ThreatQuotient

Qualys Operation User Guide

Version 1.1.0

November 06, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 4.45.0
Support Tier	ThreatQ Supported

Introduction

The Qualys Operation for ThreatQ is used for searching Qualys for assets that are vulnerable for specific CVE IDs. Upon execution of the operation for a selected CVE ID in ThreatQ, it searches for hosts vulnerable for that CVE, and if it finds any, it would list the hosts IPs, the Qualys IDs associated with the vulnerability, the severities, and the dates of the execution of the scan.

> The operation provides you with the options to store the vulnerable hosts as Assets in ThreatQ as well as adding discovered assets to your ThreatQ instance. The Asset object type is required for these options. If you are running ThreatQ version 5.9 or earlier, see the steps for installing Asset custom object in the Prerequisites chapter.

The operation provides the following action:

- **Search for Vulnerable Assets** - finds any vulnerable hosts and ingests the results back into the ThreatQ.

The operation is compatible with the following indicator type:

- CVE

Prerequisites

Review the following prerequisites before attempting to install and run the operation.

Asset Custom Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

> ⚠ You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system object.

Use the steps provided to install the custom object.

> ⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   < > cd /tmp/
   ```
4. Create a new directory:

   ```
   < > mkdir qualys_op
   ```
5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the qualys_op directory.

   ```
   < > mkdir images
   ```
7. Upload the asset.svg
8. Navigate to the **/tmp/qualys_op**.

   The directory should resemble the following:

   - tmp
     - **qualys_op**
       - **asset.json**
       - **install.sh**
       - **images**
         - **asset.svg**
9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf qualys_op
```

Installation

The operation requires the installation of a custom object before installing the actual operation. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the operation. Attempting to install the operation without the custom object will cause the operation install process to fail.

Perform the following steps to install the integration:

The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration zip file.
3. Extract the zip file's contents and install the Asset custom object if you are on ThreatQ version 5.9 or earlier.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration .whl file using one of the following methods:
   - Drag and drop the .whl file into the dialog box
   - Select **Click to Browse** to locate the .whl file on your local machine

   ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

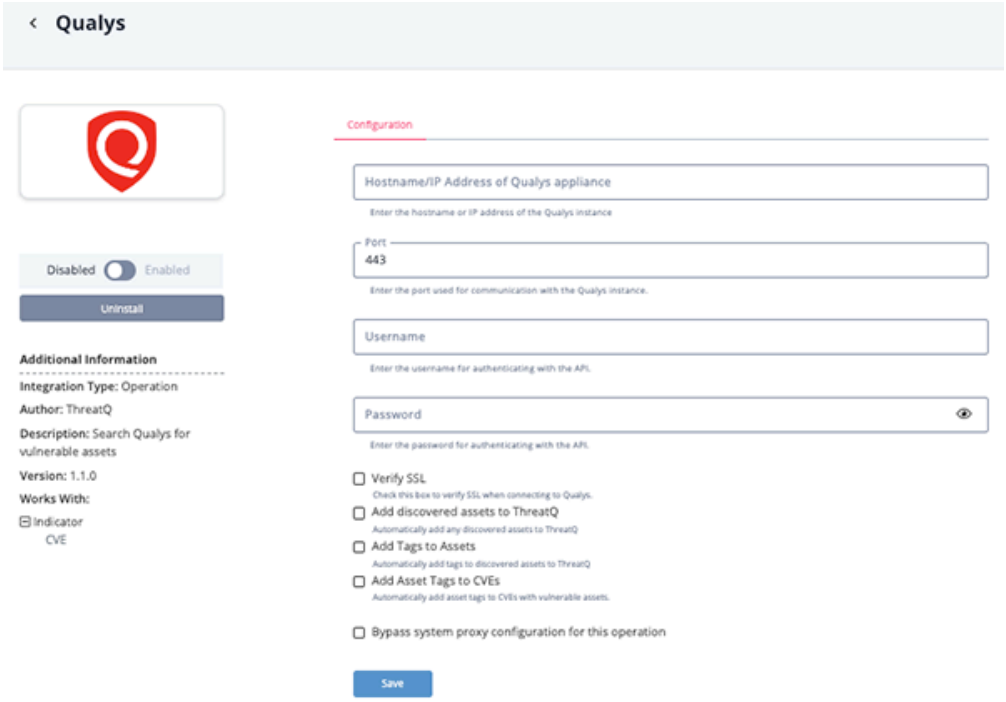
Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname	Your Hostname or IP address of Qualys.
Port	The communication port. The default setting is 443.
Username	Your Qualys username
Password	The password associated with the username above.
Verify SSL	Check this box to verify SSL when connecting to the Qualys instance.
Add Discovered Assets to ThreatQ	Automatically add any discovered assets to ThreatQ.
Add Assets to ThreatQ	Automatically add any discovered assets to ThreatQ.
Add Asset Tags to CVEs	Automatically add asset tags to CVEs with vulnerable assets.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Search for Vulnerable Hosts	Search for assets vulnerable for a specific CVE ID.	Indicator	CVE

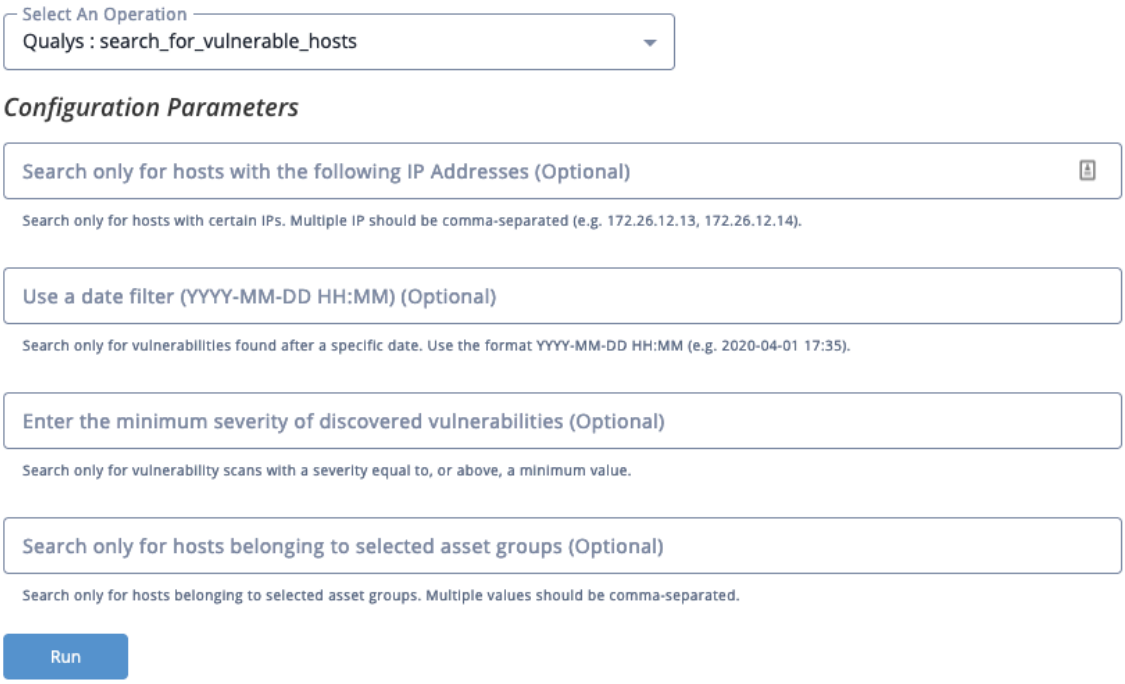
Search for Vulnerable Hosts

The Search for Vulnerable Hosts action creates a dynamic search list of assets in Qualys and returns all the assets vulnerable to the selected CVE. The Dynamic list will be deleted after the vulnerabilities have been extracted.

Configuration Options

The Search for Vulnerable Hosts action provides the following optional configuration filters:

PARAMETER	DESCRIPTION
Search Only for Hosts for specific IP Addresses	Search only for hosts with certain IPs. Multiple IP should be comma-separated (example: 172.26.12.13, 172.26.12.14).
Use Filter Date	Search only for vulnerabilities found after a specific date. The following format is accepted: **YYYY-MM-DD HH:MM** (example: 2020-04-01 17:35).
Minimum Severity	Search only for vulnerability scans with a severity equal to, or above, a minimum value.
Search Only for Hosts per Selected Asset Group	Search only for hosts belonging to selected asset groups. Multiple values should be comma-separated.


Select An Operation
Qualys : search_for_vulnerable_hosts
Configuration Parameters
Search only for hosts with the following IP Addresses (Optional)
Search only for hosts with certain IPs. Multiple IP should be comma-separated (e.g. 172.26.12.13, 172.26.12.14).
Use a date filter (YYYY-MM-DD HH:MM) (Optional)
Search only for vulnerabilities found after a specific date. Use the format YYYY-MM-DD HH:MM (e.g. 2020-04-01 17:35).
Enter the minimum severity of discovered vulnerabilities (Optional)
Search only for vulnerability scans with a severity equal to, or above, a minimum value.
Search only for hosts belonging to selected asset groups (Optional)
Search only for hosts belonging to selected asset groups. Multiple values should be comma-separated.
Run

Search

```
POST <configured_qualys_host>/api/2.0/fo/qid/search_list/dynamic/
```

API Body Parameters:

```
{
    "action": "create",
    "title": "ThreatQ Search",
    "cve_ids": "CVE-2019-17053",
    "global": 1
}
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://qualysapi.qg2.apps.qualys.com/api/2.0/
simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-03-27T13:56:05Z</DATETIME>
        <TEXT>New search list created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1704353</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Detection

```
GET <configured_qualys_host>/api/2.0/fo/asset/host/vm/detection/
```

API Request Parameters:

```
{
    "action": "list"
}
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
        "https://qualysapi.qg2.apps.qualys.com/api/2.0/fo/asset/host/vm/
detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-03-27T13:57:05Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>6506432</ID>
                <IP>10.10.10.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS><![CDATA[Windows 2008 R2 Enterprise Service Pack 1]]></OS>
                <DNS><![CDATA[2k8r2-u-10-11.sample.qualys.com]]></DNS>
                <DNS_DATA>
                    <HOSTNAME><![CDATA[2k8r2-u-10-11]]></HOSTNAME>
                    <DOMAIN><![CDATA[sample.qualys.com]]></DOMAIN>
                    <FQDN><![CDATA[2k8r2-u-10-11.sample.qualys.com]]></FQDN>
                </DNS_DATA>
                <NETBIOS><![CDATA[2K8R2-U-10-11]]></NETBIOS>
                <LAST_SCAN_DATETIME>2018-04-13T03:49:05Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2018-04-13T03:48:50Z</
LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>352</LAST_VM_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <QID>38170</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <PORT>3389</PORT>
                        <PROTOCOL>tcp</PROTOCOL>
                        <SSL>1</SSL>
                        <RESULTS>
                            <![CDATA[Certificate #0 CN=2k8r2-u-10-11(2k8r2-
u-10-11) doesn&apos;tresolve]]></RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2018-01-26T04:45:50Z</
FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2018-04-13T03:48:50Z</
```

```
LAST_FOUND_DATETIME>
                        <TIMES_FOUND>111</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2018-04-13T03:48:50Z</
LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2018-04-13T03:49:05Z</
LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2018-04-13T03:49:05Z</
LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
                <TAGS>
                    <TAG>
                        <TAG_ID>7588415</TAG_ID>
                        <NAME>windows</NAME>
                    </TAG>
                </TAGS>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.IP	Asset.Value	N/A	N/A	10.10.10.11	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.TAGS[].TAG.NAME	Asset.Tag	N/A	N/A	windows	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.LAST_SCAN_DATETIME	Asset.Attributes	Last Scan Date	N/A	2018-04-13T03:49:05Z	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.DETECTION_LIST[].DETECTION.QID	Asset.Attributes	Qualys ID	N/A	38170	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.DETECTION_LIST[].DETECTION.SEVERITY	Asset.Attributes	Severity	N/A	2	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.DETECTION_LIST[].DETECTION.STATUS	Asset.Attributes	Scan Status	N/A	Active	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.DETECTION_LIST[].DETECTION.TYPE	Asset.Attributes	Scan Type	N/A	Confirmed	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST[].HOST.DETECTION_LIST[].DETECTION.LAST_FOUND_DATETIME	Asset.Attributes	Last Found Date	N/A	2018-04-13T03:49:05Z	N/A

Delete

```
POST <configured_qualys_host>/api/2.0/fo/qid/search_list/dynamic/
```

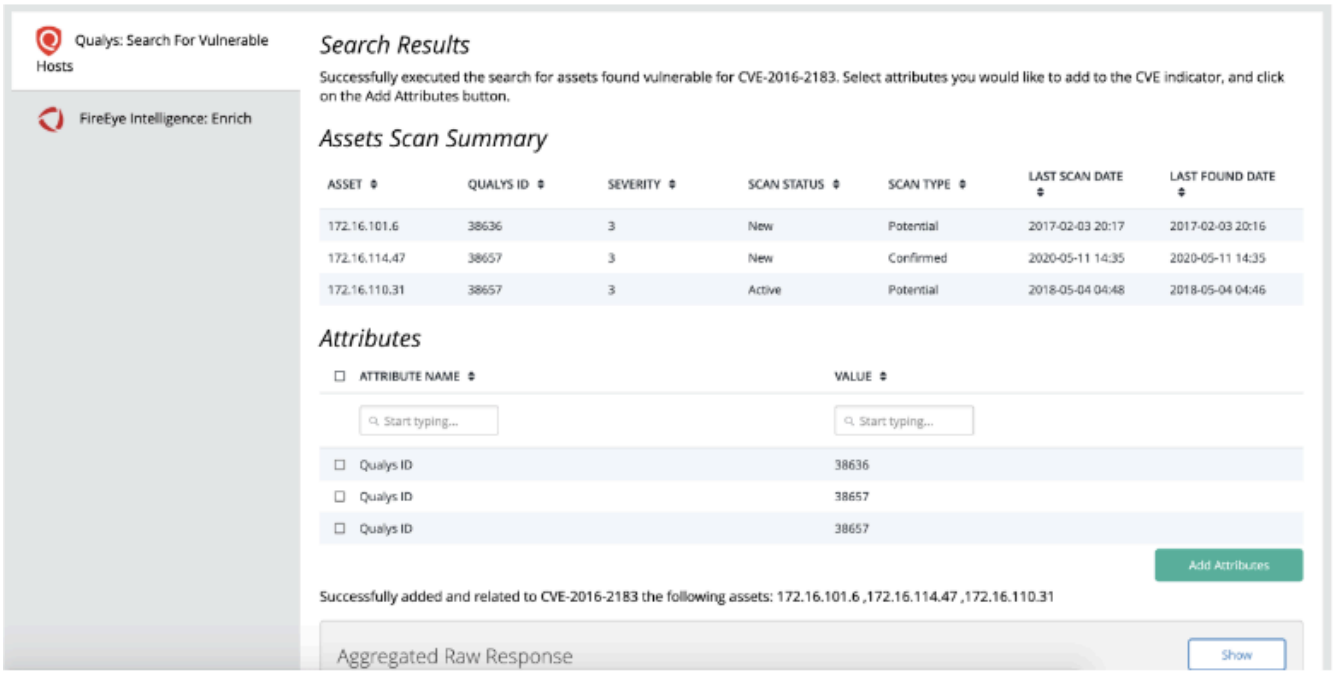
API Body Parameters:

```
{
    "action": "delete",
    "id": "1704353
}
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://qualysapi.qg2.apps.qualys.com/api/2.0/
simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-03-27T13:59:05Z</DATETIME>
        <TEXT>dynamic search list deleted successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1704353</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Example Result



Change Log

- **Version 1.1.0**
  - Added two new configuration fields: **Add Discovered Assets to ThreatQ** and **Add Asset Tags to CVEs**.
  - Fixed an issue where the Dynamic Search List would not be deleted if no vulnerable assets were discovered.
  - Fixed an issue where QID attributes were duplicated within the attributes table (in the operation's response).
  - Implemented additional error handling to properly display errors and the source of those errors.
  - Updated minimum ThreatQ version to 4.45.0
- **Version 1.0.0 rev-b (Guide Update)**
  - Added IP Whitelist section to Prerequisites chapter.
- **Version 1.0.0 rev-a (Guide Update)**
  - Updated the Prerequisites chapter regarding the Asset object. ThreatQ version 5.10.0 introduced the Asset object as a seeded default system object. Users on ThreatQ 5.10.0 or later do not have to install the Asset custom object prior to installing the integration.
- **Version 1.0.0**
  - Initial release