ThreatQuotient

FireEye HX Alerts Connector

Version 1.0.1 rev-a

September 19, 2024

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	>= 4.35.0
Python Version	3.6
Support Tier	ThreatQ Supported

Introduction

The FireEye HX Alerts Connector for ThreatQ enables the automatic ingestion of alerts and relevant indicators/context from FireEye, into ThreatQ.

The integration ingests the following system objects:

- Events
- Indicators

Prerequisites

Review the following requirements before attempting to install the connector.

FireEye HX and API

The FireEye HX Alerts connector requires a deployed instance of FireEye HX and that the API is network accessible by ThreatQ.

Time Zone

> ⚠ The time zone steps are for ThreatQ v5 only. ThreatQ v6 users should skip these steps.

You should ensure all ThreatQ devices are set to the correct time, time zone, and date (UTC is recommended), and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the list-`timezones` command line option.

For example, enter the following command to list all available time zones in Europe:

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

Enter the following command, as root, to change the time zone to UTC:

```
timedatectl set-timezone UTC
```

Integration Dependencies

> ⚠ The integration must be installed in a python 3.6 environment.

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you will need to download and install these dependencies separately as the integration will not be able to download them during the install process.

Items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

DEPENDENCY	VERSION	NOTES
threatqsdk	>=1.8.2	N/A
threatqcc	>=1.4.1	N/A
python-dateutil	N/A	N/A

Installation

> ⚠ **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.

ThreatQ v6 Process

1. Download the connector integration file from the ThreatQ Marketplace.
2. Transfer the connector whl file to the `/tmp/` directory on your instance.
3. SSH into your instance.
4. Move the connector whl file from its `/tmp/` location to the following directory: `/opt/tqvenv`
5. Navigate to the custom connector container:

   ```
   kubectl exec -n threatq -it deployments/custom-connectors -- /bin/bash
   ```

6. Create your python 3 virtual environment:

   ```
   python3.6 -m venv /opt/tqvenv/<environment_name>
   ```

7. Active the new environment:

   ```
   source /opt/tqvenv/<environment_name>/bin/activate
   ```

8. Run the pip upgrade command:

   ```
   pip install --upgrade pip
   ```

9. Install the required dependencies:

   ```
   pip install setuptools==59.6.0 threatqsdk threatqcc
   ```

10. Install the connector:

    ```
    pip install /opt/tqvenv/tq_conn_fireeye_hx_alerts-<version>-py3-none-any.whl
    ```

11. Perform an initial run of the connector:

    ```
    /opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts --cron="0 */2 * * *"
    ```

> The `--cron` argument above is used to generate a cron job for the connector. After running the command above, the cronjob will be created under the /etc/cron.d/ directory. This entry will initially be commented out upon creation - see the CRON chapter for more details.

12. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	**Leave this field blank as it will be set dynamically.**
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.
ThreatQ Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

Example Output

```
/opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts --cron="0 */2
* * *"
ThreatQ Host:
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

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

ThreatQ v5 Process

1. Navigate to the ThreatQ Marketplace and download the .whl file for the integration.
2. Create the following directory:

```
mkdir /opt/tqvenv/
```

3. Install python 3.6:

```
sudo yum install -y python36 python36-libs python36-devel python36-pip
```

4. Create a virtual environment:

```
python3.6 -m venv /opt/tqvenv/<environment_name>
```

5. Activate the virtual environment:

```
source /opt/tqvenv/<environment_name>/bin/activate
```

6. Run the pip upgrade command:

```
pip install --upgrade pip
```

7. Install the required dependencies:

```
pip install threatqsdk threatqcc setuptools==59.6.0
```

8. Transfer the whl file to the `/tmp` directory on your ThreatQ instance.
9. Install the connector on your ThreatQ instance:

```
pip install /tmp/tq_conn_fireeye_hx_alerts-<version>-py3-none-any.whl
```

> A driver called `tq-conn-fireeye-hx-alerts` will be installed. After installing, a script stub will appear in `/opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts`.

10. 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/
```

11. Perform an initial run using the following command:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts -ll /var/
log/tq_labs/ -c /etc/tq_labs/ -v3
```

12. 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.
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.

PARAMETER	DESCRIPTION
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.
ThreatQ Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

Example Output

```
/opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts -ll /var/log/
tq_labs/ -c /etc/tq_labs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostname>
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

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

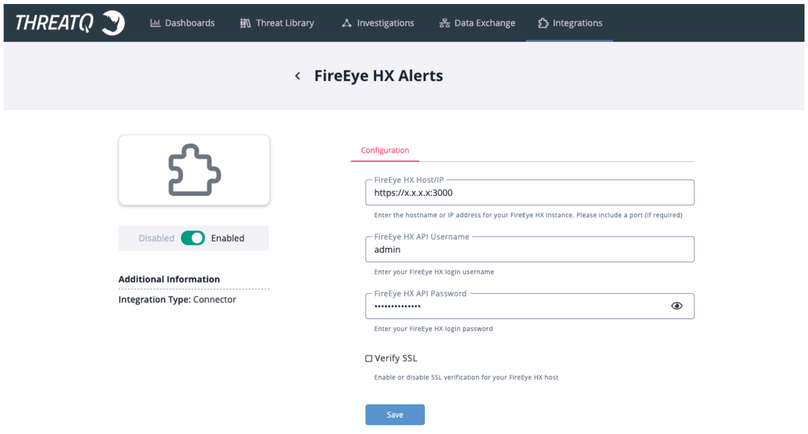
Configuration

> 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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
FireEye HX Host/IP	Enter the hostname or IP address, including port (if required), for your FireEye HX instance.
FireEye HX API Username	Enter your FireEye HX login username. Confirm that the user account is an API user, and not a regular user account, when configuring a username/ password. To create/view user accounts, log into FireEye HX, and navigate to **Admin -> Appliance Settings -> User Accounts**.
FireEye HX API Password	Enter your FireEye HX login password.
Verify SSL	Enable or disable SSL verification for your FireEye HX host.



FireEye HX Alerts

Disabled ● Enabled

Additional Information

Integration Type: Connector

FireEye HX Host/IP: https://x.x.x.x:3000

Enter the hostname or IP address for your FireEye HX instance. Please include a port (if required)

FireEye HX API Username: admin

Enter your FireEye HX login username

FireEye HX API Password: ••••••••••••••

Enter your FireEye HX login password

□ Verify SSL

Enable or disable SSL verification for your FireEye HX host

5. Review any additional settings, 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:

ThreatQ v6 Driver Command

```
/opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts
```

ThreatQ v5 Driver Command

```
/opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-alerts -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 the help message and exits.
`-v`	Sets the log verbosity (3 means everything).
`-c`	The path to the directory where you want to store your config file.
`-ll`	The path to the directory where you want to store your logs.
`-ep` `--external-proxy`	A flag to enable the use of the system proxy, configured in ThreatQ
--cron	ThreatQ v6 Only - creates a CRON entry for the connector based on a pre-loaded ThreatQ template. See the CRON section for more details.

Accessing Connector Logs

ThreatQ v6

ThreatQ version 6 aggregates the logs for all custom connectors to its output container. You can access the container's log using the following command:

```
kubectl logs -n threatq deployments/custom-connectors
```

ThreatQ v5

The connector log directory was created in 10 of the installation process and is identified using the `-ll` argument flag when executing the driver.

Accessing Connector Configuration

ThreatQ v6

The custom connector configuration file can be found in the following directory: `/etc/tq_labs/`.

ThreatQ v5

The custom connector configuration file was created in step 10 of the install process and identified using the `-c` argument flag when executing the driver.

CRON

ThreatQ v6 CRON

The addition of the `--cron` argument in the initial run of connector, performed during the install process, resulted in the creation of a cron job file for the connector in the following directory: `/etc/cron.d/`. The contents of the file will resemble the following structure:

```
#{schedule} root /bin/bash -c "source /etc/env-vars.sh; {venv_path}/bin/
{executable} --config=/etc/tq_labs > /proc/1/fd/1 2>/proc/1/fd/2"
```

The `{schedule}` will be replaced with the cron settings you entered with the `--cron` flag and the `{executable}` will be replaced for with the connector's driver command.

You will also see a `#` at the beginning of the file. This comments out the job. This allows you to configure the custom connector in the ThreatQ UI first. After you have configured the connector in ThreatQ, you can remove the `#` from the file content's in order to activate the cron job.

To summarize this process:

1. Install the connector and perform an initial run using the `--cron` argument to create the cron job.
2. Complete the connector's configuration settings in the ThreatQ UI.
3. Access the connector's cron file in the `/etc/cron.d/` directory and remove the # from the beginning of the file.

ThreatQ v5 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
   ```

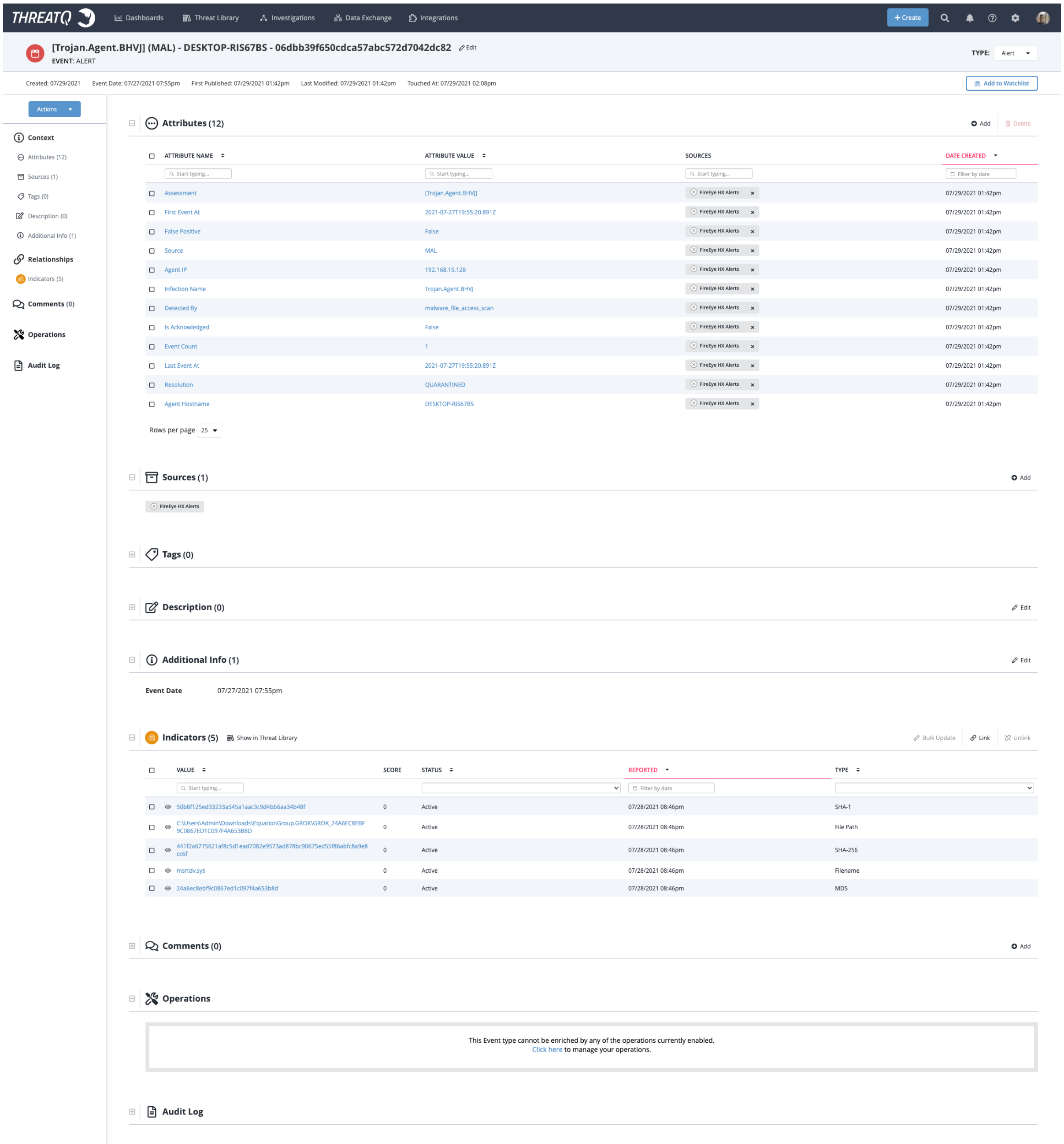
   This will enable the editing of the crontab, using vi. Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.
3. Enter the commands below:

   Every 2 Hours Example

```
0 */2 * * * /opt/tqvenv/<environment_name>/bin/tq-conn-fireeye-hx-
alerts -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

4. Save and exit CRON.

FireEye HX Alert Example



[Trojan.Agent.BHVJ] (MAL) - DESKTOP-RIS67BS - 06dbb39f650cdca57abc572d7042dc82

EVENT: ALERT

TYPE: Alert

Created: 07/29/2021 Event Date: 07/27/2021 07:55pm First Published: 07/29/2021 01:42pm Last Modified: 07/29/2021 01:42pm Touched At: 07/29/2021 02:08pm

Attributes (12)

ATTRIBUTE NAME	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Assessment	[Trojan.Agent.BHVJ]	FireEye HX Alerts	07/29/2021 01:42pm
First Event At	2021-07-27T19:55:20.891Z	FireEye HX Alerts	07/29/2021 01:42pm
False Positive	False	FireEye HX Alerts	07/29/2021 01:42pm
Source	MAL	FireEye HX Alerts	07/29/2021 01:42pm
Agent IP	192.168.15.128	FireEye HX Alerts	07/29/2021 01:42pm
Infection Name	Trojan.Agent.BHVJ	FireEye HX Alerts	07/29/2021 01:42pm
Detected By	malware_file_access_scan	FireEye HX Alerts	07/29/2021 01:42pm
Is Acknowledged	False	FireEye HX Alerts	07/29/2021 01:42pm
Event Count	1	FireEye HX Alerts	07/29/2021 01:42pm
Last Event At	2021-07-27T19:55:20.891Z	FireEye HX Alerts	07/29/2021 01:42pm
Resolution	QUARANTINED	FireEye HX Alerts	07/29/2021 01:42pm
Agent Hostname	DESKTOP-RIS67BS	FireEye HX Alerts	07/29/2021 01:42pm

Rows per page 25

Sources (1)

FireEye HX Alerts

Tags (0)

Description (0)

Additional Info (1)

Event Date 07/27/2021 07:55pm

Indicators (5)

VALUE	SCORE	STATUS	REPORTED	TYPE
50b8f125ed33233a545a1aac3c9d4bb6aa34b48f	0	Active	07/28/2021 08:46pm	SHA-1
C:\Users\Admin\Downloads\EquationGroup.GROK\GROK_24A6EC8EBF9C0867ED1C097F4A653B8D	0	Active	07/28/2021 08:46pm	File Path
441f2a6775621af8c5d1ead7082e9573ad878bc90675ed55f86abfc8a9e8cc6f	0	Active	07/28/2021 08:46pm	SHA-256
msrtdv.sys	0	Active	07/28/2021 08:46pm	Filename
24a6ec8ebf9c0867ed1c097f4a653b8d	0	Active	07/28/2021 08:46pm	MD5

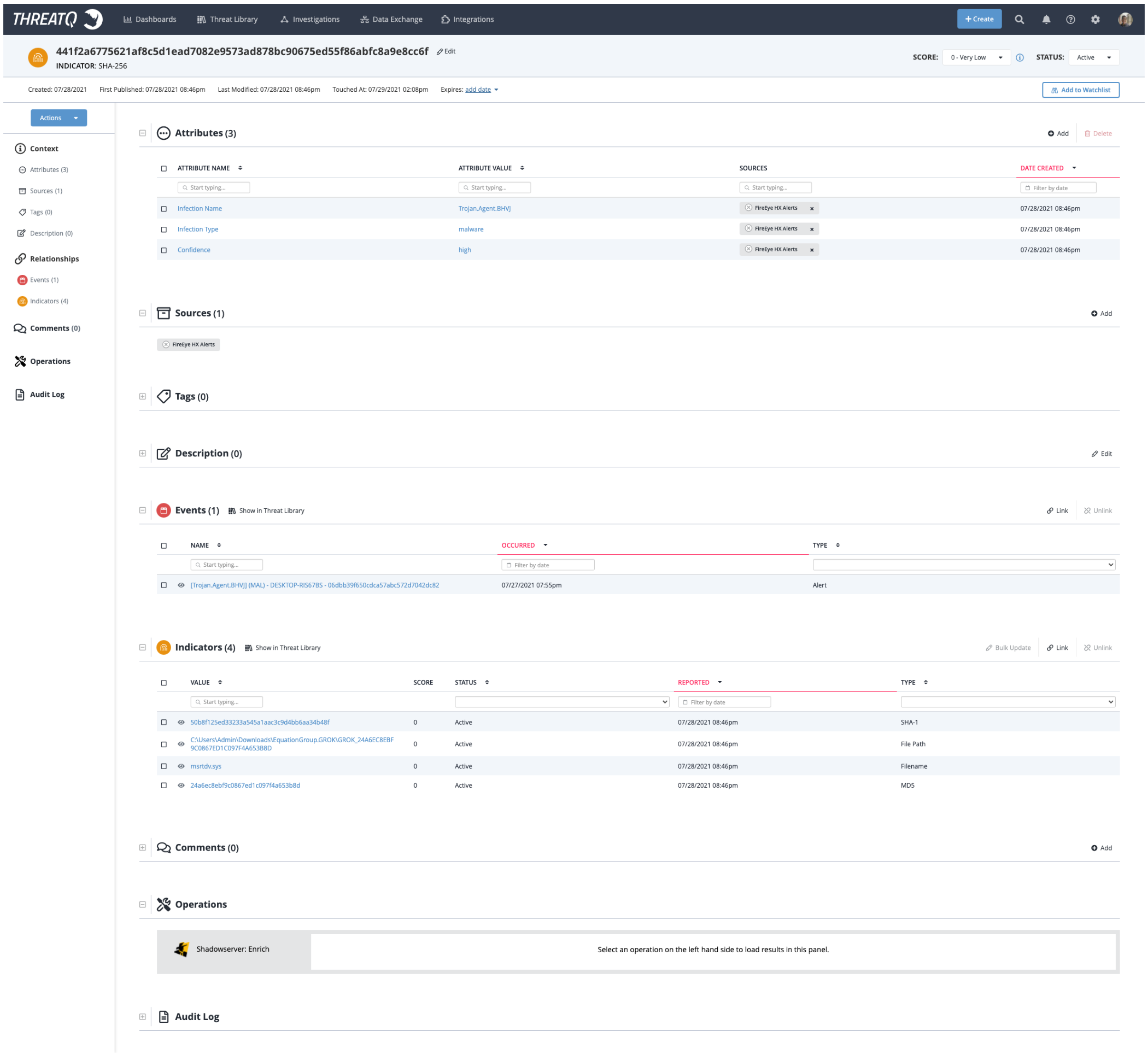
Comments (0)

Operations

This Event type cannot be enriched by any of the operations currently enabled.
Click here to manage your operations.

Audit Log

FireEye HX Indicator Example



441f2a6775621af8c5d1ead7082e9573ad878bc90675ed55f86abfc8a9e8cc6f

INDICATOR: SHA-256

SCORE: 0 - Very Low STATUS: Active

Created: 07/28/2021 First Published: 07/28/2021 08:46pm Last Modified: 07/28/2021 08:46pm Touched At: 07/29/2021 02:08pm Expires: add date

Attributes (3)

□	ATTRIBUTE NAME	ATTRIBUTE VALUE	SOURCES	DATE CREATED
□	Infection Name	Trojan.Agent.BHVJ	FireEye HX Alerts	07/28/2021 08:46pm
□	Infection Type	malware	FireEye HX Alerts	07/28/2021 08:46pm
□	Confidence	high	FireEye HX Alerts	07/28/2021 08:46pm

Sources (1)

FireEye HX Alerts

Tags (0)

Description (0)

Events (1)

□	NAME	OCCURRED	TYPE
□	[Trojan.Agent.BHVJ] (MAL) - DESKTOP-RIS67BS - 06dbb39f650cdca57abc572d7042dc82	07/27/2021 07:55pm	Alert

Indicators (4)

□	VALUE	SCORE	STATUS	REPORTED	TYPE
□	50b8f125ed33233a545a1aac3c9d4bb6aa34b48f	0	Active	07/28/2021 08:46pm	SHA-1
□	C:\Users\Admin\Downloads\EquationGroup.GROK\GROK_24A6EC8EBF9C0867ED1C097F4A653B8D	0	Active	07/28/2021 08:46pm	File Path
□	msrtdv.sys	0	Active	07/28/2021 08:46pm	Filename
□	24a6ec8ebf9c0867ed1c097f4a653b8d	0	Active	07/28/2021 08:46pm	MD5

Comments (0)

Operations

Shadowserver: Enrich

Select an operation on the left hand side to load results in this panel.

Audit Log

ThreatQ Mapping

Sample Response:

```
2021-07-29 14:02:50 - threatqcc.custom_connector DEBUG: Using Current working
directory for config path
2021-07-29 14:02:50 - tq_conn_fireeye_hx_alerts DEBUG: Private Connection
Established
2021-07-29 14:02:50 - fireeye_hx_alerts INFO: Fetching alerts from FireEye HX
(2021-06-25T00:00:00.000Z - 2021-07-29T14:02:50.000Z)
2021-07-29 14:02:54 - fireeye_hx_alerts INFO: Parsing 6 alerts from FireEye HX
2021-07-29 14:02:54 - fireeye_hx_alerts INFO: Uploading alert,
[[Trojan.Agent.BHVJ] (MAL) - DESKTOP-RIS67BS -
06dbb39f650cdca57abc572d7042dc82] with [5] indicator(s) to ThreatQ...
2021-07-29 14:03:01 - fireeye_hx_alerts INFO: Uploading alert, [[EICAR-Test-
File (not a virus)] (MAL) - DESKTOP-RIS67BS - 44501e068f39b6d7749e8ff5447e08bf]
with [4] indicator(s) to ThreatQ...
2021-07-29 14:03:08 - fireeye_hx_alerts INFO: Uploading alert, [[EICAR-Test-
File (not a virus)] (MAL) - DESKTOP-RIS67BS - f62d937e9b168f88be7fd41d8a3320a7]
with [4] indicator(s) to ThreatQ...
2021-07-29 14:03:14 - fireeye_hx_alerts INFO: Uploading alert, [[EICAR-Test-
File (not a virus)] (MAL) - DESKTOP-RIS67BS - 89931c062f6be0f969b5ab1e8efab490]
with [4] indicator(s) to ThreatQ...
2021-07-29 14:03:20 - fireeye_hx_alerts INFO: Uploading alert, [[Address
140.82.113.4 connected] No Github (IOC) - DESKTOP-RIS67BS -
db092a2c710aed74ed31ff568e4d5d0b] with [1] indicator(s) to ThreatQ...
2021-07-29 14:03:28 - fireeye_hx_alerts INFO: Uploading alert, [[Address
140.82.113.4 connected] No Github (IOC) - DESKTOP-RIS67BS -
584c59c2febc3c47ec494558bfc8fa8f] with [1] indicator(s) to ThreatQ...
2021-07-29 14:03:37 - tq_conn_fireeye_hx_alerts INFO: [::] Completed execution
of the FireEye HX Alerts Connector in 46 seconds.
```

ThreatQuotient provides the following default mapping for this endpoint:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.assessment`, `.source`, `._id`	Event Title	Alert	`.first_event_at`	`[Trojan.Agent.BHVJ] (MAL) - DESKTOP-RIS67BS - 06dbb39f650cdca57abc572d7042dc82`	Key value's are formatted together to form a title
`.last_alert.event_values.detections.detection[].action.actioned-object.file-object.md5sum`	Indicator Value	MD5	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].action.actioned-object.file-object.sha256sum`	Indicator Value	SHA-256	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].action.actioned-object.file-object.sha1sum`	Indicator Value	SHA-1	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].action.actioned-object.file-object.file-path`	Indicator Value	File Path	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].action.actioned-object.file-object.size`	Attribute	File Size	`.created_at`	N/A	N/A
`.last_alert.event_values`	Indicator Value	Filename	`.created_at`	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.detections.detection[].action.actioned-object.file-object.original-file-name					
.last_alert.event_values.detections.detection[].action.actioned-object.file-object.hidden	Attribute	Is Hidden	.created_at	N/A	N/A
.last_alert.event_values.detections.detection[].action.actioned-object.file-object.temporary	Attribute	Is Temporary	.created_at	N/A	N/A
.last_alert.event_values.detections.detection[].action.actioned-object.file-object.read-only	Attribute	Is Read-only	.created_at	N/A	N/A
.last_alert.event_values.detections.detection[].action.actioned-object.file-object.packed	Attribute	Is Packed	.created_at	N/A	N/A
.last_alert.event_values.detections.detection[].action.actioned-object.file-object.system-file	Attribute	Is System File	.created_at	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.last_alert.event_values.detections.detection[].infected-object.file-object.md5sum`	Indicator Value	MD5	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.sha256sum`	Indicator Value	SHA-256	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.sha1sum`	Indicator Value	SHA-1	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.file-path`	Indicator Value	File Path	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.size`	Attribute	File Size	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.original-file-name`	Indicator Value	Filename	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.d`	Attribute	Is Hidden	`.created_at`	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`etection[].infected-object.file-object.hidden`					
`.last_alert.event_values.detections.detection[].infected-object.file-object.temporary`	Attribute	Is Temporary	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.read-only`	Attribute	Is Read-only	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.packed`	Attribute	Is Packed	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infected-object.file-object.system-file`	Attribute	Is System File	`.created_at`	N/A	N/A
`.last_alert.event_values.detections.detection[].infection.confidence-level`	Attribute	Confidence	`.created_at`	high	N/A
`.last_alert.event_values.detections.detection[].infection.infection-type`	Attribute	Infection Type	`.created_at`	malware	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.last_alert.event_values.detections.detection[].infection.infection-name`	Attribute	Infection Name	`.created_at`	Trojan.Agent.BHVJ	N/A
`.last_alert.event_type`	Attribute	Event Type	`.created_at`	N/A	N/A
`.last_alert.resolution`	Attribute	Resolution	`.created_at`	QUARANTINE	N/A
`.last_alert.md5values[]`	Indicator Value	MD5	`.created_at`	N/A	N/A
`.last_alert.agent.hostname`	Attribute	Agent Hostname	`.created_at`	DESKTOP-RIS67BS	N/A
`.last_alert.event_values.ipv4NetworkEvent/remoteIP`	Indicator Value	IP Address	`.created_at`	N/A	N/A
`.acknowledgement.acknowledged`	Attribute	Is Acknowledged	`.created_at`	false	N/A
`.acknowledgement.acknowledged_by`	Attribute	Acknowledged By	`.created_at`	false	N/A
`.grouped_by.detected_by`	Attribute	Detected By	`.created_at`	malware_file_access_scan	N/A
`.grouped_by.infection-name`	Attribute	Infection Name	`.created_at`	Trojan.Agent.BHVJ	N/A
`.grouped_by.host.hostname`	Attribute	Agent Hostname	`.created_at`	DESKTOP-RIS67BS	N/A
`.grouped_by.host.primary_ip_address`	Attribute	Agent IP	`.created_at`	N/A	N/A
`.grouped_by.md5sum`	Indicator Value	MD5	`.created_at`	N/A	N/A
`.grouped_by.file-path`	Indicator Value	File Path	`.created_at`	N/A	N/A
`.dispositions[].disposition`	Attribute	Disposition	`.created_at`	N/A	N/A
`.source`	Attribute	Source	`.created_at`	IOC	N/A
`.has_fp_disposition`	Attribute	False Positive	`.created_at`	false	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.assessment`	Attribute	Assessment	`.created_at`	`[Trojan.Agent.BHVJ]`	N/A
`.file_full_path`	Indicator Value	File Path	`.created_at`	N/A	N/A
`.first_event_at`	Attribute	First Event At	`.created_at`	2021-07-24T19:54:24.000Z	N/A
`.last_event_at`	Attribute	Last Event At	`.created_at`	2021-07-24T19:54:24.000Z	N/A
`.stats.events`	Attribute	Event Count	`.created_at`	6	N/A

Average Connector Run

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

METRIC	RESULT
Run Time	46 seconds
Events	6
Event Attributes	70
Indicators	19
Indicator Attributes	53

Change Log

- **Version 1.0.1 rev-a**
  - Guide Update - Added ThreatQ 6x documentation.
- **Version 1.0.1**
  - The connector will now disable the proxy if one is not provided.
- **Version 1.0.0**
  - Initial Release