ThreatQuotient

VMware Carbon Black Cloud Enterprise EDR Connector Guide

Version 1.0.0

Friday, May 15, 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.

Last Updated: Friday, May 15, 2020

Contents

Versioning

- Current Integration Version: `1.0.0`
- Supported on ThreatQ Version: >= `4.25.0`

Introduction

The VMware Carbon Black Cloud Enterprise EDR Connector allows a user to export prioritized threat intelligence from ThreatQ into reports within Carbon Black Threat Hunter. Carbon Black Threat Hunter will match endpoint activity to the threat intelligence from ThreatQ and generate alerts.

Installation

The connector can be installed in one of two methods:

- Via ThreatQ Repository
- Via .whl File

Via ThreatQ Repository

Run the following command:

```
pip install tq-conn-cb-threat-hunter
```

Via .whl File

Run the following command:

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

Configuration

The connector must first initially be configured and manually run in order for to UI configuration portion to be installed on the ThreatQ platform. After this has been completed, the UI portion of the connector configuration must be completed.

Initial Configuration

1. Create a directory for the connector using the following commands:

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

> This step can be skipped if these directories already exist.

2. Run the connector for the first time using the following command:

```
tq-conn-cb-threat-hunter -v 3 -ll /var/log/tq_
labs/ -c /etc/tq_labs/
```

3. Complete the following fields when prompted:

Field	Details
ThreatQ Host	Your ThreatQ Host.
ThreatQ CID	Your ThreatQ Client ID
ThreatQ Username	Your ThreatQ User name
ThreatQ Password	Your ThreatQ user password.
Status	The default status that will be assigned to indicators.

4. The UI configuration portion will be now installed on the ThreatQ platform.

UI Configuration

> 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 feed:

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

Parameter	Description
Threat Hunter API FQDN	The FQDN to access Threat Hunter's API. Default setting is `defense.-conferdeploy.net`

Parameter	Description
API ID	Your Threat Hunter API ID for authentication.
API Secret Key	Your Threat Hunter API Secret Key for authentication.
Organization Key	Your Threat Hunter Organization Key for authentication.
Saved Search Names (Threat Library)	Comma-separated list of Threat Library search names you want to export.
Report Tags	Comma-separated list of tags to add to the reports. These tags will be added to each report.
ThreatQ Hostname or IP Address	This is the hostname or IP address of your ThreatQ instance.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed 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. Once the integration successfully completes, a CRONjob will need to be created in order for the connector to run on a schedule.

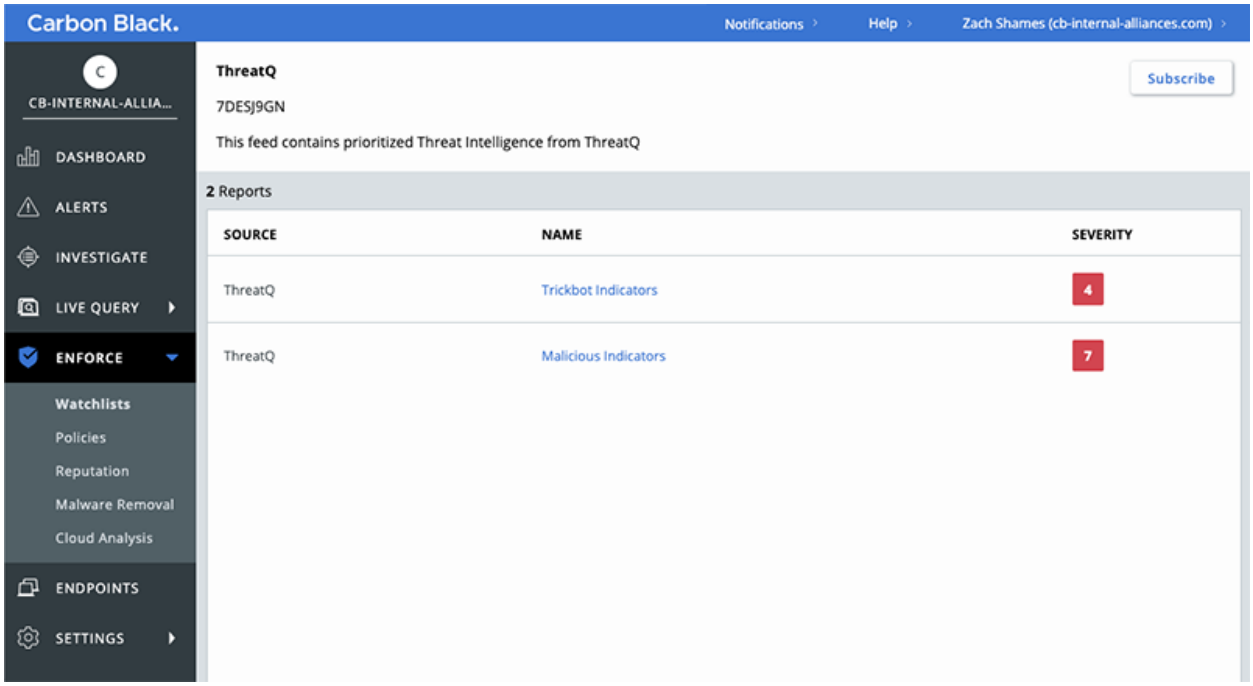
1. Run the `Initial Configuration` command:

```
tq-conn-cb-threat-hunter -v 3 -ll /var/log/tq_
labs/ -c /etc/tq_labs/
```

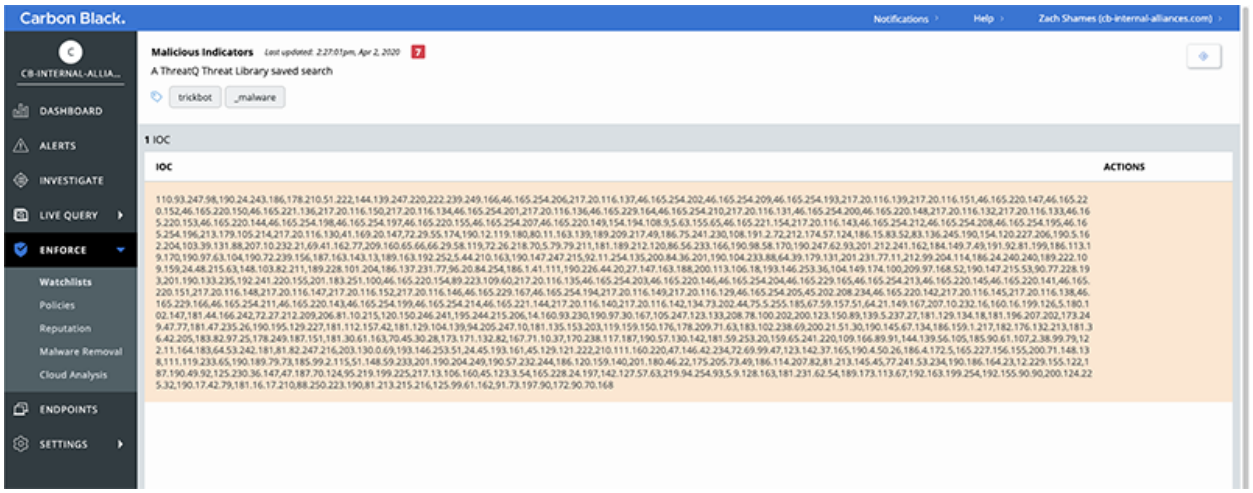
Optional Arguments:

Argument	Description
`-ll`	**Required -** The path to the directory where you want to store your logs.
`-c`	**Required -**The path to the directory where you want to store your config file
`-n, --name`	Change the name of the connector.
`-v`	**Required -** Sets the log verbosity (3 means everything)

Feed Reports Example



Single Report Example



CRON

To run this script on a reoccurring basis use CRON or some other system schedule. The argument in the cron script must specify the config and log locations.

This can be run multiple times a day and can be run as often as required.

Setting Up the CRONJOB

Use CRON or some other on system schedule to run this script on a reoccurring basis.

> The argument in the cron script must specify the config and log locations.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following commands:

   ```
   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:

   4 Hour Example

   ```
   0 */4 * * * tq-conn-cb-threat-hunter -v 3 -ll
   /path/to/log/dir -c /path/to/config/dir --cache
   /path/to/cache/dir
   ```

4 Hour Bespoke Name Example

```
0 */4 * * * tq-conn-cb-threat-hunter -n
<Bespoke_Name> -v 3 -ll /path/to/log/dir -c
/path/to/config/dir --cache /path/to/cache/dir
```

Change Log

- **Version 1.0.0**
  - Initial Release