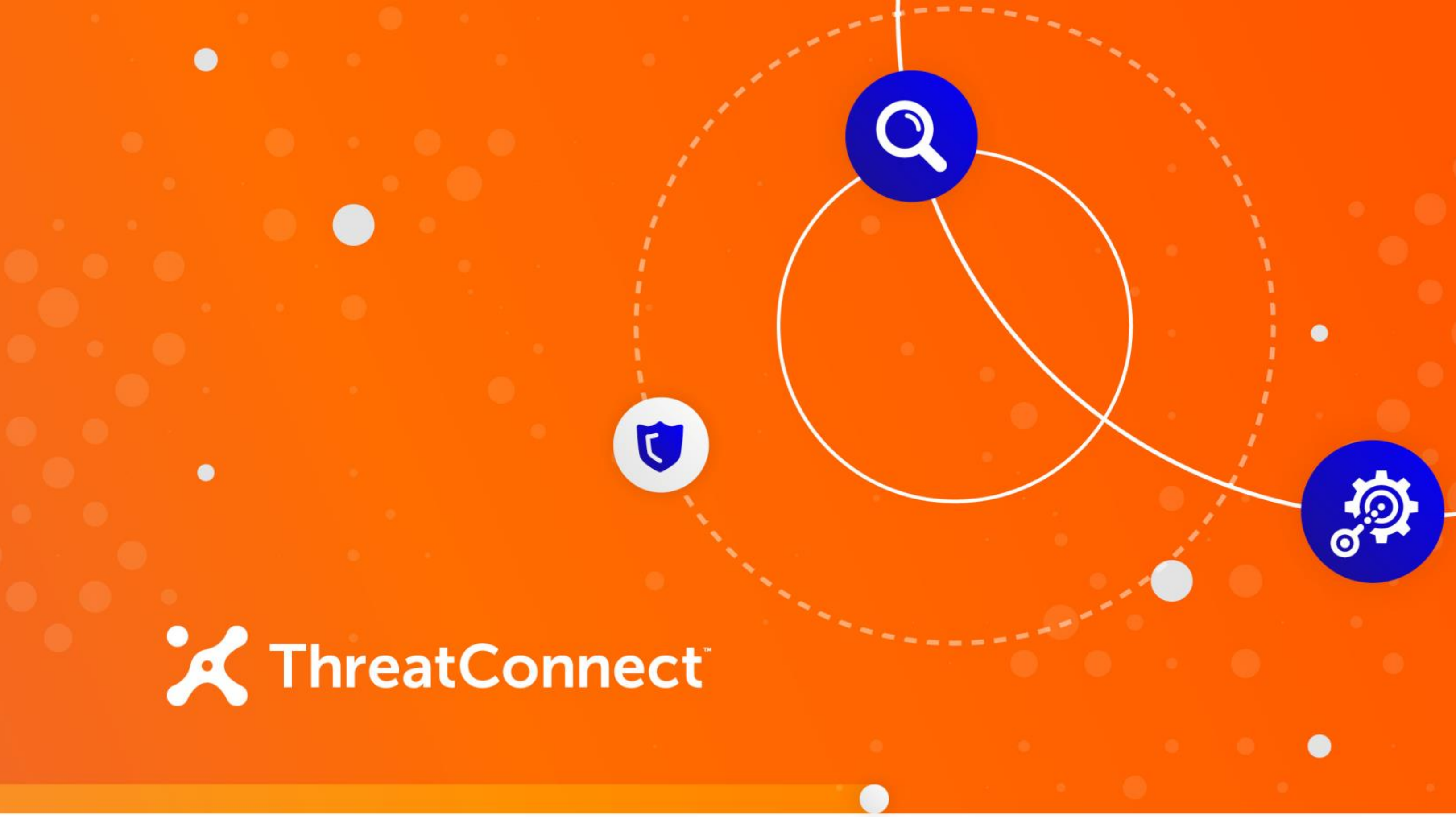

Tenable.sc™ Integration

Configuration Guide

Software Version 2.0

January 5, 2022

30050-03 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 Tenable.sc integration with ThreatConnect® helps organizations determine where threats and vulnerabilities cross paths and understand where they are most at risk. It does this by comparing Common Vulnerabilities and Exposures (CVE) data from sources in ThreatConnect with Nessus® scan results in Tenable.sc. Any matching unpatched vulnerabilities found within Tenable.sc are tagged accordingly in ThreatConnect, with the option to store scan result details as an Attribute. In addition, Workflow Cases and Tasks can be created to notify users about the matching vulnerabilities and the need for further action.

The integration works by querying Tenable® for scan results over a given period of time (typically 30 days upon first run, and then from the previous run until the current run for subsequent runs) and downloading those data. The data are parsed for CVE tags, which are matched against CVE data within ThreatConnect Indicators and Groups of the type(s) selected in the configuration. Any found Indicators or Groups are then updated with the data for that CVE from Tenable, and, if desired, a Tag is applied to indicate that matching Tenable CVE data were found for that object.

DEPENDENCIES

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) keys for source and target servers

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.***

Tenable Dependencies

- Tenable.sc environment containing Nessus scan results

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 created via the ThreatConnect web user interface. It will be shown only when running older versions of ThreatConnect that lack built-in token security.	Yes
Tenable.sc base URL	The base URL for the location at which Tenable is installed. It should include "http" or "https" (e.g., `https://sc.tenalab.online/`).	Yes
Tenable Access Key	The Tenable Access Key used to log into Tenable.sc. It needs to have access to the scan results.	Yes
Tenable Secret Key	The password associated with the Tenable Access Keys.	Yes
Verify SSL Cert	Clearing this checkbox will override SSL verification for connecting to non-public instances. It is recommended to keep this checkbox selected.	No
Owners	The owner(s) whose data will be compared with the scan results. At least one owner must be selected.	Yes
Item to Create when Match Found	The selected item—Task or Workflow Case—will be created when a matched unpatched vulnerability is found.	Yes
Group Types to Search for CVE Tags	The Group type(s) to be included when comparing with Tenable scan results.	No

Indicator Types to Search for CVE Tags	The Indicator type(s) to be included when comparing with Tenable scan results.	No
Tag(s) to Apply to Groups, Indicators and Workflow Case or Task (delimited by ‘|’)	Tag(s) to be applied to matched Indicators and Groups. Note that the Tags will be applied only to Indicators and Groups in the selected Owner(s).	No
Assignee	The ThreatConnect username, typically an email address, of the assignee of the Workflow Task or Cas that is created.	No
Workflow Case or Task Name Prefix	A value to add to the Scan ID when naming the new Workflow Case or Task.	No
Store Scan Result Details	When this checkbox is selected, the details of the scan result will be stored as a File Artifact attached to the Workflow Case or as a Document Group attached to the Task.	No
Last Run	Only data modified since the entered date will be imported into ThreatConnect. The value of this parameter will be automatically updated each time the job successfully completes.	Yes
Logging Level	Determines the verbosity of the logging output for the application.	Yes
Advanced Settings	This parameter is for advanced settings, such as setting the next run date and time. It is not to be used except as directed by ThreatConnect Support.	No

VIEWING THE START TIME AND LOG INFORMATION

The value of the **Start Time** parameter can be viewed by looking at the Job parameters within ThreatConnect. Users with access to the ThreatConnect server can have each Job write results to a **message.tc** file. The following is an example of the contents of the file for this integration:

```
Success. Saving runtime: 1536678707
```

Users with access to view the log or have it emailed to them will be able to view the same value near the bottom of the log, such as in the following example:

```
INFO  11:12:17 com.threatconnect.app.tenable.steps.SaveRunData - Success.
Saving runtime: 1536678707
```

The **Start Time** parameter can be changed to catch up on missed data or altered for testing purposes by setting the value of the parameter in the Job in ThreatConnect.

When the logging level is set at **INFO** or higher, other lines will be available in the log that give insight into how the Job ran:

```
INFO  11:11:44 com.threatconnect.app.tenable.steps.DownloadScans - Number of
scans to process: 5

INFO  11:12:12 com.threatconnect.app.tenable.steps.QueryTCTags - Number of
CVEs matched: 1

INFO  11:12:12 com.threatconnect.app.tenable.steps.EnrichEntities -
Vulnerable tag to be added: Tenable Vulnerable
```