ThreatConnect™

Qualys® Vulnerability Management Integration

Configuration Guide

Software Version 2.0.0

December 21, 2021

30030-04 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 Qualys Vulnerability Management Integration with ThreatConnect® helps an organization see where threats and vulnerabilities cross paths and understand where the organization is most at risk. It does this by matching Common Vulnerabilities and Exposures (CVE®) data from sources in ThreatConnect against Qualys scan results. Any matching unpatched vulnerabilities found within Qualys are tagged accordingly in ThreatConnect, with the option to store scan result details as an Attribute. In addition, Tasks can be created to notify users of the matching vulnerabilities and the need for further action. Scan result details will be provided as an Attribute of the Task or a Document associated to the Task.

DEPENDENCIES

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) key

Qualys Dependencies

- Active Qualys Vulnerability Management username and password, with API access enabled

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 ThreatConnect API Access ID created via the ThreatConnect Web UI.	Yes
API base URL	The URL for API calls to Qualys.	Yes
Username	The Qualys account username.	Yes
Password	The Qualys account password.	Yes
Owners	The set of ThreatConnect owners to search for CVE-tagged entities.	Yes
Group Types to Search for CVE Tags	The Group types to check for CVE tags (any of Incident, Signature, Adversary, E-Mail, Threat, or Document).	No
Indicator Types to Search for CVE Tags	The Indicator types to check for CVE tags (any of File, URL, IP Address, Email Address, or Host).	No
Tag(s) to Apply to Groups, Indicators and Workflow Case or Task (delimited by '|')	The Tag(s) to apply to matched CVE-tagged entities. The default value is **Qualys Vulnerable**.	No

Item to Create when Match Found	The Qualys Case or Legacy Task to be created when a CVE match is found. The default value is **Workflow Case**.	Yes
Assignee	The user in ThreatConnect to whom the item created in Qualys will be assigned.	No
Workflow Case or Task Name Prefix	A value to add to the Scan ID when naming the new Workflow Case or Task.	No
Matched CVEs Only	If this checkbox is selected, items will be created only for CVEs matching data in ThreatConnect. If this checkbox is cleared, items will be created for all scan results.	No
Store Scan Result Details	Select this checkbox to store Qualys scan result details in the Task description.	No
Logging Level	The logging level for job output.	No
Last Run	The last time the job ran successfully. The default value is **7 days ago.**	No

ATTRIBUTE TYPES

The two Attributes detailed in Table 2 must be created at the Source or System level in order for the app to function properly. They are included in the **attribute.csv** file packaged with the app for easy import.

NOTE: Both Attributes are formatted with Markdown. To enable Markdown for each Attribute's respective Attribute Type, select the** Allow Markdown **checkbox on the** Configure Attribute Type **window, or upload the Attribute Types to ThreatConnect via a JSON file with the** allowMarkdown **field to** true**. See the "Attribute Types" section of** ThreatConnect Community and Source Administration Guide **or** ThreatConnect System Administration Guide **for more information on enabling Markdown for Attribute Types at the Source and System level, respectively.

Table 2

Name	Max Length	Description	Error Message	Mapping
Qualys Scan Results	600	This Attribute is the Qualys scan results.	Invalid Qualys Scan Results	File, Host, Url, Address, EmailAddress, Incident, Adversary, Document, Email, Signature, Threat, Victim
Associated Objects	5000	This Attribute details the associated objects in ThreatConnect that were matched against the Qualys vulnerability.	Invalid Object	Task