ThreatQuotient

Qualys Action Bundle User Guide

Version 1.0.1

August 28, 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	1.0.1
Compatible with ThreatQ Versions	>= 5.14.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Qualys Action Bundle provides the following actions:

- **Qualys Initiate Asset Scan** - submits a list of FQDN / IP Addresses to initiate a vulnerability scan.
- **Qualys Find Vulnerable Assets** - retrieves latest vulnerability scan results for IP Addresses.
- **Qualys CVE Enrichment** - enriches a CVE with additional context and assets.

The actions are compatible with the following system object types:

- Assets

  > The value of the Asset must be a valid IP Address.

- Indicators
  - CVE
  - FQDN
  - IP Address

The actions return the following enriched system objects:

- Assets
- Indicators
- Vulnerabilities

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- Qualys information
  - Host
  - Username
  - Password
  - Appliance name - can be located in Scans Application ({host}fo/tools/scannerAppliances.php).
  - Option title - can be located in Scans Options Profiles ({host}/fo/tools/optionProfiles.php).
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
  - Indicator (CVE, FQDN, IP Address)
  - Assets (must be a valid IP Address)

Installation

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

Configuration

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

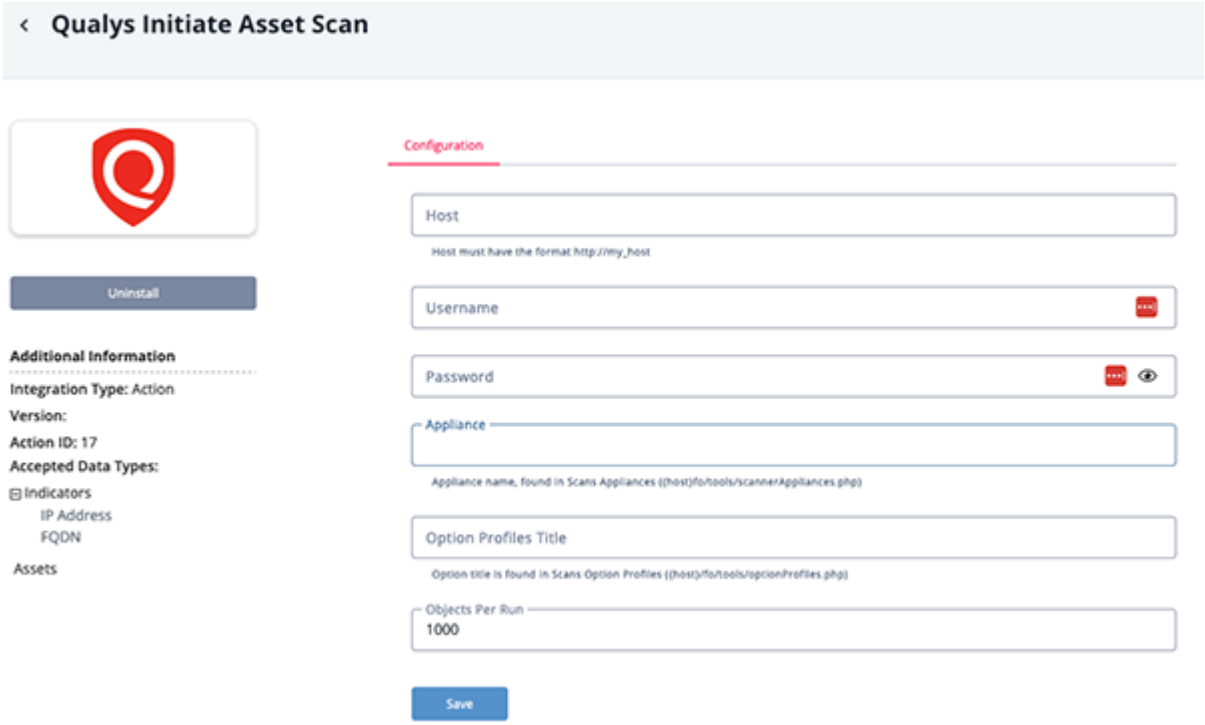
To configure the integration:

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

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Host	The Host or IP of the Qualys Platform.
Username	Your username to log into Qualys Platform.
Password	The password to log into Qualys Platform.
Qualys Tags *(Find Vulnerable Assets and CVE Enrichment Actions Only)*	Enable this option if Qualys tags should be included.
Save CVE Data As *(Find Vulnerable Assets Action Only)*	Select how to CVE data is ingested into the ThreatQ platform. Options include Indicators (default) and Vulnerabilities.
Vulnerability Look Up *(Find Vulnerable Assets Action Only)*	Select the supporting context. Options include:

PARAMETER	DESCRIPTION
	◦ Severity (default) ◦ CVSS Score (default) ◦ CVSS3 Score (default) ◦ Category ◦ Product ◦ Vendor ◦ Vendor Reference Id ◦ Vendor Reference URL ◦ Patchable ◦ Last Server Modification Time
Context Look Up *(CVE Enrichment Action Only)*	Select the supporting context. Options include: ◦ NVD Publish Date (default) ◦ Qualys Vulnerability Score (default) ◦ Qualys Vulnerability Score Last Changed Date (default) ◦ CVSS Score (default) ◦ CVSS Version (default) ◦ Exploit Maturity
Appliance *(Initiate Asset Scan Action Only)*	Enter Appliance name. This information can be found in Scans Appliances ({host}fo/tools/scannerAppliances.php).
Option Profiles Title *(Initiate Asset Scan Action Only)*	Enter the Option Profiles title. This information can be found in Scans Option Profiles ({host}/fo/tools/optionProfiles.php)
Objects per run	Enter the maximum number of objects to submit per run.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The action bundle provides the following actions:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Qualys Initiate Asset Scan	Submits a list of FQDN / IP Addresses to initiate a vulnerability scan.	Indicators, Assets	FQDN/IP Address
Qualys Find Vulnerable Assets	Retrieves latest vulnerability scan results for IP Addresses.	Indicators, Assets	IP Address
Qualys CVE Enrichment	Enriches a CVE with additional context and assets.	Indicators	CVE

Qualys Initiate Asset Scan

The **Qualys Initiate Asset Scan** action triggers a scan on the Qualys platform. Once the scan exists on the platform, it will grab the scan reference, and it will trigger the launch of the scan with Indicator or Asset values from the collection. All asset values must be valid IP Addresses. Launch datetime is saved as attribute for every Indicator in the collection.

`POST {{ Qualys_host }}/api/2.0/fo/scan/`

Sample Request:

```
{
  "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"POST",
  "params":{
    "action":"launch",
    "fqdn":"arcsight-soar.threatq.com,compute-1.amazonaws.com",
    "ip":"54.236.82.237,18.233.226.119",
    "iscanner_name":"Qualys-OpenStack",
    "option_title":"Scan",
    "target_from":"assets"
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/scan/"
}
```

Sample Response:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-07-23T14:22:22Z</DATETIME>
        <TEXT>New vm scan launched</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>30648027</VALUE>
            </ITEM>
            <ITEM>
                <KEY>REFERENCE</KEY>
                <VALUE>scan/1690122142.48027</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Qualys Scan (Supplemental)

```
POST {{ user_fields.Qualys_host }}/api/2.0/fo/scan/
```

Sample Request:

```
{
  "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"POST",
  "params":{
    "action":"list",
    "scan_ref":"scan/1690125120.48394",
    "show_last":1
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/scan/"
}
```

Sample Response:

```
<SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-07-23T14:44:26Z</DATETIME>
        <SCAN_LIST>
            <SCAN>
                <REF>scan/1690123397.48125</REF>
                <TYPE>API</TYPE>
                <TITLE>
                    <![CDATA[N/A]]>
                </TITLE>
                <USER_LOGIN>threa2br</USER_LOGIN>
                <LAUNCH_DATETIME>2023-07-23T14:43:17Z</LAUNCH_DATETIME>
                <DURATION>Pending</DURATION>
                <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
                <PROCESSED>0</PROCESSED>
                <STATUS>
                    <STATE>Queued</STATE>
                    <SUB_STATE>Launch_Requested</SUB_STATE>
                </STATUS>
                <TARGET>
                    <![CDATA[54.236.82.237,arcsight-
soar.threatq.com,compute-1.amazonaws.com]]>
                </TARGET>
            </SCAN>
        </SCAN_LIST>
    </RESPONSE>
</SCAN_LIST_OUTPUT>
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
SCAN_LIST_OUTPUT.RESPONSE.SCAN_LIST.SCAN.LAUNCH_DATETIME	Indicator/Asset Attribute	Scan Initiated	N/A	2023-07-23T14:43:17Z	N/A

Qualys Find Vulnerable Assets

The Find Vulnerable Assets action submits a list of IP address to Qualys in order to obtain assets and CVE vulnerability data. The IP addresses must belong to a collection that contains Indicators or Assets. All asset values must be valid IP Addresses. This data is ingested as assets, attributes for the submitted indicators and as vulnerability based on user configuration. All attributes are updatable.

`POST "{{host}}/api/2.0/fo/asset/host/vm/detection/"`

Sample Response:

```
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-07-13T13:15:11Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <HOST>
                <ID>1726122</ID>
                <IP>172.16.114.111</IP>
                <DNS>
                    <![CDATA[ec2-18-233-226-119.compute-1.amazonaws.com]]>
                </DNS>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <LAST_SCAN_DATETIME>2023-07-13T11:53:02Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2023-07-13T11:51:32Z</
LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>7919</LAST_VM_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <QID>6</QID>
                        <TYPE>Info</TYPE>
                        <SEVERITY>1</SEVERITY>
                        <RESULTS>
                            <![CDATA[IP address        Host name
172.16.114.111        No registered hostname]]>
                        </RESULTS>
                        <FIRST_FOUND_DATETIME>2023-07-13T10:59:28Z</
FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2023-07-13T11:51:32Z</
LAST_FOUND_DATETIME>
                        <TIMES_FOUND>2</TIMES_FOUND>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2023-07-13T11:53:02Z</
LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
```

```
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Get Vuln Knowledge Base(Supplemental)

This supplemental feed retrieves vulnerabilities for specified Qualys IDs.

```
GET {{user_fields.Qualys_host}}/api/2.0/fo/knowledge_base/vuln/
```

Sample Response:

```
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-07-20T12:44:57Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>150651</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Joomla! Core Webservice Endpoints Improper access
control Vulnerability (CVE-2023-23752)]]>
                </TITLE>
                <CATEGORY>Web Application</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2023-06-25T22:00:02Z</
LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2023-02-22T08:51:52Z</PUBLISHED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[joomla%21]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[joomla]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[Joomla! Security]]>
                        </ID>
                        <URL>
                            <![CDATA[https://developer.joomla.org/security-
centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
```

```
                        <![CDATA[CVE-2023-23752]]>
                    </ID>
                    <URL>
                        <![CDATA[http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2023-23752]]>
                    </URL>
                </CVE>
            </CVE_LIST>
            <DIAGNOSIS>
                <![CDATA[Joomla! is a free and open-source content
management system for publishing web content on websites.<P>
An improper access check allows unauthorized access to webservice endpoints.<P>
Affected Versions:<BR>
Joomla! versions 4.0.0 to 4.2.7<BR><P>QID Detection Logic:
(Unauthenticated)<BR>
This QID sends a HTTP GET request to access vulnerable webservice endpoint and
based on the response confirms if the target application is vulnerable.]]>
            </DIAGNOSIS>
            <CONSEQUENCE>
                <![CDATA[Successful exploitation could allow a remote
attacker to access sensitive information regarding the target
application.<P>]]>
            </CONSEQUENCE>
            <SOLUTION>
                <![CDATA[Customers are advised to install latest <A
HREF="https://downloads.joomla.org/" TARGET="_blank"> Joomla version 4.2.8</A>.
For more information regarding this vulnerability please visit<A HREF="https://
developer.joomla.org/security-centre/894-20230201-core-improper-access-check-
in-webservice-endpoints.html" TARGET="_blank"> Joomla! Security Advisory.</
A><P>Patch:<BR>
Following are links for downloading patches to fix the vulnerabilities:
<P><A HREF="https://developer.joomla.org/security-centre/894-20230201-core-
improper-access-check-in-webservice-endpoints.html" TARGET="_blank">Joomla!
Security Advisory</A>]]>
            </SOLUTION>
            <CORRELATION>
                <EXPLOITS>
                    <EXPLT_SRC>
                        <SRC_NAME>
                            <![CDATA[blogs]]>
                        </SRC_NAME>
                        <EXPLT_LIST>
                            <EXPLT>
                                <REF>
                                    <![CDATA[CVE-2023-23752]]>
                                </REF>
                                <DESC>
                                    <![CDATA[Joomla (CVE-2023-23752) - a
request parameter breaks through the Rest API]]>
                                </DESC>
```

```
                                    <LINK>
                                        <![CDATA[https://xz.aliyun.com/t/
12175]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                    </EXPLOITS>
                </CORRELATION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="2">
                        <![CDATA[Exploit_Public]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                    <ADDITIONAL_INFO>Patch Available, Exploit Available</
ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

ThreatQuotient provides the following default mapping for this function:

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	172.16.114.111	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.ID	Asset Attribute	Host ID	N/A	1726122	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.TRACKING_METHOD	Asset Attribute	Tracking Method	N/A	IP	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.DNS	Asset Attribute	DNS Hostname	N/A	ec2-18-233-226-119.compute-1.amazonaws.com	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.TAGS.TAG	Asset Tags	N/A	N/A	N/A	If 'Qualys Tags' user field is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.TITLE	Vulnerability Value	N/A	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Joomla! Core Webservice Endpoints Improper access control Vulnerability (CVE-2023-23752)	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.DIAGNOSIS	Vulnerability Description	N/A	N/A	Joomla! is a free and open-source content management system for publishing web content on websites....	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.SEVERITY_LEVEL	Vulnerability Attribute	Severity	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME		If 'Severity' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.CATEGORY	Vulnerability Attribute	Category	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Web Application	If 'Category' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.SOFTWARE_LIST.SOFTWARE.PRODUCT	Vulnerability Attribute	Product	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	joomla%21	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.SOFTWARE_LIST.SOFTWARE.VENDOR	Vulnerability Attribute	Vendor	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	joomla	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.VENDOR_REFERENCE_LIST.VENDOR_REFERENCE.ID	Vulnerability Attribute	Vendor Reference Id	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Joomla! Security	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.VENDOR_	Vulnerability Attribute	Vendor Reference URL	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	https://developer.joomla.org/security-centre/894-20230201-core-improper-a	If 'Qualys Tags' Supporting Context is checked

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
REFERENCE_LIST.VENDOR_REFERENCE.URL				ccess-check-in-webservice-endpoints.html	
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.CVSS.BASE	Vulnerability Attribute	CVSS Score	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.CVSS_V3.BASE	Vulnerability Attribute	CVSS3 Score	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PATCHABLE	Vulnerability Attribute	Patchable	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	1 mapped to Yes	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.LAST_SERVICE_MODIFICATION_DATETIME	Vulnerability Attribute	Last Server Modification Time	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	2023-06-25T22:00:02Z	If 'Qualys Tags' Supporting Context is checked
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.CVE_LIST.CVE.ID	Vulnerability/ Indicator Value	N/A / CVE	N/A	CVE-2023-23752	Vulnerability/ Indicator based on 'Save CVE Data as' selection
N/A	Vulnerability/ Indicator Attribute	Vulnerability found by Qualys	N/A	Yes	N/A

Qualys CVE Enrichment

Action that enriches a CVE indicator with context information from Qualys and related assets. In order to get from Qualys the list of related assets, a dynamic search list needs to be created. The search list id is used to retrieve Qualys IDs, that later are passed to `api/2.0/fo/asset/host/vm/detection/`. After the data is processed, the search list is deleted.

Dynamic Search list APIs are using the same base link with different parameters:

`POST {{host}}/api/2.0/fo/qid/search_list/dynamic/`

Create dynamic search list Request sample:

```
{
  "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"POST",
  "params":{
    "action":"create",
    "cve_ids":"CVE-2023-37454,CVE-2023-23333,CVE-2023-23752,CVE-2023-33246",
    "global":1,
    "title":"ThreatQ Search"
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/qid/search_list/
dynamic/"
}
```

Create dynamic search list Response sample:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-07-20T10:21:18Z</DATETIME>
        <TEXT>New search list created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1725971</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

List search list's QIDs Request sample:

```
{
  "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"GET",
  "params":{
```

```
    "action":"list",
    "ids":"1725971",
    "show_qids":1
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/qid/search_list/
dynamic/"
}
```


List search list's QIDs Response sample:


```
<DYNAMIC_SEARCH_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-07-20T11:11:52Z</DATETIME>
        <DYNAMIC_LISTS>
            <DYNAMIC_LIST>
                <ID>1725977</ID>
                <TITLE>
                    <![CDATA[ThreatQ Search]]>
                </TITLE>
                <GLOBAL>Yes</GLOBAL>
                <OWNER>
                    <![CDATA[Haig Colter (threa2br)]]>
                </OWNER>
                <CREATED>2023-07-20T11:09:22Z</CREATED>
                <MODIFIED_BY>
                    <![CDATA[Haig Colter (threa2br)]]>
                </MODIFIED_BY>
                <MODIFIED>2023-07-20T11:09:22Z</MODIFIED>
                <QIDS>
                    <QID>150651</QID>
                    <QID>730735</QID>
                    <QID>993602</QID>
                </QIDS>
                <CRITERIA>
                    <DISCOVERY_METHOD>
                        <![CDATA[All]]>
                    </DISCOVERY_METHOD>
                    <CVE_ID>
                        <!
[CDATA[CVE-2023-37454,CVE-2023-23333,CVE-2023-23752,CVE-2023-33246]]>
                    </CVE_ID>
                    <CVE_ID_FILTER>
                        <![CDATA[Contains]]>
                    </CVE_ID_FILTER>
                </CRITERIA>
            </DYNAMIC_LIST>
        </DYNAMIC_LISTS>
    </RESPONSE>
</DYNAMIC_SEARCH_LIST_OUTPUT>
```

Create dynamic search list Response sample:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-07-20T10:21:18Z</DATETIME>
        <TEXT>New search list created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1725971</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

List search list's QIDs Request sample:

```
{
  "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"GET",
  "params":{
    "action":"list",
    "ids":"1725971",
    "show_qids":1
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/qid/search_list/
dynamic/"
}
```

Delete dynamic search list Request sample:

```
{
 "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"POST",
  "params":{
    "action":"delete",
    "id":"1725971"
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/qid/search_list/
dynamic/"
}
```

Delete dynamic search list Response sample:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-07-23T18:21:15Z</DATETIME>
```

```
        <TEXT>dynamic search list deleted successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1725971</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Qualys CVE Detections(Supplemental)

Retrieves Assets from Qualys for QIDs associated with CVE Indicators passed previously to the dynamic search list and ingest into ThreatQ.

`POST "{{host}}/api/2.0/fo/asset/host/vm/detection/`

Sample Request:

```
{
  "headers":{
    "X-Requested-With":"Qualys Action 1.0.0"
  },
  "method":"POST",
  "params":{
    "action":"list",
    "qids":[
      "150651",
      "730735",
      "993602"
    ],
    "show_tags":1
  },
  "timeout":119,
  "url":"https://qualysguard.qg2.apps.qualys.com/api/2.0/fo/asset/host/vm/
detection/"
}
```

```
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-07-13T13:15:11Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <HOST>
                <ID>1726122</ID>
                <IP>172.16.114.111</IP>
                <DNS>
                    <![CDATA[ec2-18-233-226-119.compute-1.amazonaws.com]]>
                </DNS>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <LAST_SCAN_DATETIME>2023-07-13T11:53:02Z</LAST_SCAN_DATETIME>
```

```
                <LAST_VM_SCANNED_DATE>2023-07-13T11:51:32Z</
LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>7919</LAST_VM_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <QID>6</QID>
                        <TYPE>Info</TYPE>
                        <SEVERITY>1</SEVERITY>
                        <RESULTS>
                            <![CDATA[IP address        Host name
172.16.114.111        No registered hostname]]>
                        </RESULTS>
                        <FIRST_FOUND_DATETIME>2023-07-13T10:59:28Z</
FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2023-07-13T11:51:32Z</
LAST_FOUND_DATETIME>
                        <TIMES_FOUND>2</TIMES_FOUND>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2023-07-13T11:53:02Z</
LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Qualys CVE Knowledge Base(Supplemental)

Retrieves context data from Qualys for a CVE Indicator.

`POST {{host}}/api/2.0/fo/knowledge_base/qvs/`

Sample Response:

```
{
  "CVE-2021-23017": {
    "base": {
      "id": "CVE-2021-23017",
      "idType": "CVE",
      "qvs": "42",
      "qvsLastChangedDate": 1664755200,
      "nvdPublishedDate": 1622553300
    },
    "contributingFactors": {
      "cvss": "7.7",
      "cvssVersion": "v3.x",
      "cvssString": "AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L",
      "exploitMaturity": [
        "poc"
      ],
```

```
      "trending": [
        "07202023,06242023,06222023,06232023,07212023,06252023"
      ],
      "rti": [
        "remote"
      ]
    }
  }
}
```

ThreatQuotient provides the following default mapping for this function:

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	172.16.114.111	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.ID	Asset Attribute	Host ID	N/A	1726122	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.TRACKING_METHOD	Asset Attribute	Tracking Method	N/A	IP	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.DNS	Asset Attribute	DNS Hostname	N/A	ec2-18-233-226-119.compute-1.amazonaws.com	N/A
HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST.TAGS.TAG	Asset Tags	N/A	N/A	N/A	If 'Qualys Tags' user field is checked
CVE_value.base.nvdPublishedDate	Indicator Attribute	NVD Published Date	N/A	1622553300	Timestamp, if `NVD Published Date` Supporting Context is checked
CVE_value.base.Qvs	Indicator Attribute	Qualys Vulnerability Score	N/A	42	If `Qualys Vulnerability Score` Supporting Context is checked
CVE_value.base.qvsLastChangedDate	Indicator Attribute	Qualys Vulnerability Score Last Changed Date	N/A	1664755200	Timestamp, if `Qualys Vulnerability Score Last Changed Date` Supporting Context is checked
CVE_value.contributingFactors.cvss	Indicator Attribute	CVSS Score	N/A	7.7	If `CVSS Score` Supporting Context is checked
CVE_value.contributingFactors.cvssVersion	Indicator Attribute	CVSS Version	N/A	v3.x	If `CVSS Version` Supporting Context is checked
CVE_value.contributingFactors.exploitMaturity	Indicator Attribute	Exploit Maturity	N/A	["poc"]	If `Exploit Maturity` Supporting Context is checked

Enriched Data

> Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

Qualys Initiate Asset Scan

METRIC	RESULT
Run Time	1 minute
Indicators	1
Indicator Attributes	3

Qualys Find Vulnerable Assets

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	1
Vulnerability	1
Vulnerability Attributes	9
Asset	1
Asset Attributes	2

Qualys CVE Enrichment

METRIC	RESULT
Run Time	2 minutes
Indicators	4
Indicator Attributes	24
Asset	1
Asset Attributes	3

Known Issues / Limitations

- If the event that the Qualys CVE Enrichment action fails, you will have to manually delete the **ThreatQ Search** search list in `{host}/fo/scan/scanSearchLists.php` in order to run the action again.

Change Log

- **Version 1.0.1**
  - Resolved an error for the Qualys CVE Enrichment action that would occur when Qualys did not return any enrichment data.
- **Version 1.0.0**
  - Initial release