ThreatQuotient

Tenable.io Action Bundle

Version 1.2.0

October 29, 2024

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	1.2.0
Compatible with ThreatQ Versions	>= 5.25.0
ThreatQ TQO License Required	Yes
Compatible with Tenable.io API Versions	>= 6.4.0
Support Tier	ThreatQ Supported

Introduction

The actions included with the Tenable.io Action Bundle integrate with the Tenable.io API and provide visibility into the assets and vulnerabilities for an organization. The actions can run scans to identify vulnerabilities and submit data from a collection to retrieve vulnerability data for ingestion into the ThreatQ library.

The action bundle provides the following actions:

- **Tenable.io Initiate Asset Scan** - submits a list of FQDN / IP Addresses Assets to initiate a vulnerability scan.
- **Tenable.io Find Vulnerable Assets** - retrieves latest vulnerability scan results for FQDN / IP Addresses Assets.
- **Tenable.io Remediated Assets** - retrieves latest vulnerability scan results for FQDN / IP Address Assets and unrelates the ones that are related to the Asset, but are not vulnerable anymore.
- **Tenable.io CVE Enrichment** - enriches a CVE with additional context and assets.

The actions are compatible with the following system object types:

- Assets
- Indicators
  - CVE
- Vulnerabilities

The actions return the following enriched system objects:

- Assets
- Indicators
  - CVE
- Vulnerabilities

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 object types:
  - Assets
  - Indicators
    - CVE
  - Vulnerabilities

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 bundle zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the 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
6. Select the individual actions to install and click **Install**.

   > 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.

7. The actions will be added to the integrations page. 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:

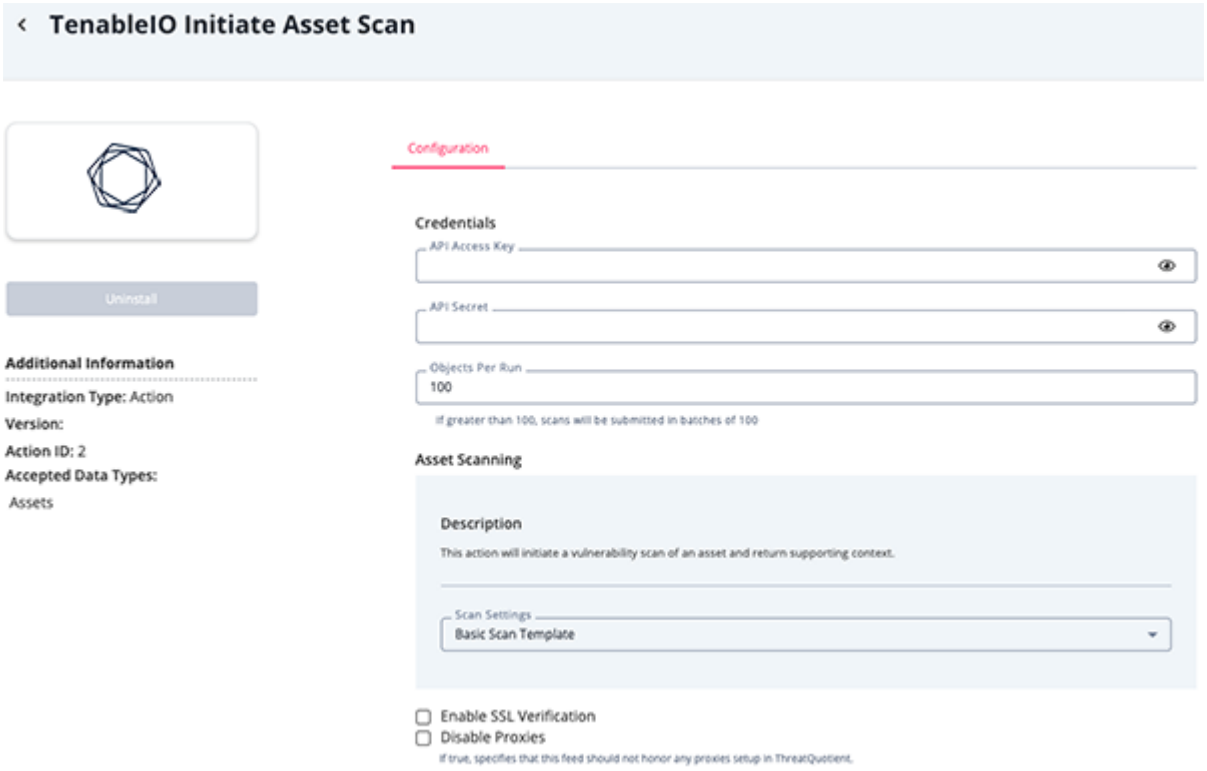
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

Initiate Asset Scan Parameters

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.
Scan Settings	Select a Scan Setting template to initiate a vulnerability scan of the asset and return support content. Options include **Basic Scan Template** (default) and **Custom**.
Scan Template ID	Enter a Scan ID Template. This parameter is only accessible if the `Custom` option is selected for the **Scan Settings** parameter.

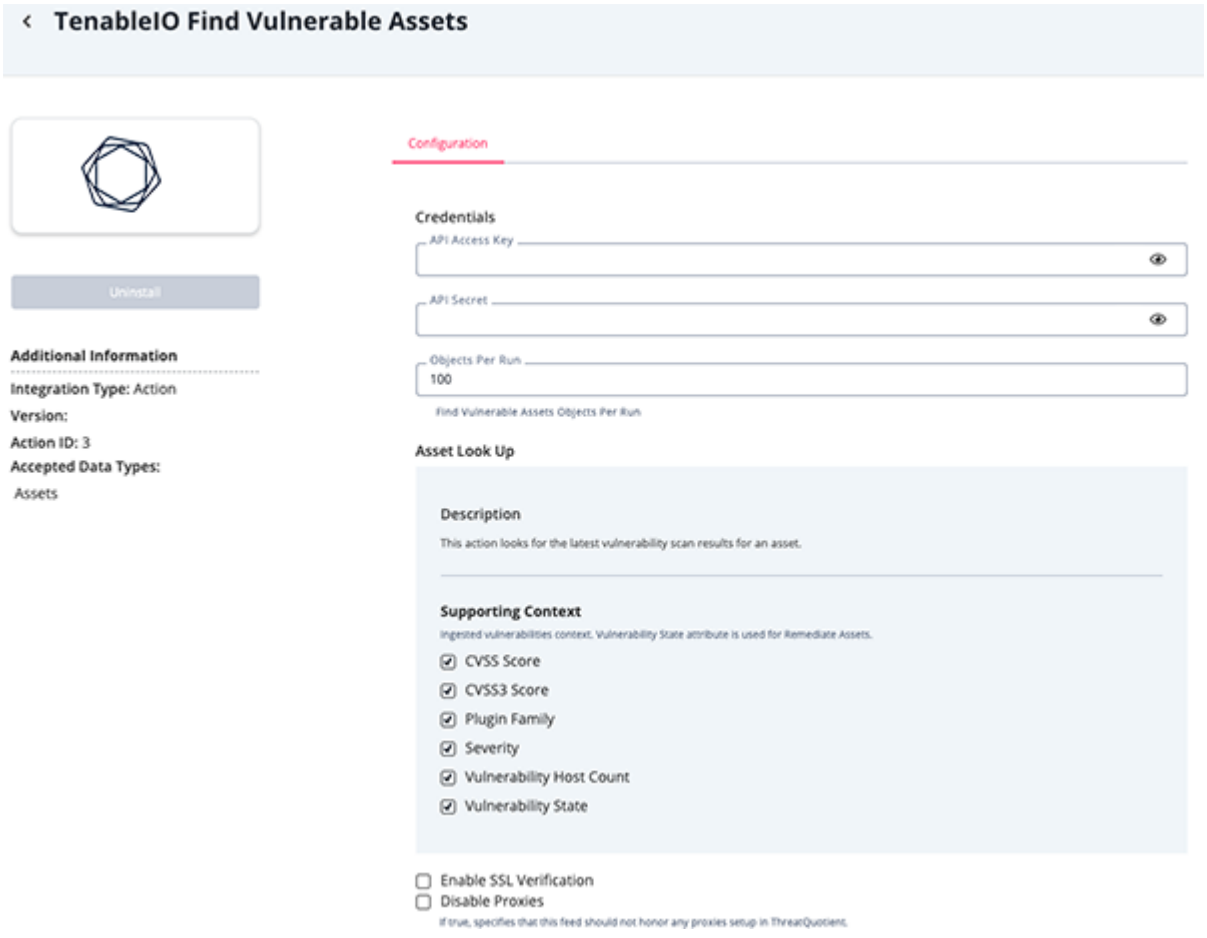
PARAMETER	DESCRIPTION
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.



Find Vulnerable Assets Parameters

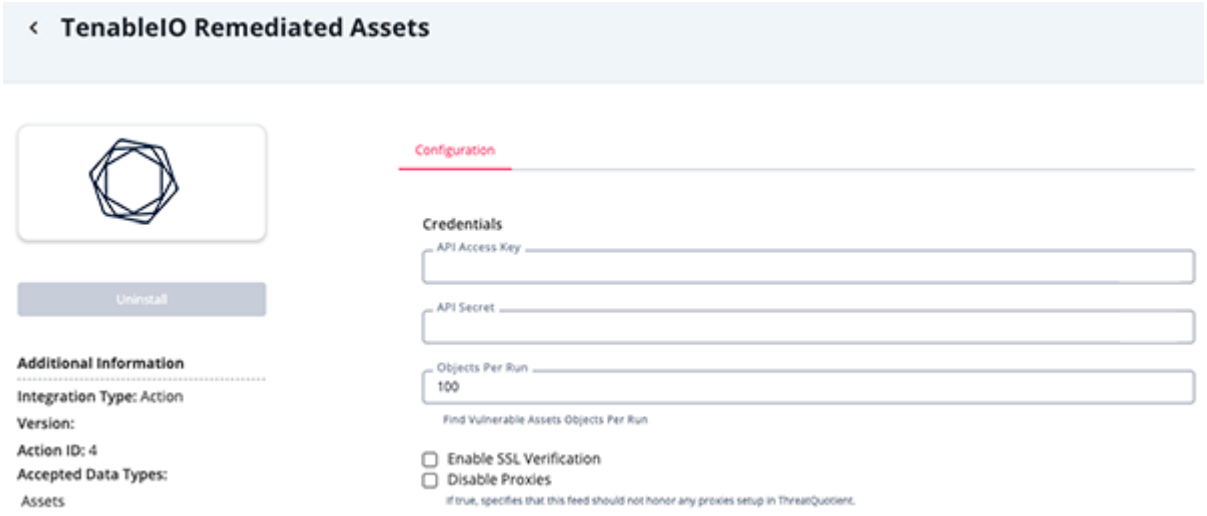
PARAMETER	DESCRIPTION
API Access Key	Your Tenable Access Key. This key can be generated under the Generate API Key section of the Tenable.io account settings.
API Secret	Your Tenable API Secret. This can be generated under the Generate API Key section of the Tenable.io account settings.

PARAMETER	DESCRIPTION
Object Per Run	The Maximum number of objects to submit per workflow run. The max value for this parameter is 50,000.
Supporting Context	Select the supporting attributes context to ingest for the Vulnerability. Options include: ◦ CVSS Score ◦ CVSS3 Score ◦ Plugin Family ◦ Severity ◦ Vulnerability Host Count ◦ Vulnerability State
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.



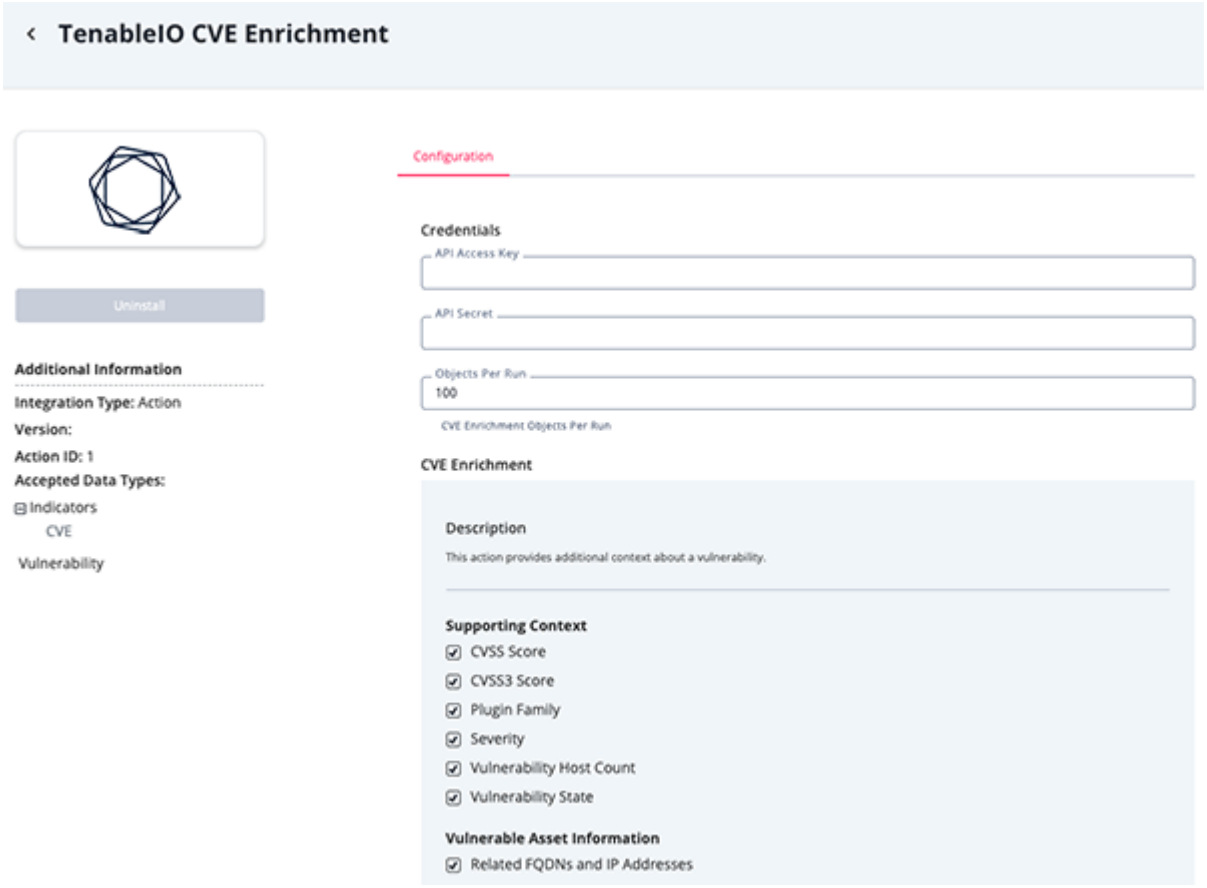
Remediated Assets Parameters

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.
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.



CVE Enrichment Parameters

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.
Supporting Context	Select the supporting attributes context to ingest for Vulnerability. Options include: ◦ CVSS Score ◦ CVSS3 Score (default) ◦ Plugin Family ◦ Severity (default) ◦ Vulnerability Host Count ◦ Vulnerability State (default)
Vulnerable Asset Information	Enable this parameter for CVE enrichment of Related FQDNs and IP Addresses.
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.



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

Actions

The bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Initiate Asset Scan	Trigger a new scan for a list of indicators.	Assets	N/A
Find Vulnerable Assets	Retrieves latest vulnerability scan results.	Assets	N/A
CVE Enrichment	Enrich CVE indicators with vulnerabilities.	Indicator, Vulnerability	Indicators - CVE
Remediated Assets	Unrelates vulnerabilities that are not present in latest scan results	Assets	N/A

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": "00000000-0000-0000-0000-000000000000000000000000000001",
    "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

The **TenableIO Find Vulnerable Assets** action submits a FQDN/IP address Assets to Tenable.io in order to obtain vulnerability data. This data is added as attributes for the submitted assets. All attributes are updatable.

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

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 action:

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	User-configurable; Updatable
.vulnerabilities[].vulnerability_state	vulnerability.attribute	Vulnerability State	N/A	Resurfaced	User-configurable; Updatable
.vulnerabilities[].count	vulnerability.attribute	Vulnerable Hosts Count	N/A	51	User-configurable; Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerabilities[].cvss_base_score	vulnerability.attribute	CVSS Base Score	N/A	6.4	User-configurable; Updatable
.vulnerabilities[].cvss3_base_score	vulnerability.attribute	CVSS3 Base Score	N/A	6.5	User-configurable; Updatable
.vulnerabilities[].severity	vulnerability.attribute	Severity	N/A	2	User-configurable; Updatable

CVE Enrichment

The CVE Enrichment action pushes each CVEs vulnerabilities or indicators 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=eq&filter.0.value={{cve}}"`

Sample Response:


```
{
    "vulnerabilities": [
        {
            "count": 1,
            "plugin_family": "Misc.",
            "plugin_id": 143221,
            "plugin_name": "ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities
(VMSA-2020-0026)",
            "vulnerability_state": "Active",
            "vpr_score": 6.5,
            "severity": 3,
            "accepted_count": 0,
            "recasted_count": 0,
            "counts_by_severity": [
                {
                    "count": 1,
                    "value": 3
                }
            ],
            "cvss_base_score": 7.2,
            "cvss3_base_score": 8.2
        }
    ],
    "total_vulnerability_count": 1,
    "total_asset_count": 0
}
```


ThreatQuotient provides the following default mapping for this action:

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	User-configurable; Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerabilities[].vulnerability_state	vulnerability.attribute	Vulnerability State	N/A	Resurfaced	User-configurable; Updatable
.vulnerabilities[].count	vulnerability.attribute	Vulnerable Hosts Count	N/A	51	User-configurable; Updatable
.vulnerabilities[].cvss_base_score	vulnerability.attribute	CVSS Base Score	N/A	6.4	User-configurable; Updatable
.vulnerabilities[].cvss3_base_score	vulnerability.attribute	CVSS3 Base Score	N/A	6.5	User-configurable; Updatable
.vulnerabilities[].severity	vulnerability.attribute	Severity	N/A	2	User-configurable; Updatable

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/assets/vulnerabilities?filter.0.filter=plugin.attributes.cve.raw&filter.0.quality=eq&filter.0.value={{cve}}
```

Sample Response:

```
{
  "assets": [
    {
      "id": "f60e219b-f8d9-481f-8dac-cfaf511bdf91",
      "severities": [
        {
          "count": 0,
          "level": 0,
          "name": "Info"
        }
      ],
      "total": 1,
      "fqdn": ["example.com"],
      "ipv4": [
        "192.168.1.20"
      ],
      "ipv6": [],
      "last_seen": "2024-09-17T19:40:12.204Z",
      "netbios_name": [],
      "agent_name": []
    }
  ],
  "total_asset_count": 1
}
```

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.assets[].fqdn[], assets[].ipv4[]	related asset.value	Asset	N/A	example.com(192.168.1.20)	User-configurable
.assets[].ipv4	asset.attribute	IP Address	N/A	192.168.1.20	N/A
.assets[].fqdn	asset.attribute	FQDN	N/A	example.com	N/A

Remediated Assets

The TenableIO Remediated Assets action submits a FQDN/IP address Assets to Tenable.io in order to obtain latest vulnerability data. If the Assets has related Vulnerabilities in TQ that are not found in latest results, then the Vulnerability is unrelated and the Vulnerability State attribute is set to Fixed.

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

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 action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	vulnerability.attribute	Vulnerability State	N/A	`Fixed`	Updatable; Attribute is set to `Fixed` only when it is unrelated from the Asset

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.

Initiate Asset Scan

METRIC	RESULT
Run Time	1 minute
Assets	3
Asset Attributes	3

Find Vulnerable Assets

METRIC	RESULT
Run Time	1 minute
Assets	4
Vulnerabilities	36
Vulnerability Attributes	211

Remediated Assets

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	33
Vulnerability Attributes	33

CVE Enrichment

METRIC	RESULT
Run Time	1 minute
Indicators	2
Assets	1
Asset Attributes	1
Vulnerabilities	5
Vulnerability Attributes	18

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 1.2.0**
  - Added a new action: **Tenable.io Remediated Assets**.
  - Updated Initiate Asset Scan and Find Vulnerable Assets actions to accept Assets instead of indicators.
  - Updated the search to only retrieve exact matches instead of substring matches for **TenableIO Find Vulnerable Asset** feed.
  - Updated the **TenableIO CVE Enrichment** action to accept collection of CVE Vulnerabilities or Indicators and to ingest related FQDN/IP Addresses as Assets instead of Indicators.
  - Updated the minimum ThreatQ version to 5.25.0.
- **Version 1.1.0**
  - Bulk scans are now supported.
  - Updated minimum ThreatQ version to 5.12.1.
  - The provider's logo will now appear in the action details view of ThreatQ, as well as the Workflow builder, if you install the action bundle using the zip file provided by the ThreatQ Marketplace.
- **Version 1.0.0**
  - Initial release