ThreatConnect™

Flashpoint® Intelligence Reports Integration

Installation and Configuration Guide

Software Version 1.0

July 18, 2019

30045-02 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 4

DEPENDENCIES 4

ThreatConnect Dependencies 4
Flashpoint Dependencies 4

APPLICATION SETUP AND CONFIGURATION 4

CONFIGURATION PARAMETERS 5

Parameter Definition 5

DATA MAPPING 7

Reports 7
Technical Indicators 8

OVERVIEW

The ThreatConnect® integration with Flashpoint ingests Flashpoint Intelligence Reports (Cyber and Physical Threats) and Technical Indicators into ThreatConnect. The reports are searchable and stored in ThreatConnect, with the full HTML version available for viewing. Technical Indicators are associated to the reports and contain additional context for research and monitoring, such as MITRE ATT&CK™ Tags. See the ThreatConnect Knowledge Base article "MITRE ATT&CK" for more information on how MITRE ATT&CK classifications are represented in ThreatConnect.

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
- Active subscription to Flashpoint Intelligence Reports

APPLICATION SETUP AND CONFIGURATION

System Administrators should use the ThreatConnect Feed Deployer to set up and configure the Flashpoint Intelligence Reports 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.

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.
Collect reports	This parameter toggles the collection of Reports on and off.
Collect events/indicators	This parameter toggles the collection of Events and Indicators on and off.
Convert existing documents to reports	If Document Group objects still exist in the Flashpoint Intelligence Reports Source from an older version of the integration, this parameter toggles on a feature that will convert these Documents into Reports and clean up the data.
Destination Owner	This parameter is the ThreatConnect owner to which the imported Indicators will belong.
Threat Rating	This parameter is the default Threat Rating for all Indicators created in ThreatConnect.

Confidence Rating	This parameter is the default Confidence Rating for all Indicators created in ThreatConnect.
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

Reports

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

Table 2

Flashpoint API Field	ThreatConnect Field
Title	document: name Attribute: "Title"
tags	Tags
summary	Attribute: "Description"
id platform_url	Attribute: "External ID"
body	File Attachment (HTML)
sources[*].title sources[*].original	Attribute: "Source"
posted_at	Attribute: "Creation Date

Technical Indicators

The data mapping in Table 3 illustrates how Flashpoint Technical Indicators data are mapped from MISP API endpoints into ThreatConnect's data model.

Table 3

MISP API Field	ThreatConnect Field
[*]['Event']['date']	Incident: Event Date
[*]['Event']['info']	Incident: Title
[*]['fpid']	Incident: Attribute: "External ID"
[*]['href']	Incident: Attribute: "Source"
[*]['Event']['Tag']	Incident: Tag
[*]['Event']['Attribute'][*]['value']	Indicator
[*]['Event']['Attribute'][*]['comment']	Indicator: Attribute: "Description"
[*]['Event']['Attribute'][*]['fpid']	Indicator: Attribute: "External ID"
[*]['Event']['Attribute'][*]['href']	Indicator: Attribute: "Source"
[*]['Event']['Attribute'][*]['category'] and [*]['Event']['Attribute'][*]['type']	Indicator: Tag