ThreatConnect™

# BAE Systems® Threat Intelligence Integration

## Configuration Guide

**Software Version 1.0**

**August 20, 2019**

30060-02 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 BAE Systems Threat Intelligence enables ThreatConnect customers to import Events and Attributes from the BAE MISP instance into ThreatConnect as Incidents 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 Adversaries and associated to Incidents in ThreatConnect. Attack Patterns are created as MITRE ATT&CK™ Tags on Incidents. See the ThreatConnect Knowledge Base article "MITRE ATT&CK" 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. Private Instance customers can enable these settings during configuration on the Account Settings screen within their Private Instance of ThreatConnect.***

## 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 |
| --- | --- |
| BAE Threat Intelligence API Key | This parameter is the BAE Threat Intelligence API key. |
| Verify Certificate | This parameter enables certificate verification when connecting to the BAE MISP server. |
| ThreatConnect Source Owner | This parameter is the ThreatConnect Source into which data will be imported. |
| Last Run (YYYY-MM-DD) or '30 days ago' | This parameter defines how far back to import events on the first run of the job. Subsequent job runs will pull events published since the last run time. |
| Return events with attachments | This parameter is a filter for limiting the import to events with attachments. |
| Return only metadata | This parameter restricts the import to events only and will skip the Attributes. |
| Return only published events | This parameter restricts the import to events that have been published. |
| Return only attributes with IDS flag set | This parameter restricts the import to Attributes that have the IDS flag set to true. |
| Return deleted attributes | This parameter enables the import to get deleted Attributes. |
| Add custom tags to events | This parameter defines the Tags that will be added to the Incidents created in ThreatConnect. |

| | |
|---|---|
| MISP Attributes Used to Create Indicators | This parameter is a multi-select list of Indicator types to be imported from BAE Threat Intelligence. |
| Logging level | This parameter is the logging level for the app. |

# 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 | Attribute: “External ID” |
| Event.timestamp | Incident: “Event Date” |
| Event.publish_timestamp | Attribute: “Source Date Time”” |
| Event.Tag | Tags |
| Event."Threat Level" | Attribute: “Threat Level” |
| response[*].Event.Attribute[*].type == "comment" | Attribute: “Description” |
| response[*].Event.Attribute[*].type == "text" | Incident: Title |

## Attributes

Table 3

| MISP API Field | ThreatConnect Field |
|---|---|
| Event.Attribute[*].type == "md5" | File: md5 |
| Event.Attribute[*].type == "sha1" | File: sha1 |
| response[*].Event.Attribute[*].type == "sha256" | File: sha256 |
| response[*].Event.Attribute[*].type == "filename\|md5" | File: File Occurrences: File Name<br>File: md5 |
| response[*].Event.Attribute[*].type == "filename\|sha1" | File: File Occurrences: File Name<br>File: sha1 |
| response[*].Event.Attribute[*].type == "filename\|sha256" | File: File Occurrences: File Name<br>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 == "domain\|ip" | Host<br><br>Address |
| 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<br>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 | Incident: Tag (MITRE ATT&CK) |