ThreatConnect™

RH-ISAC Integration

Installation and Configuration Guide

Software Version 1.0

July 16, 2019

30047-02 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 Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC) ingests Indicators from the TruSTAR API into ThreatConnect, enabling analysts to access the context and awareness of ThreatConnect on industry-specific Indicators, as well as take action quickly and effectively. The integration ingests Vetted and Non-Vetted Enclaves as separate feeds in ThreatConnect. The Vetted Source contains Indicators (Address, File, Host, and URL) only, while the Non-Vetted Source contains Reports and Indicators. Once a vetted Indicator is in ThreatConnect, it is easy to see the connection between the Indicator and the original report from which it was collected.

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 customer. Private Instance customers can enable these settings during configuration on the** Account Settings **screen within their Private Instance of ThreatConnect.

RH-ISAC Dependencies

Active RH-ISAC membership and API key

APPLICATION SETUP AND CONFIGURATION

System Administrators should use the ThreatConnect Feed Deployer to set up and configure the RH-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.
RH-ISAC API ID	This parameter is the RH-ISAC (TruSTAR Platform) API Access ID.
RH-ISAC API Key	This parameter is the RH-ISAC (TruSTAR Platform) API Secret Key.
Destination Owner	This parameter is the Source in which the Indicators will be saved in ThreatConnect.
ThreatConnect Confidence Value for each indicator	This parameter is the Confidence Rating that will be applied to all Indicators for this integration in ThreatConnect.
Logging Level	This parameter is the logging level for the app.
Last Run	This parameter is the epoch time of the last time this job ran successfully.

DATA MAPPING

The data mappings in Table 2 and Table 3 illustrate how data are mapped from the RH-ISAC (TruSTAR Platform) API endpoints into Report and Indicator objects, respectively, in ThreatConnect.

Reports

Table 2

TruSTAR API Field	ThreatConnect Field
id	Attribute: "External ID"
created	Report: Publish Date
updated	Attribute: "External Date Last Modified"
title	Report: Name
sector.label	Attribute: "TruSTAR Sector"
timeBegan	Attribute: "TruSTAR Time Began"
reportBody	Report: Attachment
externalTrackingId	Attribute: "TruSTAR External Tracking ID"
enclaveIds	Attribute:" TruSTAR Enclave"

Indicators

Table 3

TruSTAR API Field	ThreatConnect Field
indicatorType	Indicator: Type
value	Indicator: Value
priorityLevel	Rating (Low=2, Medium=3, High=4)
sightings	Attribute: "External Sightings"
firstSeen	Attribute: "First Seen"
lastSeen	Attribute: "Last Seen"
enclaveIds	Attribute: "TruSTAR Enclave"
tags	Tags
source	Attribute: "Source"
notes	Attribute: "TruSTAR Note"