
# CrowdStrike® Falcon Intelligence™ Integration

## User Guide

**Software Version 3.0**

**May 21, 2021**

30039-06 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 CrowdStrike Falcon Intelligence allows ThreatConnect customers to import information Reports, Indicators, 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 Reports and Adversaries in ThreatConnect. Reports are also associated with Adversaries 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. Private Instance customers can enable these settings during configuration on the** Account Settings **screen within their Private Instance of ThreatConnect.***

## Falcon Intelligence Dependencies

- Active subscription to CrowdStrike Falcon Intelligence with API key

# APPLICATION SETUP AND CONFIGURATION

1. Install the app in TC Exchange™.
2. Use the ThreatConnect Feed Deployer to set up and configure the CrowdStrike Falcon Intelligence integration.

   ***NOTE: It is essential that the* Run Jobs after deployment *and* Activate Jobs after deployment *checkboxes on the* Confirm *page of the Feed Deployer are unchecked.***

# 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. |
| Destination Owner | This parameter is the name of the Falcon Intelligence Source. |
| Indicator Types | This parameter is the Indicator type(s) to import from CrowdStrike. |
| CrowdStrike API ID | This parameter is the CrowdStrike API ID. |
| CrowdStrike API Key | This parameter is the CrowdStrike API key. |
| Last Run | Upon initial configuration, this parameter is how far back the app should pull Indicators on the first run. Reports and Actors will be downloaded in entirety on first run. After the first successful run of a job, this parameter will be updated to the last time the job ran successfully. The following formats are supported:<br>• Human Input (e.g., 30 days ago, last Friday)<br>• ISO 8601 (e.g., 2017-11-08T16:52:42Z)<br>• Loose Date format (e.g., 2017 12 25)<br>• Unix Time/Posix Time/Epoch Time (e.g., 1510686617 or 1510686617.298753) |
| Download Reports | This parameter enables Reports to be downloaded from CrowdStrike when the job runs. |

| | |
|---|---|
| Report Metrics | This parameter enables Report metrics to be downloaded from CrowdStrike when the job runs. |
| Proxy TC API Connection | This parameter enables proxy for connecting to the ThreatConnect API. |
| Proxy External API Connection | This parameter enables proxy for connecting to the CrowdStrike API. |
| Advanced Settings | This parameter allows for the input of advanced settings. See the “Advanced Settings” section for more information. |
| Logging Level | This parameter is the logging level (recommended value: **info**). |

# DATA MAPPING

The data mappings in Table 2, Table 3, and Table 4 illustrate how data are mapped from CrowdStrike API endpoints into the ThreatConnect data model.

## Reports

**Table 2**

| CrowdStrike API Field | ThreatConnect Field |
|---|---|
| short_description | Attribute: “Description” |
| last_modified_date | Attribute: “External Date Last Modified” |
| created_date | Date Published<br>Date Added |
| target_industries | Attribute: “Target Industry” |
| target_countries | Attribute: “Target Country” |
| type | Tags |
| url | Attribute: “Source” |
| tags | Tags |
| sub_type | Tags |
| name | Report Name |
| Actors | Association: Adversary Group |

## Actors

**Table 3**

| CrowdStrike API Field | ThreatConnect Field |
|---|---|
| name | Adversary |
| url | Attribute: “Source” |
| description | Attribute: “Description” |
| created_date | Date Added |
| last_modified_date | Attribute: “External Date Last Modified” |
| first_activity_date | Attribute: “First Seen” |
| last_activity_date | Attribute: "Last Seen" |
| active | Attribute: “Active” |
| known_as | Attribute: “Aliases” |
| kill_chain | Attribute: “Phase of Intrusion” |
| target_industries | Attribute: “Target Industry” |
| capabilities | Attribute: “Threat Level” |
| group | Tags |
| region | Tags |

| | |
|---|---|
| origins | Attribute: “Origin Country” |
| target_countries | Attribute: “Target Country” |

# Indicators

**Table 4**

| CrowdStrike API Field | ThreatConnect Field |
|---|---|
| malicious_confidence | See the Threat Rating and Confidence Rating mappings in Table 5 |
| actor | Association: Adversary Group |
| report | Association: Report Group |
| kill_chains | Attribute: “Phase of Intrusion” |
| labels | Attribute: “Additional Analysis & Context” |
| labels = ATT&CK | MITRE ATT&CK™ Tags (See *MITRE ATT&CK* for more information.) |
| domain_types | Tags |
| ip_address_types | Tags |
| created_date | Date Added |
| last_modified_date | Last Modified |

Table 5

| malicious_confidence | Threat Rating and Confidence Rating |
|---|---|
| Unverified | 0 skulls and 0 Confidence Rating |
| Low | 2 skulls and 50 Confidence Rating |
| Medium | 3 skulls and 75 Confidence Rating |
| High | 5 skulls and 100 Confidence Rating |

## TROUBLESHOOTING

The CrowdStrike Falcon Intelligence integration 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.

# 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 value in Table 6 is available for configuration in Advanced Settings.

**Table 6**

| Key | Value |
|---|---|
| playbook_trigger_enabled | Boolean – denotes whether this job app's executions will be able to trigger new Playbook executions. |