ThreatQuotient

Tenable IO Operation Guide

Version 1.1.0

August 29, 2022

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	>= 4.40.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/tenable-io-operation

Introduction

The Tenable.io Operation is an enrichment operation used to search for vulnerable assets in Tenable.io. The operation offers the option to add any discovered assets to ThreatQ and relate them to the CVE.

The operation provides the following action:

- **Search for Vulnerable Assets** - retrieves threat data information for a submitted CVE.

Prerequisites

Review the following prerequisites before attempting to install or upgrade the operation.

Asset Custom Object

The integration requires the Asset custom object.

Use the steps provided to install the asset 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 custom object 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 tenable_op
   ```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the tenable_op directory.

   ```
   mkdir images
   ```

7. Upload the asset.svg
8. Navigate to the **/tmp/tenable_op**.

   The directory should resemble the following:

   - tmp
     - **tenable_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 tenable_op
    ```

Installation

> ⚠ The operation requires that the Asset custom object be installed on your ThreatQ instance prior to installing the operation. Attempting to install or upgrade the operation without the Asset custom object will cause the installation process to fail. See the Prerequisites chapter for more details.

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration 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 feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

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	The hostname of Tenable.io.
Access Key	The API access key for Tenable.io.
Secret Key	The API secret key for Tenable.io.
Auto Discovered Assets to ThreatQ	Check this box to automatically add any discovered assets to ThreatQ. The assets will be added as an Asset object.

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 Assets	Search for Vulnerable Assets	Indicators	CVE

The action utilizes two endpoints:

- `/workbenches/vulnerabilities`
- `/workbenches/assets/vulnerabilities`

Search for Vulnerable Assets

The Search for Vulnerable Assets retrieves vulnerable assets for a CVE system object.

```
GET https://<Tenable.io Host>/workbenches/vulnerabilities
```

Sample Request:

```
{
  "filter.0.quality": "eq",
  "filter.0.filter": "plugin.attributes.cve.raw",
  "filter.0.value": "CVE-2019-17053",
  "filter.search_type": "and"
}
```

Sample Response:

```
{
  "total_asset_count": 0,
  "vulnerabilities": [
    {
      "accepted_count": 0,
      "counts_by_severity": [
        {
          "count": 2,
          "value": 3
        }
      ],
      "recasted_count": 0,
      "plugin_name": "CentOS 7 : kernel (CESA-2020:4060)",
      "cvss3_base_score": 8.1,
      "count": 2,
      "cvss_base_score": 9.3,
      "vulnerability_state": "Active",
      "plugin_family": "CentOS Local Security Checks",
      "vpr_score": 6.7,
      "severity": 3,
      "plugin_id": 141619
    }
  ],
  "total_vulnerability_count": 2
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.vulnerabilities[].severity	Vulnerability.Attribute	Severity	NA	High
response.vulnerabilities[].vpr_score	Vulnerability.Attribute	Vulnerability Priority Rating	NA	6.7
response.vulnerabilities[].plugin_name	Vulnerability.Attribute	Plugin Name	NA	CentOS 7 : kernel (CESA-2020:4060)
response.vulnerabilities[].count	Vulnerability.Attribute	Vulnerable Hosts	NA	2
response.vulnerabilities[].plugin_family	Vulnerability.Attribute	Plugin Family	NA	CentOS Local Security Checks

Search for Assets Vulnerable for the Specific CVE

The following example demonstrates the action for a specified CVE.

`GET https://<Tenable.io Host>/workbenches/assets/vulnerabilities`

Request:

```
{
  "filter.0.quality": "eq",
  "filter.0.filter": "plugin.attributes.cve.raw",
  "filter.0.value": "CVE-2019-17053",
  "filter.search_type": "and"
}
```

Response:

```
{
  "total_asset_count": 2,
  "assets": [
    {
      "agent_name": [],
      "ipv4": [
        "10.13.0.107",
        "192.168.122.1"
      ],
      "id": "00519c43-f57a-4b49-a2c6-53f426478059",
      "fqdn": [],
      "ipv6": [
        "fe80:0:0:0:6ed6:27a2:3b5b:eed9"
      ],
      "severities": [
        {
          "level": 0,
          "name": "Info",
          "count": 0
        },
        {
          "level": 1,
          "name": "Low",
          "count": 0
        },
        {
          "level": 2,
          "name": "Medium",
          "count": 0
        },
        {
          "level": 3,
          "name": "High",
          "count": 1
        },
        {
          "level": 4,
          "name": "Critical",
          "count": 0
        }
      ],
      "last_seen": "2021-02-10T22:20:41.260Z",
      "netbios_name": [],
      "total": 1
    },
    {
      "agent_name": [],
      "ipv4": [
        "172.18.0.1",
        "10.13.0.147"
      ],
      "id": "cfa68026-6409-4b89-a7bf-667f2fae9a6f",
      "fqdn": [],
      "ipv6": [
        "fe80:0:0:0:dca7:17ff:fedb:f15c",
        "fe80:0:0:0:981b:caff:fef0:aa29",
        "fe80:0:0:0:3874:4ff:feed:f33a",
        "fe80:0:0:0:42:f8ff:fe7e:b0f3",
        "fe80:0:0:0:16ed:7dde:cc7f:d7dd",
        "fe80:0:0:0:3bf4:f4ab:9433:cd29"
      ],
      "severities": [
        {
          "level": 0,
          "name": "Info",
          "count": 0
        },
        {
          "level": 1,
          "name": "Low",
          "count": 0
        },
        {
          "level": 2,
          "name": "Medium",
          "count": 0
        },
        {
          "level": 3,
          "name": "High",
          "count": 1
        },
        {
          "level": 4,
          "name": "Critical",
          "count": 0
        }
      ],
      "last_seen": "2021-02-10T22:20:41.260Z",
      "netbios_name": [],
      "total": 1
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this example:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.assets[].agent_name	Asset.Attribute	AGENT NAME	NA	homenet_agent
response.assets[].id	Asset.Attribute	ID	NA	f7f0c11b-ce76-496d-9fb6-cf9262a8bedb
response.assets[].ipv4	Asset.Attribute	IPV4 ADDRESS	NA	172.18.0.1
response.assets[].fqdn	Asset.Attribute	FQDN	NA	10.13.0.147
response.assets[].ipv6	Asset.Attribute	IPV6 ADDRESS	NA	fe80:0:0:0:dca7:17ff:fedb:f15c
response.assets[].last_seen	Asset.Attribute	LAST SEEN	NA	July 12 2022 07:38:15 PM UTC
response.assets[].netbios_name	Asset.Attribute	NETBIOS NAME	NA	NA
response.assets[].total	Asset.Attribute	TOTAL VULNERABILITIES	NA	1
response.assets[].severities	Asset.Attribute	SEVERITY	NA	High

Change Log

- **Version 1.2.0**
  - Updated the Attribute list to Asset objects in ThreatQ.
- **Version 1.1.0**
  - Added the ability to create and relate Asset objects in ThreatQ. The Asset custom object is required for this - see the Prerequisites chapter for more details.
  - Added improved logging and messaging in the ThreatQ UI.
- **Version 1.0.0**
  - Initial release