Tanium™ Threat Response – Signatures Integration Configuration Guide

Software Version 4.0

Integration Guide

March 30, 2023

30066-02 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

©2023 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.
Tanium™ is a trademark of Tanium, Inc.

Table of Contents

Overview

The ThreatConnect® integration with Tanium Threat Response – Signatures enables ThreatConnect customers to send Signature Groups 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 Signature-based searching and monitoring for malicious activity 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 – Signatures** 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 User Name	The username for the Tanium Threat Response instance.	Yes
Tanium Password	The password for the Tanium Threat Response instance.	Yes
Verify SSL for Tanium Connection	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 Signatures. The default value is **ThreatConnect**.	Yes
Last Run	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 Signature Groups. When used, all other filter-based parameters (**Signature Types**, **ThreatConnect Owners**, and **Include Tags**) will be ignored.	No
Signature Types	The type(s) of Signatures that will be sent to Tanium Threat Response. Accepted values include the following: • YARA • OpenIOC	No
ThreatConnect Owners	The ThreatConnect owner(s) whose Signature Groups will be sent to Tanium Threat Response.	No
Include Tags	The Tag(s) that Signature Groups must have in order to be sent to Tanium Threat Response. Signature Groups must include **at least one** of the specified Tags in order to be sent	No
Logging Level	Determines the verbosity of the logging output for the application.	Yes