ThreatConnect™

Booz Allen Hamilton® Cyber4Sight® ThreatBase™ Integration

Configuration Guide

Software Version 1.0

August 13, 2019

30019-03 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
Booz Allen Hamilton Cyber4Sight ThreatBase Dependencies 4

CONFIGURATION PARAMETERS 5

Parameter Definition 5

DATA MAPPING 7

Reports 7
Indicators 8

OVERVIEW

The ThreatConnect® integration with Booz Allen Hamilton Cyber4Sight ThreatBase allows users to ingest and operationalize the ThreatBase feed in ThreatConnect. The integration downloads reports and Indicators, along with all the context available in the API, and associates them together inside 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.

Booz Allen Hamilton Cyber4Sight ThreatBase Dependencies

- Active subscription for Cyber4Sight ThreatBase

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_access_id	This parameter is the ThreatConnect API Access ID.
api_secret_key	This parameter is the ThreatConnect API Secret Key.
api_default_org	This parameter is the source Owner to save Groups and Indicators.
c4s_api_secret_key	This parameter is the API key needed to access the Cyber4Sight data.
days_back	This parameter is the number of days back to retrieve data. It is set to -1 to pull all data.
low_confidence	This parameter is the Confidence Rating to use whenever an Indicator is found to have a “low” Confidence Rating. The default value is 20.
med_confidence	This parameter is the Confidence Rating to use whenever an Indicator is found to have a “med” Confidence Rating. The default value is 50.
high_confidence	This parameter is the Confidence Rating to use whenever an Indicator is found to have a “high” Confidence Rating. The default value is 80.

default_rating	Unless the Threat Rating is specifically determined by the feed, this parameter will set the default Threat Rating for each Indicator found by the parsing the feed.
default_confidence	Unless the Confidence Rating is specifically determined by the feed, this parameter will set the default Confidence Rating for each Indicator found by the parsing the feed.
tags	This parameter specifies additional Tags to add to Groups and Indicators (delimited by '|').
log_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

DATA MAPPING

The data mappings in Table 2 and Table 3 illustrate how data are mapped from ThreatBase API endpoints into ThreatConnect's data model.

Reports

Table 2

ThreatBase API Field	ThreatConnect Field
ThreatbaseID	Attribute: "ThreatBase ID"
Title	Document Name
Type	Attribute: "Report Type"
publicationDate	Attribute: "Published Date"
excerpt	Attribute: "Description"
analysis	HTML File Attachment
sources	Attribute: "Source"
mentions	Association: Indicators

Indicators

Table 3

ThreatBase API Field	ThreatConnect Field
ThreatbaseID	Attribute: “ThreatBase ID”
Title	Indicator
Type	Indicator Type
Description	Attribute: “Tactics, Techniques, and Procedures”
RelatedTTPs	Tags
LastMentionedDate	Attribute: “Date Last Mentioned”
UpdatedDate	Attribute: “Date Last Modified”
CreatedDate	Attribute: “Date Created”
Confidence	Confidence
State	Tag: “State: %state%”