BAE Systems® Threat Intelligence Integration Configuration Guide

Software Version 2.0

Integration Guide

January 3, 2023

30060-05 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 BAE Systems Threat Intelligence enables ThreatConnect customers to import Events and Attributes from the BAE MISP instance into ThreatConnect as Event Groups and Indicators (Address, Host, Email Address, URL, CIDR, File, ASN, and User Agent), respectively. In addition, the App ingests MISP Galaxy types of Threat Actors and Attack Patterns. Threat Actors are ingested as Adversary Groups and associated to Events in ThreatConnect. Attack Patterns are created as MITRE ATT&CK® Tags on Events. See *MITRE ATT&CK Information in ThreatConnect* for more information on how MITRE ATT&CK classifications are represented 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 during configuration on the **Account Settings** screen within their ThreatConnect instance.

BAE Threat Intelligence Dependencies

- Active BAE Threat Intelligence 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	Required?
Api User	The name of the ThreatConnect API user.	Yes
MISP Server URL	The URL of BAE's MISP instance. The default value is **https://sig02.threatreveal.com/**. **Important**: Do not modify the default value.	Yes
MISP API Key	The MISP API key.	Yes
ThreatConnect Source Owner	The ThreatConnect owner into which data will be imported.	Yes
MISP Organization	The MISP Organization. The default value is **BAE Systems**. **Important**: Do not modify the default value.	Yes
Add Custom Tags to Events (delimited by "|")	A set of custom Tags, separated by the pipe character (|), to be added to the Event Groups created in ThreatConnect.	No
MISP Attributes Used to Create Indicators/Groups	The MISP Attributes that will be captured as Indicators and Groups in ThreatConnect.	Yes
Return Deleted Attributes	Select this checkbox to include deleted MISP Attributes, in addition to existing ones, in the import.	No
Return Metadata Only	Select this checkbox to include only MISP Event metadata (e.g., Event	No

	data, tags, relations) in the import. If this checkbox is selected, Attributes will not be included in the import.	
Return Only "For Intrusion Detection System" Attributes Flag Set	Select this checkbox to include only MISP Attributes with the “for Intrusion Detection System” flag set to **true** in the import.	No
Return Events with Attachments	Select this checkbox to include MISP Events with attachments in the import.	No
Last Run	The date value by which to filter MISP Events. This start date value and the Event Date Type are used together to return the desired MISP Events (e.g., Last Modified Date and Historical Data Start Date of "30 days ago").	Yes
Logging Level	Determines the verbosity of the logging output for the application.	Yes
Advanced Settings	Use this parameter for additional advanced settings, as detailed in the “Advanced Settings” section. **Important**: Consult with your Customer Success Engineer before making changes to the App’s advanced settings.	No

Data Mapping

The data mappings in Tables 2–5 illustrate how data are mapped from the BAE MISP API endpoints into the ThreatConnect data model.

Events

Table 2

MISP API Field	ThreatConnect Field
Event.id	Event: Attribute: "External ID"
Event.timestamp	Event: "Event Date"
Event.publish_timestamp	Event: Attribute: "Source Date Time"
Event.Tag	Event: Tags
Event."Threat Level"	Event: Attribute: "Threat Level"
response[*].Event.Attribute[*].type == "comment"	Event: Attribute: "Description"
response[*].info	Event: Title

Attributes

Table 3

MISP API Field	ThreatConnect Field
response[*].Event.Attribute[*].type == "md5"	File: MD5
response[*].Event.Attribute[*].type == "sha1"	File: SHA1
response[*].Event.Attribute[*].type == "sha256"	File: SHA256
response[*].Event.Attribute[*].type == "filenamelmd5"	File: File Occurrences: File Name File: MD5
response[*].Event.Attribute[*].type == "filenamelsha1"	File: File Occurrences: File Name File: SHA1
response[*].Event.Attribute[*].type == "filenamelsha256"	File: File Occurrences: File Name File: SHA256
response[*].Event.Attribute[*].type == "ip-src"	Address
response[*].Event.Attribute[*].type == "ip-dst"	Address
response[*].Event.Attribute[*].type == "domain"	Host
response[*].Event.Attribute[*].type == "email-src"	Email Address
response[*].Event.Attribute[*].type == "url"	URL

response[*].Event.Attribute[*].type == "domainlip"	Host Address
response[*].Event.Attribute[*].category == "Attribution"	Attribute: "Additional Analysis and Context"
Event.Attribute[*].type == "yara"	Signature: Yara
Event.Attribute[*].type == "snort"	Signature: Snort
BAE Attribute Comment JSON : date	Indicator: Date Added
BAE Attribute Comment JSON : priority	Indicator: Threat Rating
BAE Attribute Comment JSON : confidence	Indicator: Confidence
BAE Attribute Comment JSON : condition	Indicator: Tag
BAE Attribute Comment JSON : expiryDate	Attribute: "External Date Expires"
Event.timestamp	Indicator: Last Modified

Galaxy: Threat Actor

Table 4

MISP API Field	ThreatConnect Field
name	Adversary: Name Attribute: "Adversary Type" = Group
description	Attribute: "Description"
uuid	Attribute: "External ID"
meta.cfr-suspected-victims	Attribute: "Target Country"
meta.cfr-target-category	Attribute: "Target Industry"
meta.country	Attribute: "Adversary Origin & Source"
meta.refs	Attribute: "Source"
meta.synonyms	Attribute: "Aliases"
meta.motive	Attribute: "Adversary Motivation Type"

Galaxy: Attack Pattern

Table 5

MISP API Field	ThreatConnect Field
name	Event: Tag (MITRE ATT&CK)

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. Before editing these settings, consult with your Customer Success Engineer.

The parameter in Table 6 is available for configuration in the App's advanced settings.

Table 6

Key	Value
playbook_trigger_enabled	This parameter accepts a Boolean value that denotes whether executions of the App will be able to trigger new Playbook executions.