

ThreatQuotient



FS-ISAC CDF User Guide

Version 1.0.0

August 29, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

Average Feed Run..... 11

Known Issues / Limitations 12

Change Log 13

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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	1.0.0
Compatible with ThreatQ Versions	>= 4.58.0
Support Tier	ThreatQ Supported

Introduction

FS-ISAC is an intelligence sharing community for financial services organizations. FS-ISAC provides feeds to their members containing intelligence surrounding threats targeting their industry. The FS-ISAC CDF enables the automatic ingestion of FS-ISAC feeds into ThreatQ. This integration acts as a TAXII client, fetching data from FS-ISAC's TAXII server based on a user-configured collection, parsing the intelligence, and ingesting it into ThreatQ. This feed adds additional features on top of ThreatQ's basic TAXII client functionality including, but not limited to, parsing object relationships out of STIX labels.

The integration provides the following feed:

- **FS-ISAC** - ingests intelligence from the FS-ISAC TAXII server.

The integration ingests the following system objects:

- Adversaries
- Attack Pattern
- Campaign
- Course Of Action
- Event
- Exploit Target
- Identity
- Incident
- Indicators
- Intrusion Set
- Malware
- Report
- Signatures
- Tools
- TTP

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

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 **STIX/TAXII** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
TAXII Server Version	Select the server version to poll data.
Discovery Path URL	Enter the path to the TAXII Server's Discovery Service. Options include: ◦ 2.1 - https://taxii.fsisac.com/ctixapi/ctix21/taxii2/ (default) ◦ 2.0 - https://taxii.fsisac.com/ctixapi/ctix2/taxii/
Collection Name	Enter the collection name to poll.
Disable Proxies	If enabled, the feed will not honor proxy settings set in ThreatQ.
Username	Enter your basic authentication username for FS-ISAC.
Password	Enter the password associated with the username above.
Verify SSL	Enable this parameter if the TAXII client should verify the provider's SSL certificate.

PARAMETER

DESCRIPTION

Host CA Certificate Bundle

Paste the certificate bundle in this field if you enabled the **Verify SSL** parameter.

< FS-ISAC CDF



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Configuration

Activity Log

TAXII Server Version

2.0

The version of the TAXII Server to poll for data.

Discovery Path URL

<https://taxii.fsisac.com/ctixapi/ctix21/taxii2/>

Path to the TAXII Server's Discovery Service. For TAXII 2.1, <https://taxii.fsisac.com/ctixapi/ctix21/taxii2/>. For TAXII 2.0, <https://taxii.fsisac.com/ctixapi/ctix2/taxii/>

Collection Name

Name of the collection to poll data from

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Username

Basic Authentication Username

Password

Basic Authentication Password

☒ Verify SSL

Specifies whether the TAXII client should verify a provider's SSL certificate

Host CA Certificate Bundle

Used to specify a provider's CA Certificate Bundle to verify SSL against. This denotes that Verify SSL is True.

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.

ThreatQ Mapping

This integration ingests intelligence from the FS-ISAC TAXII server.



The majority of the parsing & mapping of the data is handled by the ThreatQ's generic STIX parser. See the STIX 2.0 Data Mapping topic for further details.

In addition, labels containing links to other entities will be converted into their corresponding object relationships. For instance:

- `malware:Lokibot` -> A *Malware* object with the value, `Lokibot`
- `threat-actor:APT28` -> An *Adversary* object with the value, `APT28`
- `attack-pattern:T1059` -> An *Attack Pattern* object with the value, `T1001 - Data Obfuscation`

Average Feed 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	1 minute
Indicators	17
Indicator Attributes	31
Adversaries	4
Malware	10

Known Issues / Limitations

- You will need to create multiple feeds in order to ingest from multiple collections. This requires that you install multiple instances of this integration. To do this, you will need to modify both the feed name and namespace in the yaml file for each instance of the feed to avoid conflicts. These values must be unique.

To generate a Unique ID for Namespace:

1. Open up a terminal window.
2. Enter the following command:

```
uuidgen | tr "A-Z" "a-z"
```

Example Output:

```
uuidgen | tr "A-Z" "a-z"
b522dfcb-fe6c-4540-a8ed-76751d9bc8b0
```

3. Copy and paste that unique ID to use as the new **namespace**.
4. Enter the new feed name.

Example: FS-ISAC CDF > FS-ISAC CDF Collection 2

Original Name and Namespace

```
111 feeds:
112   FS-ISAC CDF:
113   namespace: 1f6d3a90-0b58-4c7f-8814-31e23e7ef700
```

Updated Name and Namespace

```
111 feeds:
112   FS-ISAC CDF Collection 2:
113   namespace: b522dfcb-fe6c-4540-a8ed-76751d9bc8b0
```

5. Save the yaml file and proceed with the standard CDF install steps described in this guide.

Change Log

- Version 1.0.0
 - Initial release