



Secureworks® Attacker Database Integration

Configuration Guide

Software Version 1.0

November 4, 2020

30020-03 EN Rev. A



©2020 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.
Secureworks® is a registered trademark of Secureworks, Inc.





Table of Contents

OVERVIEW.....	4
DEPENDENCIES.....	4
ThreatConnect Dependencies.....	4
Secureworks Dependencies	4
CONFIGURATION PARAMETERS	4
Parameter Definition.....	4





OVERVIEW

The ThreatConnect® integration with Secureworks Attacker Database allows IP and Domain Indicator watchlists from Secureworks to be ingested into 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.

Secureworks Dependencies

- Secureworks API key

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 ThreatConnect API user account.
Secureworks API Username	This parameter is the Secureworks API username.
Secureworks API Password	This parameter is the Secureworks API password.



Mark Removed Indicators Inactive	This checkbox determines whether Indicators removed by Secureworks get marked as inactive in ThreatConnect.
ThreatConnect Default Org Name	This parameter is the Owner in which to save Groups and Indicators.
Secureworks Watchlist Selection	This parameter determines the watchlist(s) to download.
The indicator to use	This parameter is the Indicator type of the watchlist.
Default Threat Rating	Unless specifically determined by the feed, this parameter will set the default Threat Rating for each Indicator found by the parsing the feed.
Default Confidence Rating	Unless specifically determined by the feed, this parameter will set the default Confidence Rating for each Indicator found by the parsing the feed.
Additional tags to add to groups and indicators (delimited by ' ')	This parameter specifies additional Tags to add to Groups and Indicators (delimited by ' ').
Logging level	This parameter is the logging level for the job when the app is run. Possible values are as follows: • FATAL • ERROR • WARN • INFO • DEBUG • TRACE