ThreatConnect™

Flashpoint® Risk Intelligence Observables Integration

Configuration Guide

Software Version 1.0

August 6, 2019

30044-02 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 Flashpoint Risk Intelligence Observables ingests Flashpoint RIO Torrent IPs and Forum Visitor IPs into ThreatConnect. These RIO Indicators are stored in ThreatConnect with all relevant context, enabling analysts to better understand and make connections between the threats and adversaries they are facing.

DEPENDENCIES

ThreatConnect Dependencies

- ThreatConnect version 5.6 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.

Flashpoint Dependencies

- Active Flashpoint v4 Application Programming Interface (API) key

Organization Configuration

Use the ThreatConnect Feed Deployer to set up and configure the Flashpoint Risk Intelligence Observables app, or follow the steps in the "Creating a Source" section of the ***ThreatConnect Account Administration Guide*** to create and configure the Flashpoint Risk Intelligence Observables Source, the “Creating API Accounts” section of the ***ThreatConnect Organization Administration Guide*** to generate an API key set for the ThreatConnect Organization, and the “Creating a Job” section of the ***ThreatConnect Organization Administration Guide*** to add a Job, which will activate the Flashpoint Risk Intelligence Observables app and pull down Indicators.

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.
Flashpoint API Token	This parameter is the Flashpoint API token.
Destination Owner	This parameter is the ThreatConnect owner to which the imported Indicators will belong.
Threat Rating	This parameter is the Threat Rating for the imported Indicators.
Threat Confidence	This parameter is the Confidence Rating for the imported Indicators.
Flashpoint Intelligence Dataset	This parameter is the Flashpoint RIO feed to download. Possible choices are Forums or Torrent.
Last Run	This parameter is the last time the job ran successfully. On first run of the job, this parameter is used to go back the specified number of days.
Verify External SSL Certificate	This parameter forces the validation of the external SSL certificate.

DATA MAPPING

The data mapping in Table 2 illustrates how Flashpoint RIO Torrent IP data are mapped from Flashpoint API endpoints into ThreatConnect's data model.

Table 2

Flashpoint API Field	ThreatConnect Field
ingested_at	Attribute: "Date/Time of Observed Activity"
ip_address.isp	Attribute: "Hosting Provider"
ip_address.city	Attribute: "IP Geo City"
ip_address.country	Attribute: "IP Geo Country"
ip_address.latitude	Attribute: "IP Geo Latitude"
ip_address.longitude	Attribute: "IP Geo Longitude"
ip_address.domain	Attribute: "IP Hostname"
torrent	Attribute: "Torrent Filename"
embed.torrent.hash	Attribute: "Torrent Hash"
torrent_id	Attribute: "Torrent Number"

The data mapping in Table 3 illustrates how Flashpoint RIO Forum Visitor IP data are mapped from Flashpoint API endpoints into ThreatConnect's data model.

Table 3

Flashpoint API Field	ThreatConnect Field
hit_at	Attribute: "Date/Time of Observed Activity"
ip_address.isp	Attribute: "Hosting Provider"
ip_address.city	Attribute: "IP Geo City"
ip_address.country	Attribute: "IP Geo Country"
ip_address.latitude	Attribute: "IP Geo Latitude"
ip_address.longitude	Attribute: "IP Geo Longitude"
ip_address.domain	Attribute: "IP Hostname"
forum_name	Attribute: "Forum Name"
threat_title	Attribute: "Forum Thread Title"
thread_id	Attribute: "Forum Thread Number"
request_headers.referer	Attribute: "Referrer URL"