FS-ISAC® Integration

Installation and Configuration Guide

Software Version 1.0

July 28, 2021

30073-03 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203
P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

Table of Contents

OVERVIEW

The ThreatConnect® integration with the Financial Services Information Sharing and Analysis Center (FS-ISAC) ingests Indicators from the FS-ISAC STIX™/TAXII™ 2.1 Server into ThreatConnect, enabling analysts to access the context and awareness of ThreatConnect on industry-specific Indicators, as well as to take action quickly and effectively. The integration allows users to choose and ingest high-, medium-, and low- confidence collections as a single feed in ThreatConnect.

DEPENDENCIES

ThreatConnect Dependencies

- ThreatConnect version 5.8 or newer
- Active ThreatConnect Application Programming Interface (API) key

NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration on the Account Settings screen within their Private Instance of ThreatConnect.

FS-ISAC Dependencies

- Active FS-ISAC membership and API credentials

APPLICATION SETUP AND CONFIGURATION

System Administrators should use the ThreatConnect Feed Deployer to set up and configure the FS-ISAC Feed app. See the "Feed Deployment" sub-section of the "Apps and Jobs" section of the *ThreatConnect System Administration Guide* for instructions on how to use the Feed Deployer. On the **Confirm** screen, uncheck the **Run Jobs after deployment** and **Activate Jobs after deployment** checkboxes. It is highly recommended to review the app configuration prior to running or activating the Job.

CONFIGURATION PARAMETERS

Parameter Definition

The parameters defined in Table 1 apply to the configuration parameters during the job-creation process.

Table 1

Name	Description
API User	This parameter is the name of the API user account running the app.
FS-ISAC API Username	This parameter is the FS-ISAC API Access ID.
FS-ISAC API Key	This parameter is the FS-ISAC API Secret Key.
Destination Owner	This parameter is the Source in which the Indicators will be saved in ThreatConnect.
Target Collections	This parameter is the set of collections to be imported into ThreatConnect from FS-ISAC.
Advanced Settings	This parameter allows for additional advanced settings to be configured. (See the “Advanced Settings” section for more information)
Last Run	This parameter is the epoch time of the last time this job ran successfully.
Logging Level	This parameter is the logging level for the app.

DATA MAPPING

The data mapping in Table 2 illustrates how data are mapped from the FS-ISAC STIX/TAXII feed into Indicator objects in ThreatConnect.

Table 2

FS-ISAC STIX Field	ThreatConnect Field
id	Attribute: "External ID"
pattern	Indicator: Title
confidence	Indicator: Confidence Rating
lang	N/A
type	N/A"
created	Attribute: "External Date Created"
modified	N/A
name	Attribute: "Description", "STIX Title"
valid_from	N/A"
pattern_type	N/A
object_marking_refs	Security Label
labels	Tags
created_by_ref	N/A

indicator_types	Attribute: "STIX Indicator Type"
pattern_version	N/A
spec_version	N/A

Advanced Settings

WARNING: This feature is for advanced users and requires an understanding of the individual settings available. It is possible to do damage to your ThreatConnect instance with some Advanced Settings configurations. Please consult your Customer Success Engineer before editing these settings.

The values in Table 3 are available for configuration in Advance Setting. Use a pipe delimiter "|" to separate keys when adding multiple advanced settings.

Table 3

Key	Value
first_run	Boolean (denoting whether this job execution will be the first time the job has been run)
threat_rating	Integer 0–5 (will be applied to all Indicators)
confidence	Integer 0–100 (will be added only to Indicators that do not have a confidence value set by FS-ISAC)