Tanium™ Threat Response – Indicators Integration Configuration Guide

Software Version 4.0

Integration Guide

March 30, 2023

30065-02 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 Tanium Threat Response – Indicators enables ThreatConnect customers to send Address, File, and Host Indicators from ThreatConnect to their Tanium Threat Response instance as Intel Packages based on specified criteria. This functionality allows users to operationalize intelligence from ThreatConnect in the form of searching and monitoring for malicious Indicators in their endpoint environment.

Dependencies

ThreatConnect

- 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 on the **Account Settings** screen within their ThreatConnect instance.

Tanium Threat Response Dependencies

- Active Tanium Threat Response API key

Application Setup and Configuration

Organization Administrators should set up and configure the **Tanium Threat Response – Indicators** App. See the "Creating a Job" sub-section of the "Apps and Jobs" section of *ThreatConnect Organization Administration Guide* for instructions on how to set up and configure a Job App. It is highly recommended to review the App configuration prior to running or activating the corresponding Job.

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters during the Job-creation process.

Table 1

Name	Description	Required?
Api User	The username of the ThreatConnect API account.	Yes
Tanium Address	The address of the Tanium Threat Response instance.	Yes
Tanium Username	The username for the Tanium Threat Response instance.	Yes
Tanium Password	The password for the Tanium Threat Response instance.	Yes
Verify SSL Cert	Select this checkbox to enable SSL verification for the connection between ThreatConnect and Tanium Threat Response.	No
Tanium Threat Response Source	The name of the source in Tanium Threat Response that will be created or used for adding Indicators. The default value is **ThreatConnect**.	Yes
ThreatConnect Owners	The ThreatConnect owner(s) whose Indicators will be sent to Tanium Threat Response.	No
Indicator Types	The type(s) of Indicators that will be sent to Tanium Threat Response. Accepted values include the following: • Address • File	No

	• Host	
Last Modified	The last time the App ran. Data modified since this date will be included on the first run. Thereafter, the date will be updated automatically each time the Job completes successfully. The default value is **30 days ago**. **Warning**: Do not edit this parameter.	Yes
TQL	A custom ThreatConnect Query Language (TQL) query for filtering Indicators. When used, all other filter-based parameters (**Indicator Types**, **ThreatConnect Owners**, **Include Tags**, **Exclude Tags**, **Maximum False Positive Count**, **Minimum Confidence Rating**, **Minimum ThreatAssess Score**, and **Minimum Threat Rating**) will be ignored.	No
Include Tags	The Tag(s) that Indicators must include in order to be sent to Tanium Threat Response. Indicators must include **at least one** of the specified Tags in order to be sent.	No
Exclude Tags	The Tag(s) that Indicators must exclude in order to be sent to Tanium Threat Response. Indicators that include **any** of the specified Tags will not be sent.	No
Minimum ThreatAssess Score	The minimum ThreatAssess score that Indicators must have in order to be sent to Tanium Threat Response.	No
Minimum Confidence Rating	The minimum Confidence Rating that Indicators must have in order to be sent to Tanium Threat Response.	No

Minimum Threat Rating	The minimum Threat Rating that Indicators must have in order to be sent to Tanium Threat Response.	No
Maximum False Positive Count	The maximum number of false positives that Indicators can have in order to be sent to Tanium Threat Response. When used, only Indicators with a false positive count less than or equal to the specified value will be sent.	No
Logging Level	Determines the verbosity of the logging output for the application.	Yes