ThreatQuotient

IBM X-Force Exchange Connector User Guide

Version 1.4.3

October 18, 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	1.4.3
Compatible with ThreatQ Versions	>= 4.45.0
Python Version	3.6
Support Tier	ThreatQ Supported

Introduction

The IBM X-Force Exchange connector imports data from the X-Force Exchange API into ThreatQ. It does this by setting up a connector, then, once enabled by the UI, connecting to the cloud instance of IBM X-Force Exchange and pulling down data. This is a unidirectional connector as it only consumes the data that XFE provides.

Prerequisites

Review the following requirements before attempting to install the connector.

Time Zone

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
```

`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	>=1.7.0	N/A
threatqcc	>=1.3.1	N/A
requests	N/A	N/A

Installation

The following provides you with steps on installing a Python 3 Virtual Environment and installing the connector.

Creating a Python 3.6 Virtual Environment

Run the following commands to create the virtual environment:

```
mkdir /opt/tqvenv/
sudo yum install -y python36 python36-libs python36-devel python36-pip
python3.6 -m venv /opt/tqvenv/<environment_name>
source /opt/tqvenv/<environment_name>/bin/activate
pip install --upgrade pip
pip install threatqsdk threatqcc setuptools==59.6.0
```

Proceed to Installing the Connector.

Installing the Connector

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. Navigate to the ThreatQ Marketplace and download the .whl file for the integration.
2. Activate the virtual environment if you haven't already:

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

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

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

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

5. 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/
```

6. Perform an initial run using the following command:

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

7. 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-xfe -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
Feed Name	The feed's name. This field should only be updated if deploying multiple versions of the connector.
X-Force Exchange API Key	The API key generated by the X-Force Exchange.
X-Force Exchange API Password	The password that was generated by the X-Force Exchange.
Initial Collection Days	The number of days to use during the initial pull request. The default setting is **5**.
Initial Attachment Days	The number of days to use during the initial pull of attachments, as these can be large this number can be tuned. The default setting is **10**.
X-Force Exchange URL	This field should not be changed unless the IBM X-Force team makes an upstream change.

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:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-xfe -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).
`-n, --name`	This allows you to change the name of the connector.
`-ds, --disable-ssl`	Adding this flag will disable SSL verification when contacting the API
`-ep, --external-proxy`	This enables a proxy to be used to connect to the internet for the data required by this connector. This specifies an internet facing proxy, NOT a proxy to the TQ instance.

ARGUMENT	DESCRIPTION
`-s, --start-historical`	This argument followed by a date allows the user to define a start date for a historical pull of XFE data. The date should be in the format YYYY-MM-DD HH:MM.
`-e, --end-historical`	This argument followed by a date allows the user to define the end date for a historical pull of XFE data. The date should be in the format YYYY-MM-DD HH:MM

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-xfe -c /etc/
   tq_labs/ -ll /var/log/tq_labs/ -v3
   ```
4. Save and exit CRON.

ThreatQ Mapping

Each main indicator type (Malware, URL, IP), has an associated report. Within this report are a few more attributes that we can flatten out as we ingest it into the TQ database.

Below is the mapping of the XFE Data.

XFE OBJECT	XFE TYPE	OBJECT PATH	XFE KEY	CREATE INDICATOR (Y OR N)	CREATE ATTRIBUTE (Y OR N)	V2 PATH	V2 KEY
Collection		caseFiles.caseFileID + "-" + caseFiles.title	caseFileID and title	N	N	event.name	Name
Collection		caseFiles.created	created	N	N	event.attribute	happened_at
Collection		caseFiles.tlpColor.tlpColorCode	tlpColorCode	N	N	event.attribute	TLP
Collection		caseFiles.tags	tags	N	Y	event.attribute	Tags
Collection		contents.wiki	wiki	N	N	event.description	description
Attachment		attachments.report.type	IAP	N	Y	event.attribute	Internet Application Profile
Attachment		attachments.report.type	Vuln	N	N	Ignored	Ignored
Attachment		attachments.report.type	PAM	N	N	Ignored	Ignored
Attachment		attachments.report.type	BOTNET	N	Y	event.attribute	Botnet
Attachment	IP	attachments.report.title	IP	Y	N	indictor.value	
Attachment	IP	***By virtue of type IP***	IP	N	N	indictor.class	Network
Attachment	IP	***By virtue of type IP***	IP	N	N	indictor.type	IP Address
Attachment	IP/ URL	attachments.report.data.score	Numeric 1-10	N	Y	indicator.attribute	X-Force Exchange Score
IP Report	IP	geo.country	Country	N	N	indicator.attribute	Country
IP Report	IP	reason	reason	N	Y	indicator.attribute	X-Force Exchange Reason
IP Report	IP	reasonDescription	reasonDescription	N	Y	indicator.attribute	X-Force Exchange Reason Description
IP Report	IP	cats.keys()	categories	N	Y	indicator.attribute	X-Force Exchange Category
Attachment	URL	attachments.report.title	title	Y	N	indicator.value	
Attachment	URL	attachments.report.type	URL	N	N	indicator.class	Network
Attachment	URL	attachments.report.title	title parsed for FQDN vs URL	N	N	indicator.type	FQDN or URL
URL Report	URL	result.cats.keys()	categories	N	N	indicator.attribute	X-Force Exchange Category

XFE OBJECT	XFE TYPE	OBJECT PATH	XFE KEY	CREATE INDICATOR (Y OR N)	CREATE ATTRIBUTE (Y OR N)	V2 PATH	V2 KEY
Attachment	MAL	attachment.report.data.risk	Numeric 1-10	N	Y	indicator.attribute	X-Force Exchange Risk
Attachment	MAL	***By virtue of type MAL***	MAL	N	N	indicator.class	Host
Attachment	MAL	attachments.report.title HASH length	title	Y	N	indicator.value	
Attachment	MAL	attachments.report.title HASH length	title	N	N	indicator.type	Hash type (like MD5, SHA1, etc)
Malware Report	MAL	malware.origins.external.detectionCoverage	detectionCoverage	N	Y	indicator.attribute	X-Force Exchange Detection Coverage
Malware Report	MAL	malware.origins.external.family[]	spyware, heuristic, trojan	N	Y	indicator.attribute	X-Force Exchange Malware Family
Attachment	File	***If 'file' exists*** attachments.md5checksum	checksum	Y	N	indicator.value	
Attachment	File	attachments.file.length	filesize	N	N	file.attribute	File Size
Attachment	File	attachments.file.content_type	content_type	N	N	file.attribute	File Type
Attachment	File	attachments.file.filename	filename	N	N	file.attribute	File Name
Attachment	File	attachments.aliasFileName	filename	N	N	file.attribute	File Name

All indicators are related to a specific collection. An indictor will not be processed or picked up if it is not part of a collection. Each indicator can discover another family of indicators, although, at this time, they are ignored.

Attachment Types

Attachment Types are based off of report.type within an attachment.

> The file is also included as an attachment.

TYPE	DESCRIPTION	EXAMPLES
IAP	Internet Application Profile	"HTTP_TeslaCrypt3_Trojan_CnC", "SNMP_CiscoASA_Oid_Overflow", "HTML_MScomctl_ASLR_Bypass", "ActiveX_Blocked", "ISAKMP_CiscoASA_Fragmentation_Overflow", "DNS_Glibc_GetAddrInfo_Overflow", "PSC_Protocol_Overflow", "HTTP_DLink_Command_Exec", "HTTP_AuthResponse_Possible_CSRF", "HTTP_Apache_Struts2_Exec", "JavaObjectStream_TraxTemplates_Exec", "Image_PNG_VLC_Media_Player_DoS", "Cross_Site_Scripting", "DNS_Response_Flood_DoS", "SYNFlood", "UDP_Flood_DoS", "TCP_Connections_Rate_Flood", "TCP_Connections_Open_Flood", "SYNFlood_Protection", "SYN_Bandwidth_Flood", "SYN_Bandwidth_Flood_Protection", "JavaScript_Angler_Exploit_Kit", "JavaScript_Angler_Exploit_Kit_2", "TCP_Cisco_Implant_CnC"
VUL	Vulnerability	CVE-XXXX-XXXXX, Apache DDoS, etc
BOTNET	Bot Net	"ponyloader", "betabot", "locky"
MWF	Malware Family	ponyloader", "Spam Zero-Day", "dridex", "dyreza"
PAM	Unknown	"TCP_Connections_Open_Flood", "SYNFlood_Protection", SYN_Bandwidth_Flood", "SYN_Bandwidth_Flood_Protection", "JavaScript_Angler_Exploit_Kit", "JavaScript_Angler_Exploit_Kit_2", "TCP_Cisco_Implant_CnC"
IP	IP Address v4	X.X.X.X
URL	URL	ddosprotected.eu, http://www.iotcall.com/rankup_module/rankup_board/watermark/cccc.apk, http:%2F%2Fcount11.51yes.com%2Fclick.aspx?id=115861800&logo=7, http://count19.51yes.com/click.aspx?id=193675419&logo=1, acvpnefczejny.onedumb.com, http://bridepopmississippi.com

Change Log

- **Version 1.4.3**
  - Fixed a bug that occurred when trying to ingest events with private IPs.
- **Version 1.4.2**
  - Fixed a bug that occurred when XFE downloaded a file and added a password to it.
  - Fixed an error that occurred when attempting to check if an IP address was private.
- **Version 1.4.1**
  - Added arguments to execute the connector with historical start and end dates.
  - Added the ability to filter out private IPs.
  - Resolved an issue where an incorrect reference to a dictionary key from fdict['file']['size'] to fdict['file']['length'].
- **Version 1.4.0**
  - Added Python 3 support.
- **Version 1.3.2**
  - Resolved an issue where the connector did not fetch information about indicators with .tmp file extensions in the URL.
- **Version 1.3.1**
  - Zero-width space is now stripped form report titles.
- **Version 1.3.0**
  - Added support for external proxy.
- **Version 1.1.2**
  - Resolved HTTPError Import error.
  - Resolved OS import error.
- **Version 1.1.1**
  - Resolved issue with Exchange type during event creation
  - Updated integration to use new ThreatQ SDK
- **Version 1.0.0**
  - Initial Release