MISP Import Integration

Configuration Guide

Software Version 2.0

June 1, 2021

30054-05 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
MISP Dependencies 4

CONFIGURATION PARAMETERS 4

Parameter Definition 4

DATA MAPPING 6

Events 6
Attributes 7

ADVANCED SETTINGS 8

OVERVIEW

The ThreatConnect® integration with the Malware Information Sharing Platform (MISP) enables ThreatConnect customers to import MISP Events and Attributes into ThreatConnect as Incidents and Indicators [Address, Host, Email Address, Email Subject, URL, CIDR, File, ASN, and User Agent], respectively.

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.

MISP Dependencies

- Active MISP instance with 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 name of the API user account running the app.

MISP Server URL	This parameter is the base URL to the MISP instance (e.g., https://misp.company.com).
Verify SSL Cert	This parameter enables certification verification when connecting to the MISP server.
MISP API Key	This parameter is the MISP API key with access to the v3 API.
Threat Rating	This parameter sets the default Threat Rating to be applied to all created Indicators in ThreatConnect.
Confidence Rating	This parameter sets the default Confidence Rating to be applied to all created Indicators in ThreatConnect.
ThreatConnect Source Owner	This parameter is the ThreatConnect Source into which data will be imported.
MISP Organization	This parameter is a filter for limiting the import to the Organization that reported the Event in MISP.
Add Custom Tags to Events (delimited by "I")	This parameter defines the Tags that will be added to the Incidents created in ThreatConnect.
MISP Attribute Types Used to Create Indicators	This parameter is a dropdown list of MISP attribute types to be created as Indicators in ThreatConnect.
Return Deleted Attributes	This parameter enables the import to get deleted attributes.
Return Metadata Only	This parameter restricts the import to Events only and will skip the Attributes.
Return Only "For Intrusion Detection System" Attributes flag set	This parameter restricts the import to attributes that have the Intrusion Detection System (IDS) flag set to **true**.

Last Run	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.
Logging Level	This parameter is the logging level for the app.
Advanced Settings	This parameter allows for input of advanced settings. See the “Advanced Settings” section.

DATA MAPPING

The data mappings in Table 2 and Table 3 illustrate how data are mapped from MISP API endpoints into the ThreatConnect data model.

Events

Table 2

MISP API Field	ThreatConnect Field
Event.id	Attribute: “External ID”
Event.info	Attribute: “Description”
Event.timestamp	Incident: “Event Date”
Event.publish_timestamp	Attribute: “Source Date Time””
Event.Tag	Tags
Event."Threat Level"	Attribute: “Threat Level”

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 File: md5
response[*].Event.Attribute[*].type == "filename|sha1"	File: File Occurrences: File Name File: sha1
response[*].Event.Attribute[*].type == "filename|sha256"	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 == "domain|ip"	Host Address
response[*].Event.Attribute[*].type == "AS"	ASN or CIDR
response[*].Event.Attribute[*].type == "user-agent"	User Agent
response[*].Event.Attribute[*].type == "email-subject"	Email Subject (custom Indicator)

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. Please consult your Customer Success Engineer before editing these settings.

The values in Table 4 are available for configuration in **Advanced Settings**.

Table 4

Key	Value
playbook_trigger_enabled	Boolean – denotes whether this job app's executions will be able to trigger new Playbook executions.
unpublished	Boolean – denotes whether unpublished MISP Events should be retrieved.
use_last_modified_date	Boolean – denotes whether MISP Events should be retrieved using Last Modified date or Publish Date