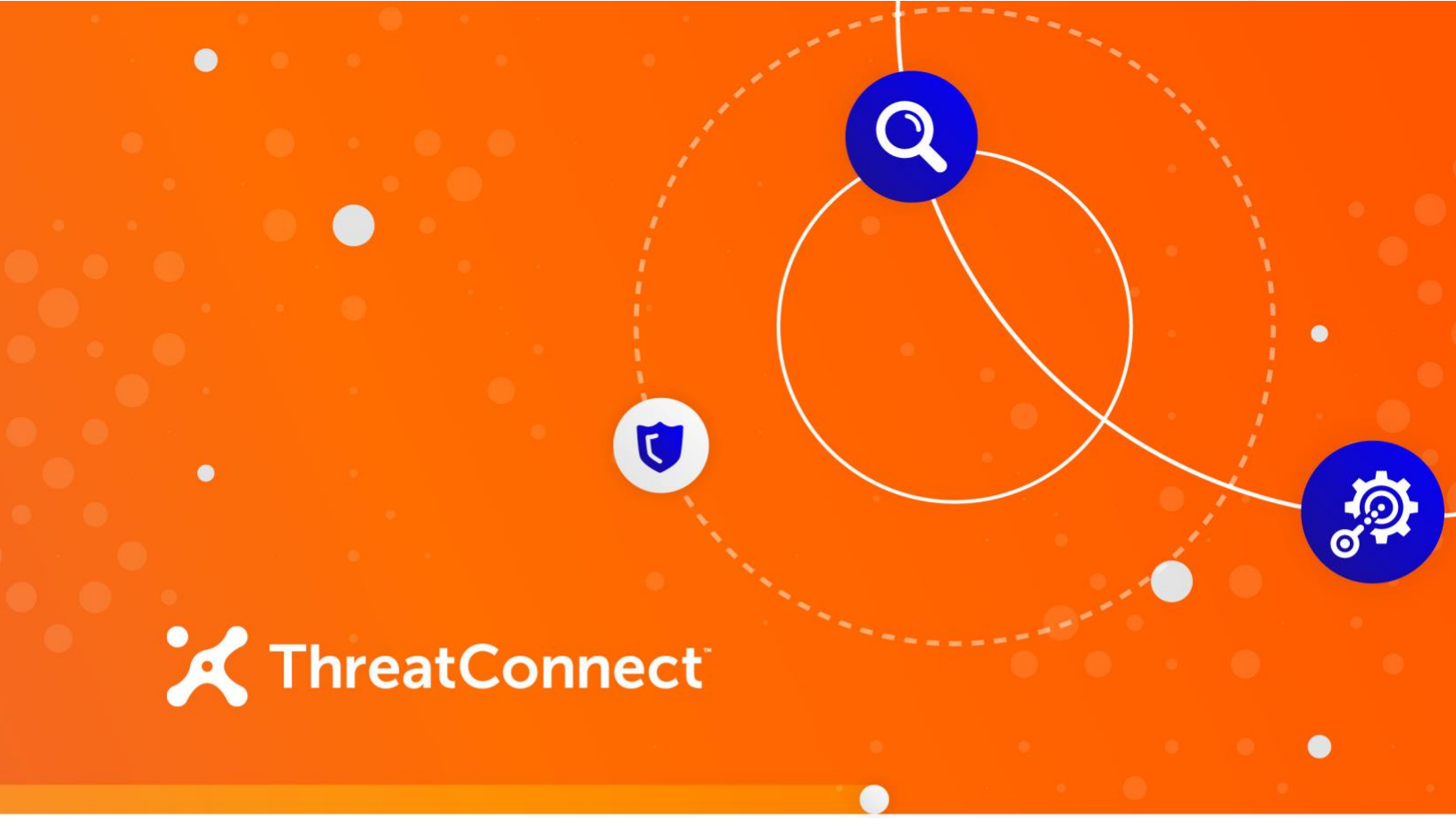

CrowdStrike Falcon® Insight Extract Integration

Configuration Guide

Software Version 2.0.0

December 21, 2021

30025-03 EN Rev. B

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® app for CrowdStrike Falcon Insight enables ThreatConnect users to automatically deploy Address, Host, and File Indicators to CrowdStrike Falcon Insight for alerting and monitoring. The integration can remove any Indicators that were previously deployed when they no longer match the configured filters.

DEPENDENCIES

ThreatConnect Dependencies

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.***

- Active ThreatConnect Application Programming Interface (API) key

Falcon Host Dependencies

- Active Falcon Insight API key

  NOTE: See the following link for information on how to manage CrowdStrike API keys: https://falcon.crowdstrike.com/documentation/46/crowdstrike-oauth2-based-apis#api-clients***. Note that you will need a CrowdStrike username and password to access this documentation.***

CONFIGURATION PARAMETERS

Parameter Definition

The parameters defined in Table 1 apply to the configuration parameters during the job-creation process.

Table 1

Name	Description	Required?
Api User	The ThreatConnect API user account.	Yes
CrowdStrike Client ID	The CrowdStrike Falcon Insight Client ID.	Yes
CrowdStrike Client Secret	The CrowdStrike Falcon Insight Client Secret.	Yes
CrowdStrike API Endpoint	The CrowdStrike environment. The default value is **US-1 (api.crowdstrike.com).**	Yes
ThreatConnect Source Owner	The owners in ThreatConnect on which to filter.	Yes
Tag Filter	The inclusive filter for Indicator Tags. Only Indicators with the Tags provided in this parameter will be deployed.	No
Indicator Type	The Indicator types to deploy to CrowdStrike Falcon Insight.	Yes
Minimum Indicator Threat Rating	The Threat Rating to apply to all Indicators. Enter a whole number between 0 and 5, inclusive. The default value is **1**.	No

Minimum Indicator Threat Confidence	The Confidence Rating to apply to all Indicators. Enter a whole number between 0 and 100, inclusive. The default value is **25**.	No
Minimum Threat Assess Score	The minimum ThreatAssess score of an Indicator to filter on. If this parameter is provided, values entered for the **Minimum Indicator Threat Rating** and **Minimum Indicator Threat Confidence** will be ignored.	No
Action	The action to take when a CrowdStrike host observes the Indicator. The default value is **No Action**.	Yes
Platforms	The platform to which the Indicator applies. Multiple selections can be made. Possible values are **Linux**, **Windows**, and **Mac**.	Yes
Description	The description for the Indicators sent to CrowdStrike Falcon Insight.	No
Expiration Days	The number of days until the Indicator will no longer be used. The default value is **2**.	No
Indicator Tags	The Tags for the deployed Indicators inside CrowdStrike Falcon Insight.	No
Host Group IDs	The list of host group IDs to which the Indicator applies (separated by commas).	No
Apply Globally	Determines whether to apply the Indicator globally. The default value is **Selected**.	No
Retrodetects	Determines whether to submit retrodetects. The default value is **Unselected**.	No

Ignore Warnings	Determines whether to ignore warnings and add all Indicators. The default value is **Selected**.	No
Logging Level	The logging level for the app. Possible values are **debug**, **info**, **warning**, **error**, and **critical**. The default value is **info**.	Yes