ThreatQuotient

Tenable.io Action Guide

Version 1.0.0

January 31, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Compatible with Tenable.io API Versions	>= 6.4.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/tenable-io-action

Introduction

The Tenable.io Action integrates with the Tenable.io API and provides visibility into the assets and vulnerabilities for an organization. The functions can run scans to identify vulnerabilities and submit data from a collection to retrieve vulnerability data for ingestion into the ThreatQ library.

The actions can perform the following functions:

- **Initiate Asset Scan** - Submits FQDN / IP Addresses to initiate a vulnerability scan
- **Find Vulnerable Assets** - Retrieves latest vulnerability scan results for FQDN / IP Addresses
- **CVE Enrichment** - Enriches a CVE with additional context and assets

The actions are compatible with the following system object types:

- FQDN
- IP Address
- IPv6 Address
- CVE

The actions return the following enriched system objects:

- Vulnerability

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

Prerequisites

- A Tenable.io API Access Key and Secret Key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one the following indicator objects:
    - FQDN
    - IP Address
    - IPv6 Address
    - CVE

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration 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
API Access Key	Your Tenable Access Key. This key can be generated under the Generate API Key section of the Tenable.io account settings.
API Secret	Your Tenable API Secret. This can be generated under the Generate API Key section of the Tenable.io account settings.
Object Per Run	The Maximum number of objects to submit per workflow run. The max value for this parameter is 50,000.

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

Action Functions

The action provides the following functions:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Initiate Asset Scan	Trigger a new scan for a list of indicators.	Indicator	FQDN, IP Address, IPv6 Address
Find Vulnerable Assets	Retrieves latest vulnerability scan results.	Indicator	FQDN, IP Address, IPv6 Address
CVE Enrichment	Enrich CVE indicators with vulnerabilities.	Indicator	CVE

Initiate Asset Scan

The **Initiate Asset Scan** action triggers a scan on the Tenable.io platform. It starts by creating the scan using the Basic Network Scan Template and default settings or a custom template. Once the scan exists on the platform, it will grab the **id** of the scan and it will trigger the launch of the scan with Indicator values from the collection.

Scan

```
POST "https://cloud.tenable.com/scans"
```

Sample Response:

```
{
  "scan": {
    "container_id": "3584b24b-7f26-4684-b644-a2a92103d6c2",
    "owner_uuid": "595e5aa0-e631-4e99-80e2-e1be8cc7bdc1",
    "uuid": "template-8b64a4a8-50b4-4077-bcc4-31f451fa3549f4f660ba792e0b0f",
    "name": "Full Network Scan",
    "description": "Scan all hosts daily",
    "policy_id": 16,
    "scanner_id": null,
    "scanner_uuid": "00000000-0000-0000-0000-00000000000000000000000000001",
    "emails": null,
    "sms": "",
    "enabled": true,
    "dashboard_file": null,
    "include_aggregate": true,
    "scan_time_window": null,
    "custom_targets": null,
    "starttime": null,
    "rrules": null,
    "timezone": "US/Central",
    "notification_filters": null,
    "tag_targets": [
      "1cf4f3a3-9878-44ce-9fa7-3a969c602e28",
      "9808942a-2053-43a7-8580-7caebdfb959f"
    ],
    "shared": 0,
    "user_permissions": 128,
    "default_permissions": 0,
    "owner": "user2@example.com",
    "owner_id": 2,
    "last_modification_date": 1544145190,
    "creation_date": 1544145190,
    "type": "public",
    "id": 26
  }
}
```

Launch

```
POST "https://cloud.tenable.com/scans/{{scan_id}}/launch"
```

Sample Response:

```
{
  "scan_uuid": "44346bcb-4afc-4db0-b283-2dd823fa8579"
}
```

Find Vulnerability Assets, CVE Enrichment

The Find Vulnerability Assets and CVE Enrichment functions enrich the selected collection of indicators with vulnerabilities for a target host or CVE.

The **Find Vulnerable Assets** action submits a FQDN or IP address to Tenable.io in order to obtain CVE vulnerability data. This data is added as attributes for the submitted indicators. All attributes cam be updated.

```
GET "https://cloud.tenable.com/workbenches/vulnerabilities?
filter.0.filter=host.target&filter.0.quality=match&filter.0.value={{host}}"
```

The **CVE Enrichment** action pushes each Indicator value to the Tenable.io platform where it will search vulnerabilities that match a target host. If there's a match, then it will pull the vulnerabilities and ingest them, otherwise it won't perform any action. Optionally, this action also has the ability to pull in any assets found to have vulnerabilities that are related to the specified CVE.

```
GET "https://cloud.tenable.com/workbenches/vulnerabilities?
filter.0.filter=plugin.attributes.cve.raw&filter.0.quality=match&filter.0.value={{cve}}"
```

Sample Response:

```
{
    "vulnerabilities": [
        {
            "count": 20,
            "plugin_family": "General",
            "plugin_id": 51192,
            "plugin_name": "SSL Certificate Cannot Be Trusted",
            "vulnerability_state": "Resurfaced",
            "accepted_count": 0,
            "recasted_count": 0,
            "counts_by_severity": [
                {
                    "count": 20,
                    "value": 2
                }
            ],
            "cvss_base_score": 6.4,
            "cvss3_base_score": 6.5,
            "severity": 2
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerabilities[].plugin_name	vulnerability.value	Vulnerability	N/A	SSL Certificate Cannot Be Trusted	N/A
.vulnerabilities[].plugin_family	vulnerability.attribute	Plugin Family	N/A	General	N/A
.vulnerabilities[].vulnerability_state	vulnerability.attribute	Vulnerability State	N/A	Resurfaced	N/A
.vulnerabilities[].count	vulnerability.attribute	Vulnerable Hosts Count	N/A	51	N/A
.vulnerabilities[].cvss_base_score	vulnerability.attribute	CVSS Base Score	N/A	6.4	N/A
.vulnerabilities[].cvss3_base_score	vulnerability.attribute	CVSS3 Base Score	N/A	6.5	N/A
.vulnerabilities[].severity	vulnerability.attribute	Severity	N/A	2	N/A

Known Issues / Limitations

- No more than 5,000 vulnerabilities can be retrieved at once
- It only retrieves vulnerabilities less than 15 months old
- No more than 10,000 scan can be created

Change Log

- **Version 1.0.0**
    - Initial release