ThreatQuotient

VMware Carbon Black Cloud Enterprise EDR Connector Guide

Version 1.1.0

July 14, 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: `1.1.0`
- Supported on ThreatQ versions >= `4.34.0`

There are two versions of this integration:

- Python 2 version
- Python 3 version

Introduction

The VMware Carbon Black Cloud Enterprise EDR integration 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 from the ThreatQuotient repository with YUM credentials or offline via a .whl file.

> ⚠ **Upgrading Users** - Review the Change Log for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. Failure to delete the previous configuration file will result in the connector failing.

1. Install the connector using one of the following methods:

   ThreatQ Repository

   a. Run the following command:

   ```
   pip install tq_conn_cb_threat_hunter
   ```

   Offline via .whl file

   To install this connector from a wheel file, the wheel file (.whl) will need to be copied via SCP into your ThreatQ instance.

   a. Download the connector whl file with its dependencies:

   ```
   mkdir /tmp/tq_conn_cb_threat_hunter

   pip download tq_conn_cb_threat_hunter -d

   /tmp/tq_conn_cb_threat_hunter/
   ```

   b. Archive the folder with the .whl files:

   ```
   tar -czvf tq_conn_cb_threat_hunter.tgz /tmp/
   tq_conn_cb_threat_hunter/
   ```

   c. Transfer all the whl files, the connector and all the dependencies, to the ThreatQ instance.

   d. Open the archive on ThreatQ:

   ```
   tar -xvf tq_conn_cb_threat_hunter.tgz
   ```

e. Install the connector on the ThreatQ instance.

> The example assumes that all the whl files are copied to `/tmp/conn` on the ThreatQ instance.

```
pip install /tmp/conn/ tq_conn_cb_threat_hunter-<version>-
<python version>-none-any.whl --no-index --find-links /
tmp/conn/
```

> pip install /tmp/conn/ tq_conn_cb_threat_hunter-1.1.0-py2-none-any.whl --no-index --find-links /tmp/conn/

> A driver called `tq-conn-cb-threat-hunter` will be installed. After installing with `pip` or `setup.py`, a script stub will appear in `/usr/bin/tq-conn-cb-threat-hunter`.

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. Use the commands below to create the required directories:

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

3. Perform an initial run using the following command:

```
tq-conn-cb-threat-hunter -v3 -ll /var/log/tq_labs/ -c /etc/
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.
Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
Email Address	This is the User in the ThreatQ System for integrations.

PARAMETER	DESCRIPTION
Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

Example Output

```
tq-conn-cb-threat-hunter -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
ThreatQ Host: <ThreatQ Host IP or Hostname>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

You will still need to configure and then enable the connector.

Configuration

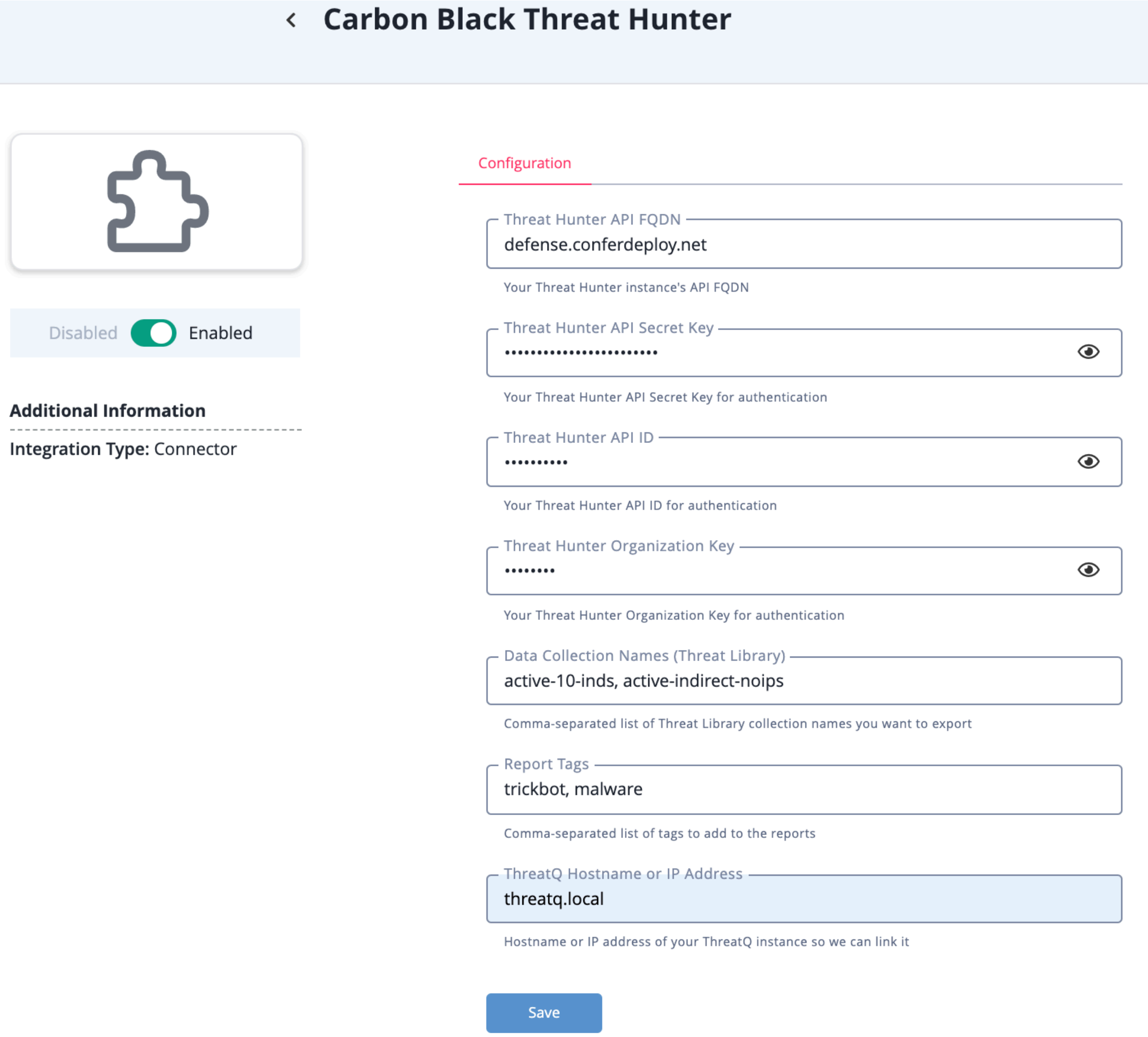
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the *Category* dropdown (optional).
3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Threat Hunter API FQDN	The FQDN to access Threat Hunter's API. The default is `defense.conferdeploy.net`
Threat Hunter API Secret Key	Your Threat Hunter API Secret Key for authentication.
Threat Hunter API ID	Your Threat Hunter API ID for authentication.
Threat Hunter Organization Key	Your Threat Hunter Organization Key for authentication.
Data Collection Names (Threat Library)	A comma-separated list of Threat Library collection names you want to export.
Report Tags	A comma-separated list of tags to add to the reports. The tags will be added to each report.

PARAMETER	DESCRIPTION
ThreatQ Hostname or IP Address	This is the hostname or IP address of your ThreatQ instance in order to link back to it. This is typically the domain/IP that can be viewed in your browser's URL bar.



Additional Information

Integration Type: Connector

Threat Hunter API FQDN: defense.conferdeploy.net

Your Threat Hunter instance's API FQDN

Threat Hunter API Secret Key: ••••••••••••••••••••••••

Your Threat Hunter API Secret Key for authentication

Threat Hunter API ID: ••••••••••

Your Threat Hunter API ID for authentication

Threat Hunter Organization Key: ••••••••

Your Threat Hunter Organization Key for authentication

Data Collection Names (Threat Library): active-10-inds, active-indirect-noips

Comma-separated list of Threat Library collection names you want to export

Report Tags: trickbot, malware

Comma-separated list of tags to add to the reports

ThreatQ Hostname or IP Address: threatq.local

Hostname or IP address of your ThreatQ instance so we can link it

5. Review any additional settings available, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Usage

Use the following command to execute the driver:

```
tq-conn-cb-threat-hunter -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

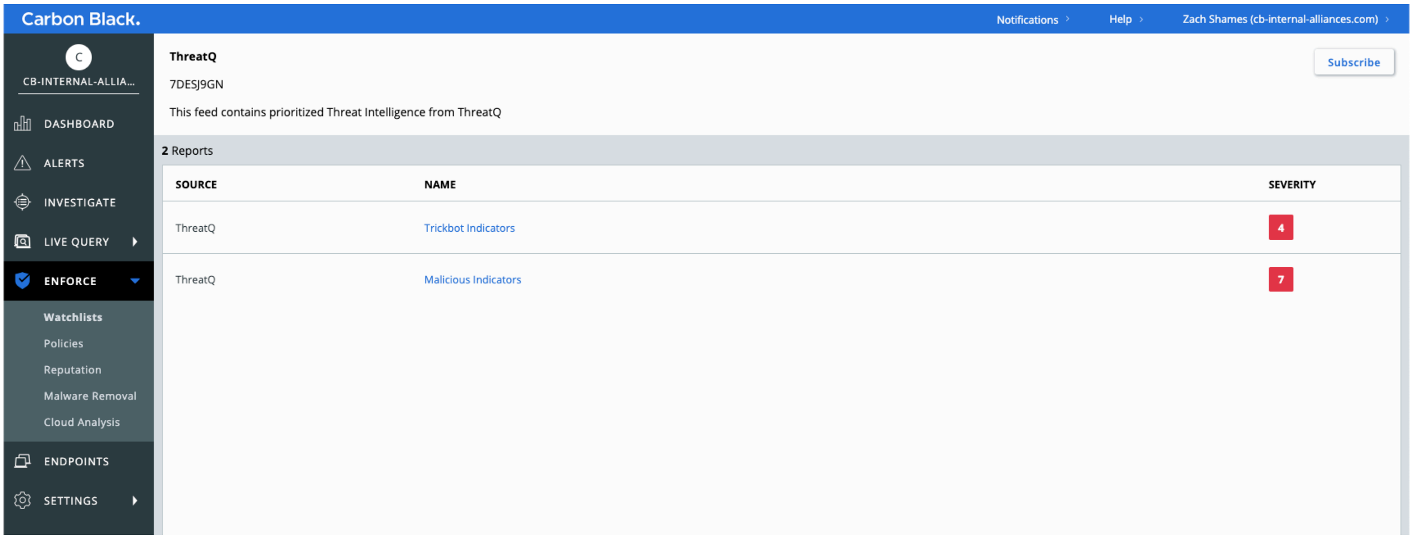
Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
`-h`, `--help`	Shows this help message and exits.
`-ll LOGLOCATION`, `--loglocation LOGLOCATION`	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).
`-c CONFIG`, `--config CONFIG`	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)
`-v {1,2,3}`, `--verbosity {1,2,3}`	This is the logging verbosity level where **3** means everything. The default setting is **1** (Warning).
`-ep, --external-proxy`	This allows you to use the proxy that is specified in the ThreatQ UI. This specifies an internet facing proxy, NOT a proxy to the TQ instance.
`-n NAME, --name NAME`	This sets the name for this connector. In some cases, it is useful to have multiple connectors of the same type executing against a

ARGUMENT	DESCRIPTION
	single TQ instance. For example, the Syslog Exporter can be run against multiple target and multiple exports, each with their own name and configuration.
`-d, --no-differential`	If exports are used in this connector, this will turn 'off' the differential flag for the execution. This allows debugging and testing to be done on export endpoints without having to rebuild the exports after the test. THIS SHOULD NEVER BE USED IN PRODUCTION.

Example Results - Feed Reports



ThreatQ

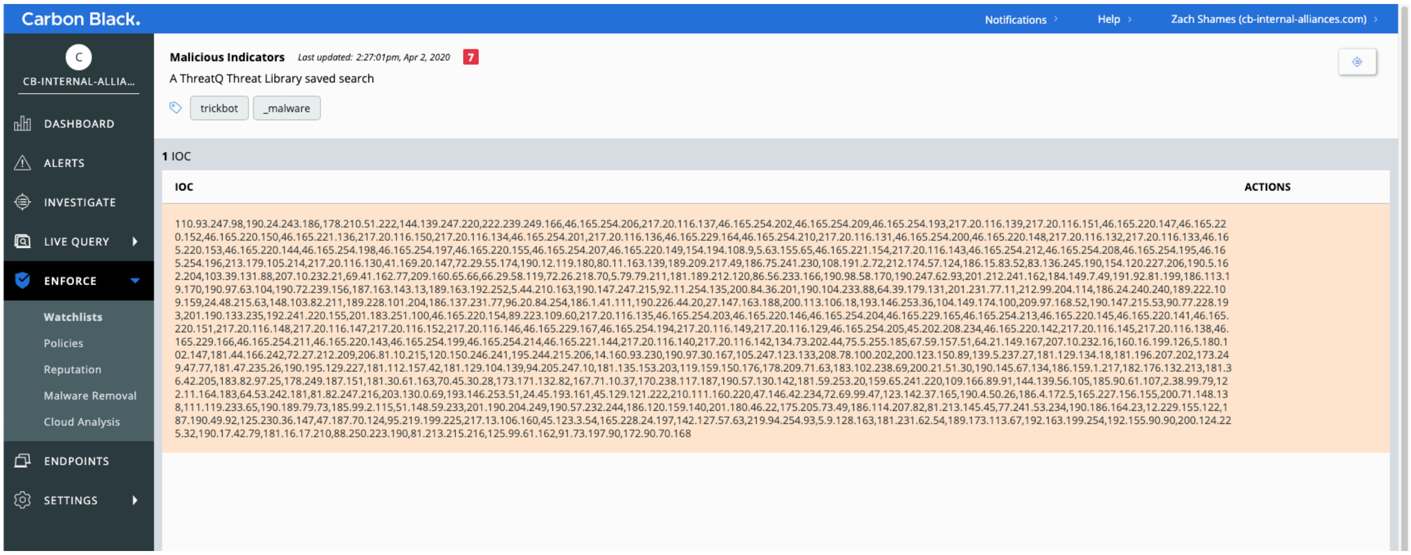
7DESJ9GN

This feed contains prioritized Threat Intelligence from ThreatQ

2 Reports

SOURCE	NAME	SEVERITY
ThreatQ	Trickbot Indicators	4
ThreatQ	Malicious Indicators	7

Example Results - Single Report



Malicious Indicators *Last updated: 2:27:01pm, Apr 2, 2020* 7

A ThreatQ Threat Library saved search

trickbot _malware

1 IOC

IOC **ACTIONS**

```
110.93.247.98,190.24.243.186,178.210.51.222,144.139.247.220,222.239.249.166,46.165.254.206,217.20.116.137,46.165.254.202,46.165.254.209,46.165.254.193,217.20.116.139,217.20.116.151,46.165.220.147,46.165.22
0.152,46.165.220.150,46.165.221.136,217.20.116.150,217.20.116.134,46.165.254.201,217.20.116.136,46.165.229.164,46.165.254.210,217.20.116.131,46.165.254.200,46.165.220.148,217.20.116.132,217.20.116.133,46.16
5.220.153,46.165.220.144,46.165.254.198,46.165.254.197,46.165.220.155,46.165.254.207,46.165.220.149,154.194.108.9,5.63.155.65,46.165.221.154,217.20.116.143,46.165.254.212,46.165.254.208,46.165.254.195,46.16
5.254.196,213.179.105.214,217.20.116.130,41.169.20.147,72.29.55.174,190.12.119.180,80.11.163.139,189.209.217.49,186.75.241.230,108.191.2.72,212.174.57.124,186.15.83.52,83.136.245.190,154.120.227.206,190.5.16
2.204,103.39.131.88,207.10.232.21,69.41.162.77,209.160.65.66,66.29.58.119,72.26.218.70,5.79.79.211,181.189.212.120,86.56.233.166,190.98.58.170,190.247.62.93,201.212.241.162,184.149.7.49,191.92.81.199,186.113.1
9.170,190.97.63.104,190.72.239.156,187.163.143.13,189.163.192.252,5.44.210.163,190.147.247.215,92.11.254.135,200.84.36.201,190.104.233.88,64.39.179.131,201.231.77.11,212.99.204.114,186.24.240.240,189.222.10
9.159,24.48.215.63,148.103.82.211,189.228.101.204,186.137.231.77,96.20.84.254,186.1.41.111,190.226.44.20,27.147.163.188,200.113.106.18,193.146.253.36,104.149.174.100,209.97.168.52,190.147.215.53,90.77.228.19
3,201.190.133.235,192.241.220.155,201.183.251.100,46.165.220.154,89.223.109.60,217.20.116.135,46.165.254.203,46.165.220.146,46.165.254.204,46.165.229.165,46.165.254.213,46.165.220.145,46.165.220.141,46.165.
220.151,217.20.116.148,217.20.116.147,217.20.116.152,217.20.116.146,46.165.229.167,46.165.254.194,217.20.116.149,217.20.116.129,46.165.254.205,45.202.208.234,46.165.220.142,217.20.116.145,217.20.116.138,46.
165.229.166,46.165.254.211,46.165.220.143,46.165.254.199,46.165.254.214,46.165.221.144,217.20.116.140,217.20.116.142,134.73.202.44,75.5.255.185,67.59.157.51,64.21.149.167,207.10.232.16,160.16.199.126,5.180.1
02.147,181.44.166.242,72.27.212.209,206.81.10.215,120.150.246.241,195.244.215.206,14.160.93.230,190.97.30.167,105.247.123.133,208.78.100.202,200.123.150.89,139.5.237.27,181.129.134.18,181.196.207.202,173.24
9.47.77,181.47.235.26,190.195.129.227,181.112.157.42,181.129.104.139,94.205.247.10,181.135.153.203,119.159.150.176,178.209.71.63,183.102.238.69,200.21.51.30,190.145.67.134,186.159.1.217,182.176.132.213,181.3
6.42.205,183.82.97.25,178.249.187.151,181.30.61.163,70.45.30.28,173.171.132.82,167.71.10.37,170.238.117.187,190.57.130.142,181.59.253.20,159.65.241.220,109.166.89.91,144.139.56.105,185.90.61.107,2.38.99.79,12
2.11.164.183,64.53.242.181,81.82.247.216,203.130.0.69,193.146.253.51,24.45.193.161,45.129.121.222,210.111.160.220,47.146.42.234,72.69.99.47,123.142.37.165,190.4.50.26,186.4.172.5,165.227.156.155,200.71.148.13
8,111.119.233.65,190.189.79.73,185.99.2.115,51.148.59.233,201.190.204.249,190.57.232.244,186.120.159.140,201.180.46.22,175.205.73.49,186.114.207.82,81.213.145.45,77.241.53.234,190.186.164.23,12.229.155.122,1
87.190.49.92,125.230.36.147,47.187.70.124,95.219.199.225,217.13.106.160,45.123.3.54,165.228.24.197,142.127.57.63,219.94.254.93,5.9.128.163,181.231.62.54,189.173.113.67,192.163.199.254,192.155.90.90,200.124.22
5.32,190.17.42.79,181.16.17.210,88.250.223.190,81.213.215.216,125.99.61.162,91.73.197.90,172.90.70.168
```

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 every two hours.

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. Enter the commands below:

   Every 2 Hours Example

   ```
   0 */2 * * * tq-conn-cb-threat-hunter -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
   ```

4. Save and exit CRON.

Change Log

- **Version 1.1.0**
  - Added Python 3 support.
- **Version 1.0.0**
  - Initial Release