CrowdStrike® Falcon Intelligence™ Engine Integration User Guide

Software Version 1.0

Integration Guide

February 2, 2023

30039-07 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

The ThreatConnect® integration with CrowdStrike Falcon Intelligence allows ThreatConnect customers to import information Reports, Indicators, Signatures, Vulnerabilities, and Actors, along with all of their context, from the CrowdStrike Falcon Intelligence feed into ThreatConnect.

The following Indicator types are currently supported: Address, Email Address, File, Host, URL, Email Subject, Mutex, and Registry Key. Indicators are associated with Report and Intrusion Set Groups in ThreatConnect. Reports are also associated with Intrusion Set Groups in ThreatConnect.

Dependencies

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) key

Note: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On-Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

Falcon Intelligence Dependencies

- Active subscription to CrowdStrike Falcon Intelligence with API key

Application Setup and Configuration

1. Install the **CrowdStrike Falcon Intelligence Engine** App via TC Exchange™.
2. Use the ThreatConnect Feed Deployer to set up and configure the **CrowdStrike Falcon Intelligence Engine** App.

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters available when using the Feed Deployer to configure the App.

Table 1

Name	Description	Required?
Sources to Create	The name of the Source to be created.	Yes
Owner	The Organization in which the Source will be created.	Yes
Activate Deprecation	Select this checkbox to allow the creation of depreciation rules for Indicators in the Source.	No
Create Attributes	Select this checkbox to allow the creation of custom Attribute Types in the Source.	No
Launch Server	Select the server on which the Service corresponding to the Feed API Service App will launch. It is recommended to select **tc-job.**	Yes
CrowdStrike API Endpoint	Select the CrowdStrike environment from which to retrieve data.	Yes
CrowdStrike Falcon Intelligence API ID	The CrowdStrike API ID.	Yes
CrowdStrike Falcon Intelligence API Secret	The CrowdStrike API secret key.	Yes

Group Types	Select the Group type(s) to import from CrowdStrike.	Yes
Indicator Types	Select the Indicator type(s) to import from CrowdStrike.	Yes

CrowdStrike Falcon Intelligence Engine

After successfully configuring and activating the Feed API Service, you can access the CrowdStrike Falcon Intelligence Engine user interface (UI). This UI allows you to interact with and manage the CrowdStrike Falcon Intelligence integration.

Follow these steps to access the CrowdStrike Falcon Intelligence Engine UI:

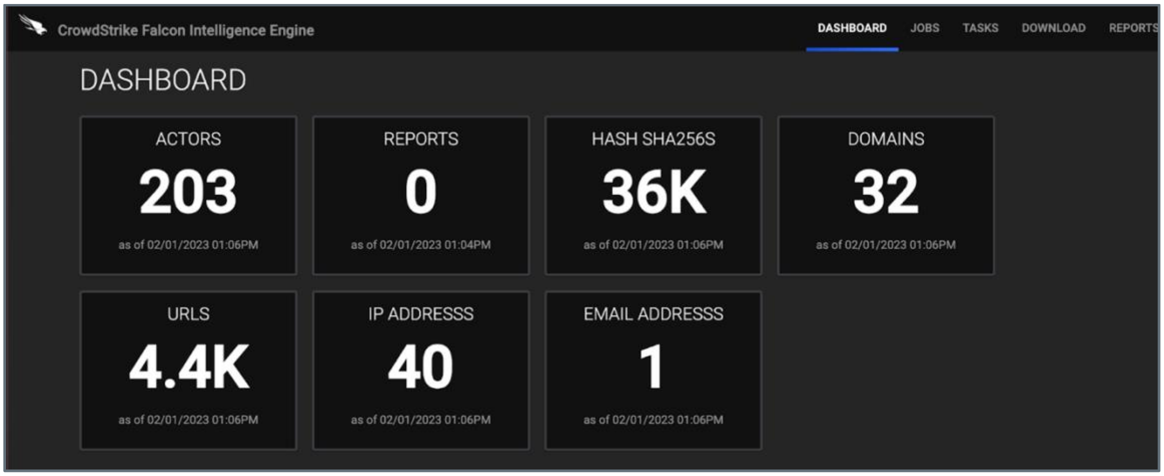
1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover over **Playbooks** and select **Services.** The **Services** tab of the **Playbooks** screen will be displayed.
3. Locate the **CrowdStrike Falcon Intelligence Engine** Feed API Service and then click the link in the Service's **API Path** field. The **DASHBOARD** screen of the CrowdStrike Falcon Intelligence Engine UI will open in a new browser tab.

The following screens are available in the CrowdStrike Falcon Intelligence Engine UI:

- **DASHBOARD**
- **JOBS**
- **TASKS**
- **DOWNLOAD**
- **REPORT**

DASHBOARD

The **DASHBOARD** screen (Figure 1) provides an overview of the total number of Actors, Reports, Hashes, Domains, IP Addresses, and Email Addresses retrieved from CrowdStrike.



DASHBOARD

ACTORS
203
as of 02/01/2023 01:06PM

REPORTS
0
as of 02/01/2023 01:04PM

HASH SHA256S
36K
as of 02/01/2023 01:06PM

DOMAINS
32
as of 02/01/2023 01:06PM

URLS
4.4K
as of 02/01/2023 01:06PM

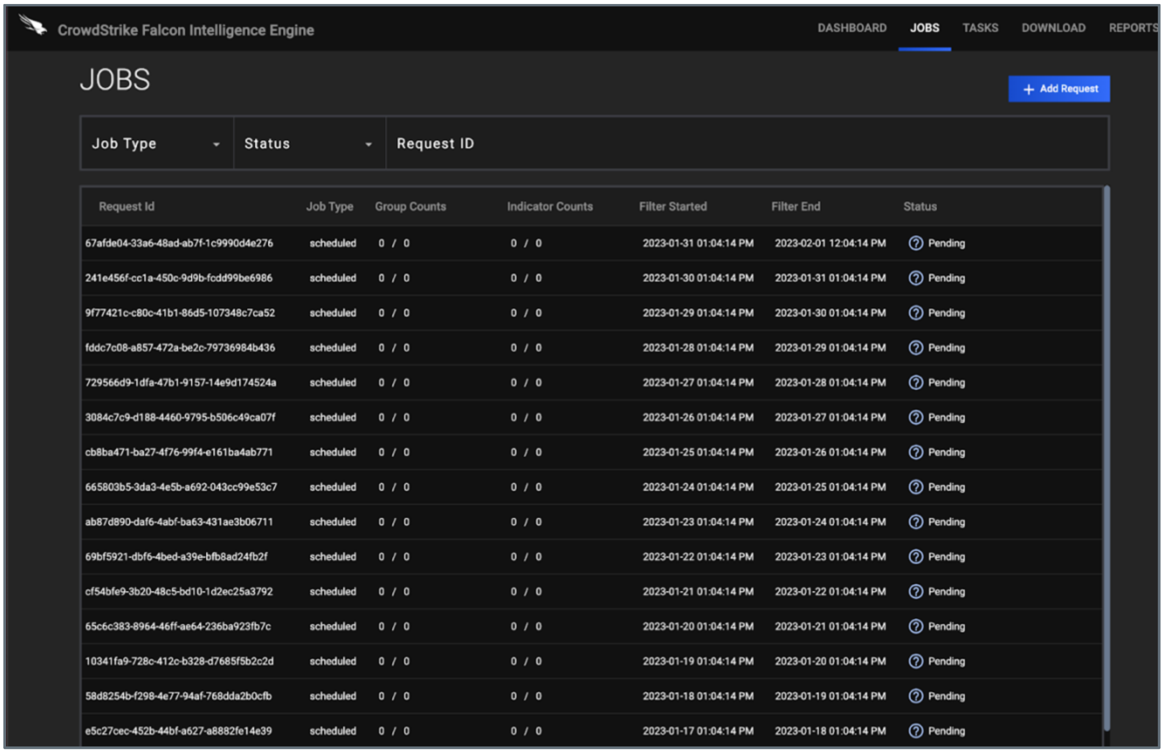
IP ADDRESSS
40
as of 02/01/2023 01:06PM

EMAIL ADDRESSS
1
as of 02/01/2023 01:06PM

Figure 1

JOBS

The **JOBS** screen (Figure 2) breaks down the ingestion of CrowdStrike data into manageable Job-like tasks.

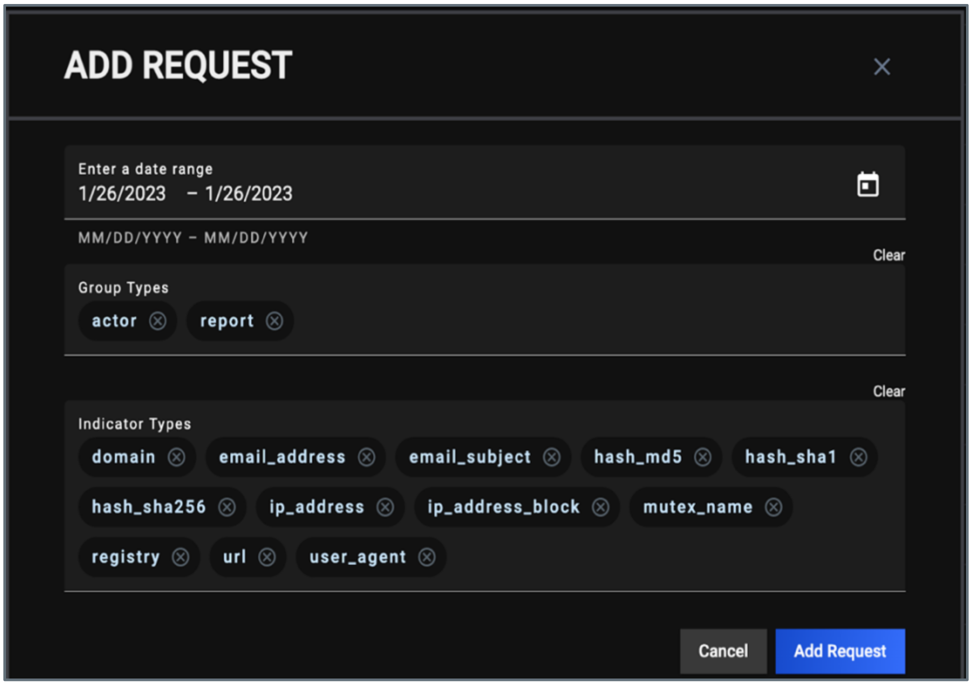


Request Id	Job Type	Group Counts	Indicator Counts	Filter Started	Filter End	Status
67afde04-33a6-48ad-ab7f-1c9990d4e276	scheduled	0 / 0	0 / 0	2023-01-31 01:04:14 PM	2023-02-01 12:04:14 PM	ⓘ Pending
241e456f-cc1a-450c-9d9b-fcdd99be6986	scheduled	0 / 0	0 / 0	2023-01-30 01:04:14 PM	2023-01-31 01:04:14 PM	ⓘ Pending
9f77421c-c80c-41b1-86d5-107348c7ca52	scheduled	0 / 0	0 / 0	2023-01-29 01:04:14 PM	2023-01-30 01:04:14 PM	ⓘ Pending
fddc7c08-a857-472a-be2c-79736984b436	scheduled	0 / 0	0 / 0	2023-01-28 01:04:14 PM	2023-01-29 01:04:14 PM	ⓘ Pending
729566d9-1dfa-47b1-9157-14e9d174524a	scheduled	0 / 0	0 / 0	2023-01-27 01:04:14 PM	2023-01-28 01:04:14 PM	ⓘ Pending
3084c7c9-d188-4460-9795-b506c49ca07f	scheduled	0 / 0	0 / 0	2023-01-26 01:04:14 PM	2023-01-27 01:04:14 PM	ⓘ Pending
cb8ba471-ba27-4f76-99f4-e161ba4ab771	scheduled	0 / 0	0 / 0	2023-01-25 01:04:14 PM	2023-01-26 01:04:14 PM	ⓘ Pending
665803b5-3da3-4e5b-a692-043cc99e53c7	scheduled	0 / 0	0 / 0	2023-01-24 01:04:14 PM	2023-01-25 01:04:14 PM	ⓘ Pending
ab87d890-daf6-4abf-ba63-431ae3b06711	scheduled	0 / 0	0 / 0	2023-01-23 01:04:14 PM	2023-01-24 01:04:14 PM	ⓘ Pending
69bf5921-dbf6-4bed-a39e-bfb8ad24fb2f	scheduled	0 / 0	0 / 0	2023-01-22 01:04:14 PM	2023-01-23 01:04:14 PM	ⓘ Pending
cf54bfe9-3b20-48c5-bd10-1d2ec25a3792	scheduled	0 / 0	0 / 0	2023-01-21 01:04:14 PM	2023-01-22 01:04:14 PM	ⓘ Pending
65c6c383-8964-46ff-ae64-236ba923fb7c	scheduled	0 / 0	0 / 0	2023-01-20 01:04:14 PM	2023-01-21 01:04:14 PM	ⓘ Pending
10341fa9-728c-412c-b328-d7685f5b2c2d	scheduled	0 / 0	0 / 0	2023-01-19 01:04:14 PM	2023-01-20 01:04:14 PM	ⓘ Pending
58d8254b-f298-4e77-94af-768dda2b0cfb	scheduled	0 / 0	0 / 0	2023-01-18 01:04:14 PM	2023-01-19 01:04:14 PM	ⓘ Pending
e5c27cec-452b-44bf-a627-a8882fe14e39	scheduled	0 / 0	0 / 0	2023-01-17 01:04:14 PM	2023-01-18 01:04:14 PM	ⓘ Pending

Figure 2

- **Job Type:** If desired, select a Job type by which to filter Jobs. Available types include **ad-hoc** and **scheduled**.
- **Status:** If desired, select a Job status by which to filter Jobs. Available statuses include the following:
  - Convert Complete
  - Convert In Progress
  - Download Complete
  - Download In Progress
  - Upload Complete
  - Upload In Progress

- **Request ID:** If desired, enter text into this box to search for a specific Job by its request ID.
- **+ Add Request**: Click this button to display the **ADD REQUEST** window (Figure 3). On this window, you can specify the date range, Group types, and Indicator types for an ad-hoc Job request. After a Job request is added, it will be displayed in the table on the **JOBS** screen (Figure 2), and its Job type will be listed as **ad-hoc**.



ADD REQUEST

Enter a date range
1/26/2023 – 1/26/2023

MM/DD/YYYY – MM/DD/YYYY

Clear

Group Types
actor ⊗ report ⊗

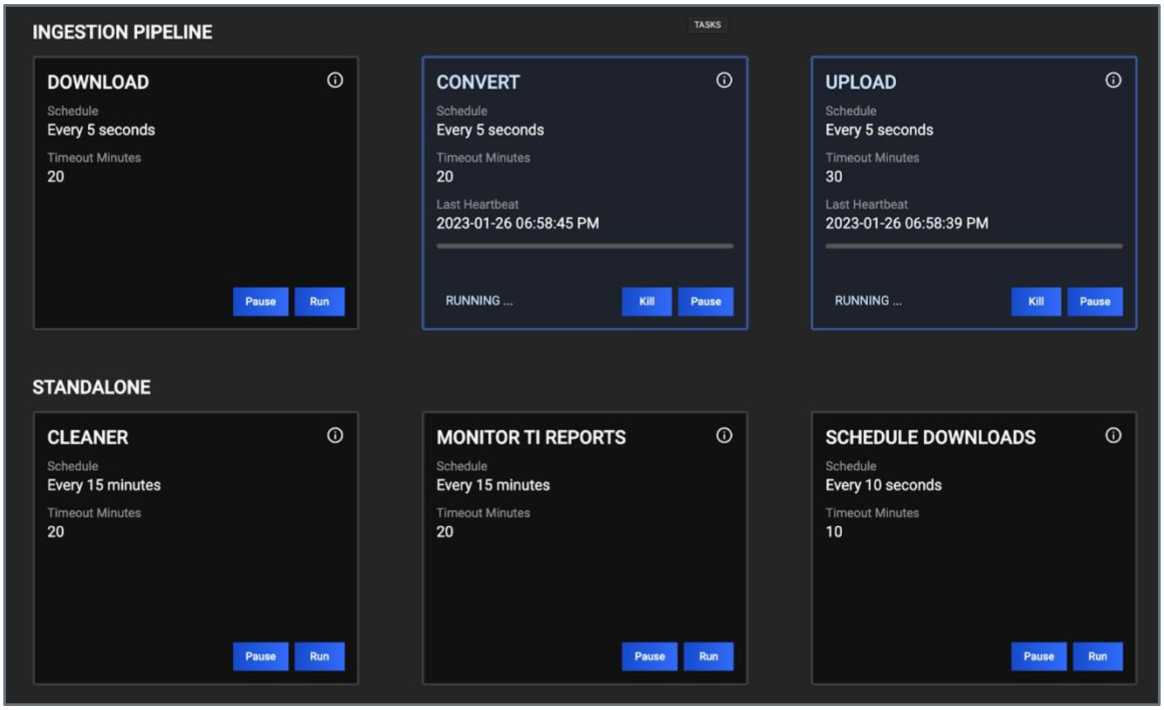
Clear

Indicator Types
domain ⊗ email_address ⊗ email_subject ⊗ hash_md5 ⊗ hash_sha1 ⊗ hash_sha256 ⊗ ip_address ⊗ ip_address_block ⊗ mutex_name ⊗ registry ⊗ url ⊗ user_agent ⊗

Figure 3

TASKS

The **TASKS** screen (Figure 4) is where you can view and manage the Tasks for each Job.



INGESTION PIPELINE

DOWNLOAD
Schedule
Every 5 seconds
Timeout Minutes
20

CONVERT
Schedule
Every 5 seconds
Timeout Minutes
20
Last Heartbeat
2023-01-26 06:58:45 PM
RUNNING ...

UPLOAD
Schedule
Every 5 seconds
Timeout Minutes
30
Last Heartbeat
2023-01-26 06:58:39 PM
RUNNING ...

STANDALONE

CLEANER
Schedule
Every 15 minutes
Timeout Minutes
20

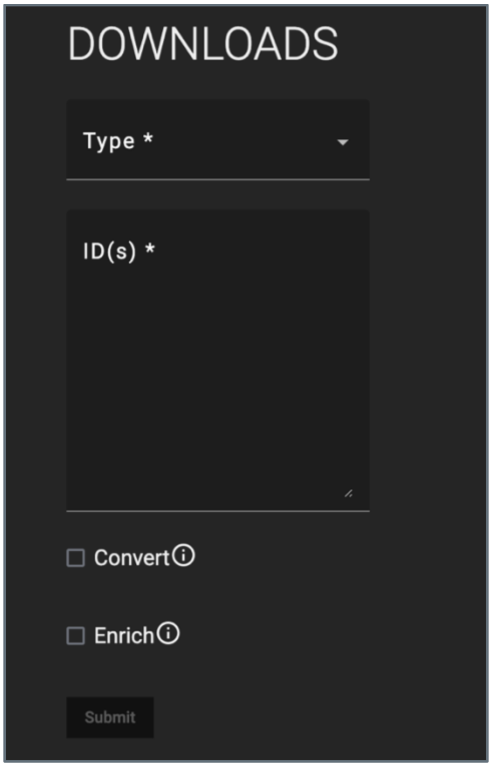
MONITOR TI REPORTS
Schedule
Every 15 minutes
Timeout Minutes
20

SCHEDULE DOWNLOADS
Schedule
Every 10 seconds
Timeout Minutes
10

Figure 4

DOWNLOADS

The **DOWNLOADS** screen (Figure 5) is where you can view data for Indicators, Actors, and Reports exactly as they appear in CrowdStrike.



DOWNLOADS

Type *

ID(s) *

□ Convert ⓘ

□ Enrich ⓘ

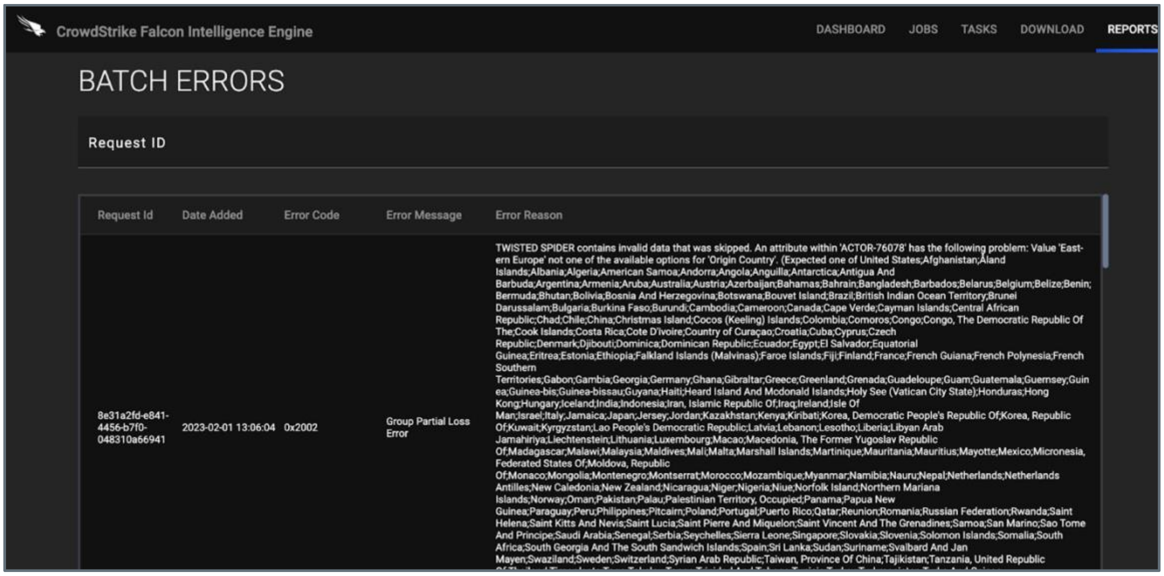
Submit

Figure 5

- **Type**: Select the type of object to download. Available options include **Actor**, **Indicators**, and **Reports**.
- **ID(s)**: Enter the CrowdStrike ID(s) for the object(s) to download. Data will be retrieved in JavaScript® Object Notation (JSON) format.
- **Convert**: Select this checkbox to convert the threat intelligence data to ThreatConnect batch format.
- **Enrich**: Select this checkbox to submit the threat intelligence data to the ThreatConnect Batch API.

REPORTS

The **REPORTS** screen provides two views: **BATCH ERRORS** and **PDF TRACKER**. The **BATCH ERRORS** screen (Figure 6) displays batch errors for each request in a tabular format. Details provided for each error include the error's code, message, and reason.



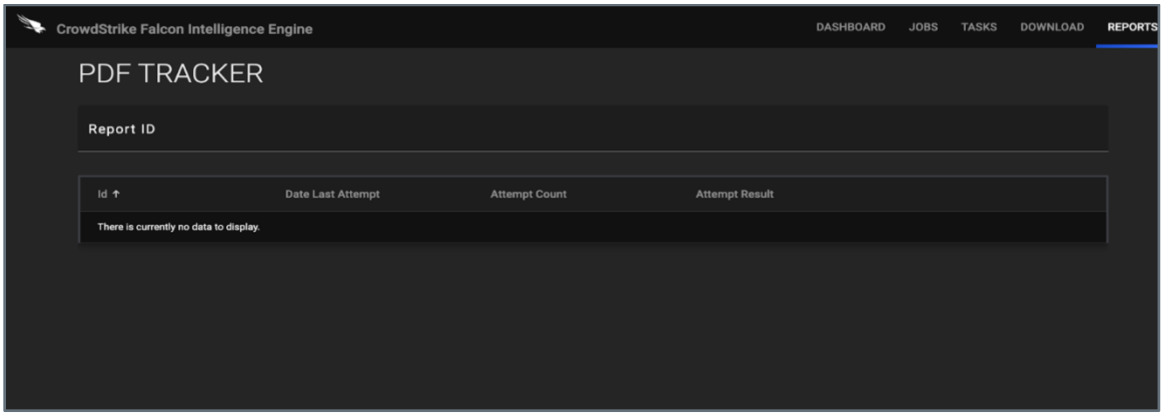
BATCH ERRORS

Request ID

Request Id	Date Added	Error Code	Error Message	Error Reason
8e31a2fd-e841-4456-b7f0-048310a66941	2023-02-01 13:06:04	0x2002	Group Partial Loss Error	TWISTED SPIDER contains invalid data that was skipped. An attribute within 'ACTOR-76078' has the following problem: Value 'Eastern Europe' not one of the available options for 'Origin Country'. (Expected one of United States;Afghanistan;Åland Islands;Albania;Algeria;American Samoa;Andorra;Angola;Anguilla;Antarctica;Antigua And Barbuda;Argentina;Armenia;Aruba;Australia;Austria;Azerbaijan;Bahamas;Bahrain;Bangladesh;Barbados;Belarus;Belgium;Belize;Benin;Bermuda;Bhutan;Bolivia;Bosnia And Herzegovina;Botswana;Bouvet Island;Brazil;British Indian Ocean Territory;Brunei Darussalam;Bulgaria;Burkina Faso;Burundi;Cambodia;Cameroon;Canada;Cape Verde;Cayman Islands;Central African Republic;Chad;Chile;China;Christmas Island;Cocos (Keeling) Islands;Colombia;Comoros;Congo;Congo, The Democratic Republic Of The;Cook Islands;Costa Rica;Cote D'ivoire;Country of Curaçao;Croatia;Cuba;Cyprus;Czech Republic;Denmark;Djibouti;Dominica;Dominican Republic;Ecuador;Egypt;El Salvador;Equatorial Guinea;Eritrea;Estonia;Ethiopia;Falkland Islands (Malvinas);Faroe Islands;Fiji;Finland;France;French Guiana;French Polynesia;French Southern Territories;Gabon;Gambia;Georgia;Germany;Ghana;Gibraltar;Greece;Greenland;Grenada;Guadeloupe;Guam;Guatemala;Guernsey;Guinea;Guinea-bis;Guinea-bissau;Guyana;Haiti;Heard Island And Mcdonald Islands;Holy See (Vatican City State);Honduras;Hong Kong;Hungary;Iceland;India;Indonesia;Iran, Islamic Republic Of;Iraq;Ireland;Isle Of Man;Israel;Italy;Jamaica;Japan;Jersey;Jordan;Kazakhstan;Kenya;Kiribati;Korea, Democratic People's Republic Of;Korea, Republic Of;Kuwait;Kyrgyzstan;Lao People's Democratic Republic;Latvia;Lebanon;Lesotho;Liberia;Libyan Arab Jamahiriya;Liechtenstein;Lithuania;Luxembourg;Macao;Macedonia, The Former Yugoslav Republic Of;Madagascar;Malawi;Malaysia;Maldives;Mali;Malta;Marshall Islands;Martinique;Mauritania;Mauritius;Mayotte;Mexico;Micronesia, Federated States Of;Moldova, Republic Of;Monaco;Mongolia;Montenegro;Montserrat;Morocco;Mozambique;Myanmar;Namibia;Nauru;Nepal;Netherlands;Netherlands Antilles;New Caledonia;New Zealand;Nicaragua;Niger;Nigeria;Niue;Norfolk Island;Northern Mariana Islands;Norway;Oman;Pakistan;Palau;Palestinian Territory, Occupied;Panama;Papua New Guinea;Paraguay;Peru;Philippines;Pitcairn;Poland;Portugal;Puerto Rico;Qatar;Reunion;Romania;Russian Federation;Rwanda;Saint Helena;Saint Kitts And Nevis;Saint Lucia;Saint Pierre And Miquelon;Saint Vincent And The Grenadines;Samoa;San Marino;Sao Tome And Principe;Saudi Arabia;Senegal;Serbia;Seychelles;Sierra Leone;Singapore;Slovakia;Slovenia;Solomon Islands;Somalia;South Africa;South Georgia And The South Sandwich Islands;Spain;Sri Lanka;Sudan;Suriname;Svalbard And Jan Mayen;Swaziland;Sweden;Switzerland;Syrian Arab Republic;Taiwan, Province Of China;Tajikistan;Tanzania, United Republic

Figure 6

The **PDF TRACKER** screen (Figure 7) is where you can view attempts ThreatConnect made to download PDF reports from CrowdStrike. The table on this screen displays the most recent date on which ThreatConnect attempted to download a PDF report, the number of times an attempt to download the report was made, and whether the report was downloaded successfully. You can also search for reports by ID on this screen, which can be useful if you do not see a CrowdStrike PDF report in ThreatConnect as expected.



PDF TRACKER

Report ID

Id ↑	Date Last Attempt	Attempt Count	Attempt Result
There is currently no data to display.			

Figure 7

Data Mappings

The data mappings in Table 2 through Table 8 illustrate how data are mapped from CrowdStrike API endpoints to the ThreatConnect data model.

Reports

ThreatConnect object type: Report Group

Table 2

CrowdStrike API Field	ThreatConnect Field
resources.id	Attribute: "Report ID"
resources.name	Attribute: "Report Title"
resource.slug	N/A
resources.type	Attribute: "Report Type"
resources.sub_type	N/A
resources.url	Attribute: "Source"
resources.short_description	Attribute: "Description"
resources.created_date	Attribute: "External Date Created"
resources.last_modified_date	Attribute: "External Date Last Modified"
resources.thumbnail.url	N/A
resources.actor.id	N/A

resources.actor.name	(Actor Association) **Note**: Actor Association refers to the association between the Report Group object and the Intrusion Set Group object. Customers should expect to see the Actor information as a Group association on the Report Group's **Details** screen.
resources.actor.url	N/A
resources.tags	Tag
resources.target_industries	Attribute: "Target Industry Sector"
resources.target_countries	Attribute: "Target Country"
resources.motivations	Attribute: "Adversary Motivation Type"

Actors

ThreatConnect object type: Intrusion Set Group

Table 3

CrowdStrike API Field	ThreatConnect Field
resources.name	Name/Summary
resources.id	Attribute: "External ID"
resources.url	Attribute: "Source"
resources.description	Attribute: "Description"
resources.created_date	Attribute: "External Date Created"
resources.last_modified_date	Attribute: "External Date Last Modified"
resources.first_activity_date	Attribute: "First Seen"
resources.last_activity_date	Attribute: "Last Seen"
resources.active	Attribute: "Active"
resources.known_as	Attribute: "Aliases" (/n Separated)
resources.motivations	Attribute: "Adversary Motivation Type"
resources.objectives	Attribute: "Goals"
resources.capabilities	Attribute: "Capabilities"

resources.origins	Attribute: "Origin Country"
resources.target_countries	Attribute: "Target Country"
resources.target_industries	Attribute: "Targeted Industry Sector"
resources.kill_chain	Attribute: "Reconnaissance"
	Attribute: "Weaponization"
	Attribute: "Delivery"
	Attribute: "Actions and Objectives"
resources.group	N/A

Indicators

ThreatConnect object type: Indicator (all types)

Table 4

CrowdStrike API Field	ThreatConnect Field
resources.id	Attribute: "External ID"
resources.indicator	Name/Summary
resources.type	Indicator Type
resources.last_updated	Attribute: "External Date Last Modified"
resources.published_date	Attribute: "External Date Created"
resources.malicious_confidence	Confidence Rating
resources._marker	N/A
resources.reports	(Report Association) **Note**: Report Association refers to the association between the Indicator and the Report Group object. Customers should expect to see the Report information as a Group association on the Indicator's **Details** screen.
resources.actors	(Actor Association) **Note**: Actor Association refers to the association between the Indicator and the Intrusion Set Group object. Customers should expect to see the Actor information

	as a Group association on the Indicator’s **Details** screen.
resources.malware_families	N/A
resources.kill_chains	Attribute: "Phase of Intrusion"
resources.labels	Attribute: "Additional Analysis and Context"
resources.domain_types	Tag
resources.ip_address_types	Tag
resources.relations	Attribute: "File Occurrence"
resources.targets	Attribute: "Targeted Industry Sector"
resources.threat_types	Tag
resources.vulnerabilities	Tag

Table 5

malicious_confidence	Threat Rating and Confidence Rating
Unverified	1 skull and 10 Confidence Rating
Low	2 skulls and 40 Confidence Rating
Medium	4 skulls and 75 Confidence Rating
High	5 skulls and 95 Confidence Rating

Malware Families

ThreatConnect object type: Malware Group

Table 6

CrowdStrike API Field	ThreatConnect Field
malware_familes	Tag Attribute: "Name"

Yara Signatures

ThreatConnect object type: Signature Group

Table 7

CrowdStrike API Field	ThreatConnect Field
resources.id	Attribute: "External ID"
resources.name	Tag
resources.type	N/A
resources.short_description	N/A
resources.description	Attribute: "Description"
resources. rich_text_description	N/A
resources. created_date	Attribute: "External Date Created"
resources.last_modified_date	Attribute: "External Date Last Modified"
resources. tags	Tag

Vulnerability

ThreatConnect object type: Vulnerability Group

Table 8

CrowdStrike API Field	ThreatConnect Field
resources.vulnerabilities	Tag

Troubleshooting

The **CrowdStrike Falcon Intelligence Engine** App is a Python®-based App that requires certificate verification. Organizations using SSL inspection solutions will need to import their internal CA certificate to the OS-trusted root certificate store in order for the connection to CrowdStrike to be initiated.