ThreatQuotient

Cortex App for TheHive Guide

Version 1.0.1

May 02, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 4.58.1
Compatible with Cortex Version	3.1.7
Compatible with The Hive Version	5.1.3
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/cortex-app-for-the-hive

Introduction

The Cortex App for the Hive is used for enriching observables in Cortex against a ThreatQ instance. After an observable is enriched in Cortex using the ThreatQ app, the enriched content can be seen in the cases in the Hive using the native Hive integration.

Prerequisites

Review and confirm the following requirements before attempting to install the application:

- Cortex and the Hive applications are installed and the integration between the two is configured. See this setup guide for detailed configuration steps of Cortex: https://docs.thehive-project.org/cortex/.
- The following steps have been reviewed: https://docs.thehive-project.org/cortex/installation-and-configuration/analyzers-responders/#run-you-own-analyzers-responders.
- Python 3 is installed on the Cortex VM.

Installation

> If you are upgrading from a previous version, review the Change Log to determine if there are any changes to configuration file such as new or removed fields. If there are changes, you must first delete your existing configuration file before proceeding with the steps below to install the new version. Contact ThreatQ Support if you require assistance.

1. Download the integration zip file from the ThreatQ Marketplace.
2. Unzip the file's contents:

```
<> unzip /path/to/archive/cortex_app_v<VERSION>.zip
```

3. Transfer the files to your Cortex instance:

```
<> scp -r /path/to/folder/cortex_app_v<VERSION>/
   tq_hive_cortex_analyzer_src <USERNAME>@<CORTEX HOST/IP>:/tmp/
```

4. Create a new folder in the Custom Analyzers installation path for Cortex:

```
<> ssh <USERNAME>@<CORTEX HOST/IP>

   sudo mkdir -p /opt/Custom-Analyzers/{analyzers,responders}/
   ThreatQ
```

5. Move the Cortex app to the Custom Analyzers directory and set the correct ownership:

```
<> cp /tmp/tq_hive_cortex_analyzer_src/*.* /opt/Custom-Analyzers/
   analyzers/ThreatQ/

   chown -R cortex:cortex /opt/Custom-Analyzers
```

6. Add the Custom Analyzers path the application.conf file as described in the following documentation:

   https://docs.thehive-project.org/cortex/installation-and-configuration/analyzers-responders/#update-cortex-configuration

7. Restart the Corext app. If the system is using systemctl, the command will be:

```
<> systemctl restart cortex
```

Configuration

Use the following steps to configure the app in Cortex.

> You should generate ThreatQ OAuth credentials prior to starting the configuration. See the OAuth Credentials topic on the ThreatQ Help Center for additional details and steps.

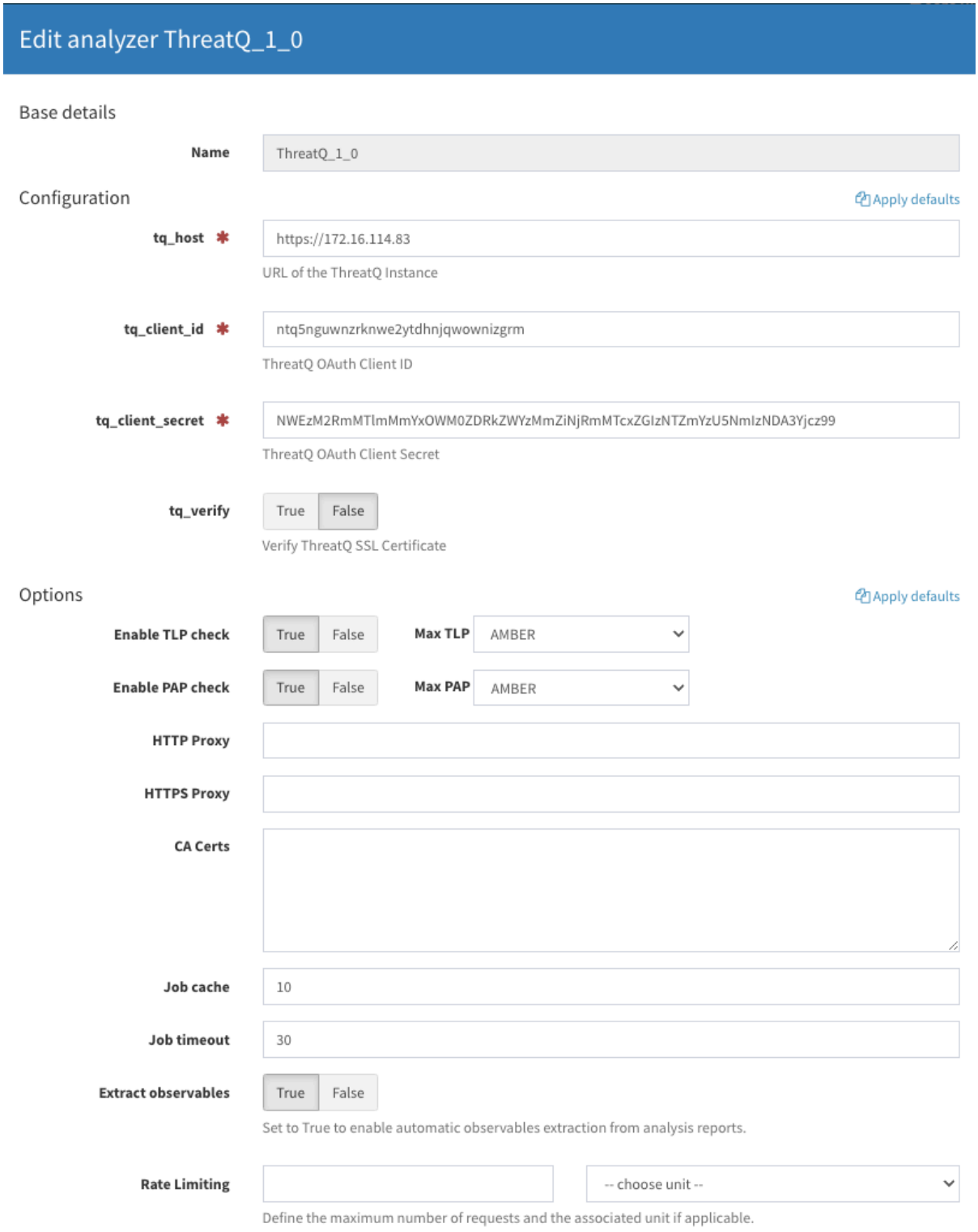
1. Log in as a user to Cortex UI.
2. Navigate to **Organization** and select the **Analyzers** tab
3. Search for **ThreatQ and click** on **Enable** and then on **Edit**.
4. Enter the required parameters and credentials and save the configuration:

PARAMETER	DESCRIPTION
tq_host	This is the hostname or IP address for the ThreatQ instance prefaced by `https://`.
tq_client_id	ThreatQ OAuth Client ID. See the OAuth Credentials topic on the ThreatQ Help Center.
tq_client_secret	ThreatQ OAuth Client Secret. See the OAuth Credentials topic on the ThreatQ Help Center.
tq_verify	Verify ThreatQ SSL Certificate. The default value is False.

5. Test the integration by logging in as a user to Cortex UI.
6. Click on **New Analysis**, select the **Data Type** from the dropdown, enter the observable value.
7. Select **ThreatQ_1_0** from the list of **Analyzers** and click on the **Start** button.

> Once completed it should show the enrichment data from ThreatQ

Once complete with the configuration, the settings in the Cortex instance will look similar to this snapshot:


Edit analyzer ThreatQ_1_0
Base details
Name
ThreatQ_1_0
Configuration
Apply defaults
tq_host
https://172.16.114.83
URL of the ThreatQ Instance
tq_client_id
ntq5nguwnzrknwe2ytdhnjqwownizgrm
ThreatQ OAuth Client ID
tq_client_secret
NWEzM2RmMTlmMmYxOWM0ZDRkZWYzMmZiNjRmMTcxZGIzNTZmYzU5NmIzNDA3Yjcz99
ThreatQ OAuth Client Secret
tq_verify
True
False
Verify ThreatQ SSL Certificate
Options
Apply defaults
Enable TLP check
True
False
Max TLP
AMBER
Enable PAP check
True
False
Max PAP
AMBER
HTTP Proxy
HTTPS Proxy
CA Certs
Job cache
10
Job timeout
30
Extract observables
True
False
Set to True to enable automatic observables extraction from analysis reports.
Rate Limiting
-- choose unit --
Define the maximum number of requests and the associated unit if applicable.

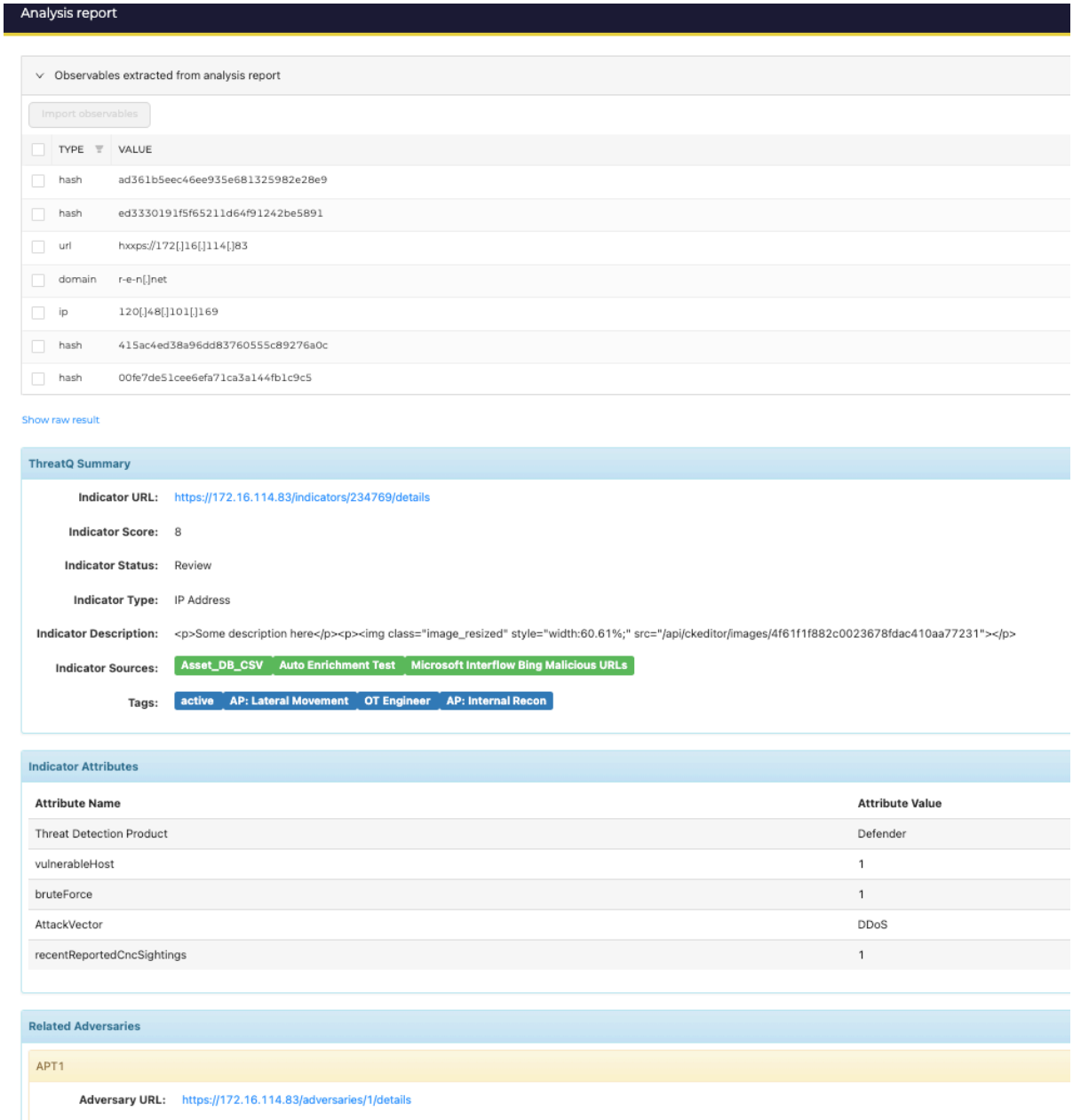
Usage of the App on The Hive

1. Login as a user to the Hive UI
2. Import the analysis HTML template provided with the ZIP file downloaded from the ThreatQ Marketplace.

   > The HTML file is in `/path/to/folder/cortex_app_v<VERSION>/tq_hive_cortex_analyzer_templates`

3. Select a case and click on the **Observables** tab.
4. Enter an observable, select the type, and click on **Confirm**.
5. To run an enrichment against ThreatQ, hover over an observable, click on the ellipsis on the right-most side and select **Run Analyzers**.
6. On the following screen click on the **ThreatQ** app and then **Run Selected Analyzers**.

The enrichment data in the Hive will look similar to this snapshot:



Average Feed Run

Object counts and runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	2 minutes

Change Log

- **Version 1.0.1**
  - Initial release