the directory where you want to store your config file.
`-ll` (optional)	The path to the directory where you want to store your logs.
`-n`, `--name` (optional)	Name of the connector. This option can be used in order to allow users to configure multiple Extrahop connector instances on the same TQ instance.

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 * * * * /usr/bin/tq-conn-extrahop -c
/path/to/config/directory/ -ll /path/to/log/directory/ -v
VERBOSITY_LEVEL
```

4. Save and exit cron..

Change Log

Version	Details
1.0.0	Initial Release which includes: • Export indicators from a Threat Library saved search to Extrahop. • Upload batching and retry capabilities.