ThreatQuotient

Tenable.sc Action

Version 1.0.0

November 26, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.25.0
Compatible with Tenable.io API Versions	>=6.4.5
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Tenable.sc Action integration captures vulnerability data from Tenable.sc for submitted ThreatQ Asset types as well as removes relationships for Assets no longer deemed vulnerable.

The integration provides the following action:

- **Tenable.sc Vulnerability Remediation** - retrieves vulnerability analysis results for IP Address Assets and unrelates the ones that are related to the Asset that are no longer vulnerable.

The action is compatible with ThreatQ Asset object types and returns enriched Vulnerability objects.

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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one Asset object type.
- Tenable.sc hostname/Ip address, API Access Key, and API Secret Key.

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

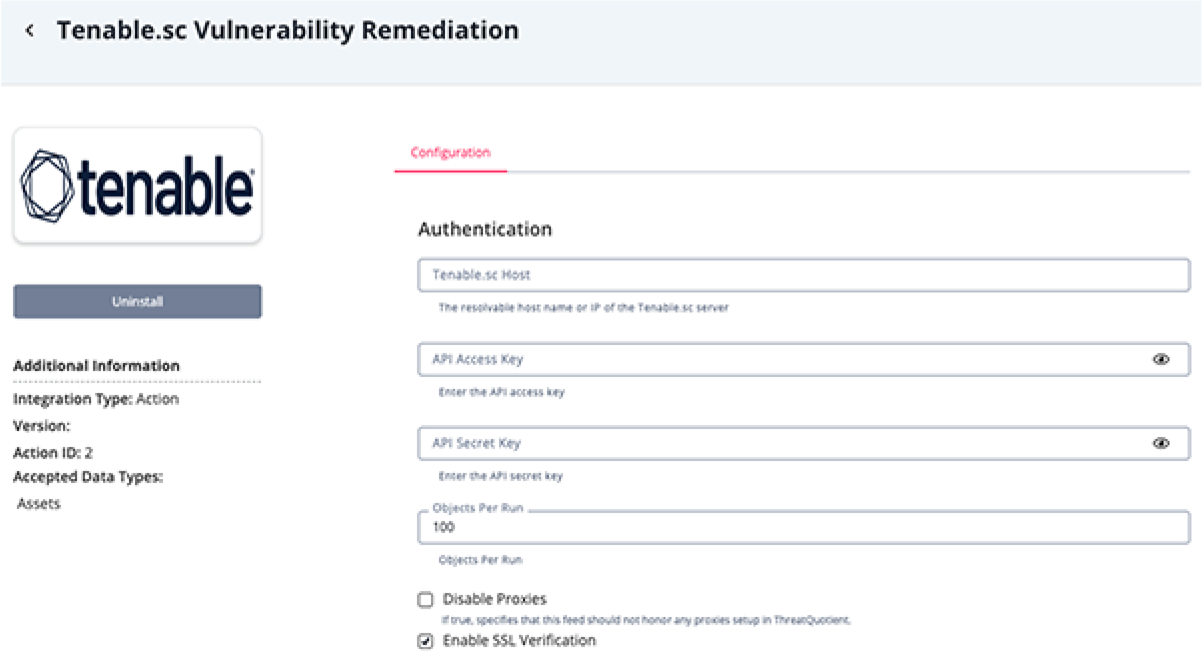
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
Tenable.sc Host	Enter the Hostname or IP Address of the Tenable.sc server
API Access Key	Enter the API Access Key generated in the Tenable.sc account settings,
API Secret Key	Enter the API Secret Key generated in the Tenable.sc account settings.
Objects per run	Enter the maximum number of objects to submit per run.
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.



Tenable.sc Vulnerability Remediation

Additional Information

Integration Type: Action

Version:

Action ID: 2

Accepted Data Types:

Assets

Authentication

Tenable.sc Host

The resolvable host name or IP of the Tenable.sc server

API Access Key

Enter the API access key

API Secret Key

Enter the API secret key

Objects Per Run: 100

Objects Per Run

□ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

☑ Enable SSL Verification

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

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Tenable.sc Vulnerability Remediation	Unrelates vulnerabilities that are not present in analysis results.	Asset	N/A

Tenable.sc Vulnerability Remediation

The Tenable.sc Vulnerability Remediation action submits IP Address Assets to Tenable.sc in order to obtain vulnerability data. If the Assets have related Vulnerabilities in TQ that are not found in analysis results, then the Vulnerability is unrelated and the Vulnerability State attribute is set to Fixed.

`POST "{host}/rest/analysis"`

> Tenable.sc Vulnerabilities are retrieved in two different requests, one for vulnerabilities(`tool="vulnipsummary"`) and another for CVEs (`tool="cveipdetail"`).

Vulnerabilities Requests

Sample Request:

```
{
    "query": {
        "endOffset": 10,
        "filters": [
            {
                "filterName": "ip",
                "operator": "=",
                "value": "1.50.134.231"
            }
        ],
        "startOffset": 0,
        "tool": "vulnipsummary",
        "type": "vuln"
    },
    "sourceType": "cumulative",
    "type": "vuln"
}
```

Sample Response:

```
{
    "type": "regular",
    "response": {
        "totalRecords": "4",
        "returnedRecords": 4,
        "startOffset": "0",
        "endOffset": "10",
        "matchingDataElementCount": "4",
        "results": [
            {
                "pluginID": "11356",
                "total": "1",
                "severity": {
                    "id": "4",
                    "name": "Critical",
                    "description": "Critical Severity"
                },
                "name": "NFS Exported Share Information Disclosure",
                "pluginDescription": "At least one of the NFS shares exported
by the remote server could be mounted by the scanning host.  An attacker may be
able to leverage this to read (and possibly write) files on remote host.
\n\nNote: Shares protected by an ACL that includes the IP of the Nessus host
will not be tested.",
                "repositoryID": "2",
                "hosts": [
                    {
                        "iplist": "1.50.134.231",
                        "uuidIPsList": "",
                        "repository": {
                            "id": "2",
                            "name": "Staged-Large",
                            "description": "",
                            "dataFormat": "IPv4"
                        }
                    }
                ],
                "family": {
                    "id": "28",
                    "name": "RPC",
                    "type": "active"
                }
            }
          ]
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1732194773
}
```

CVEs Requests

Sample Request:

```
{
    "query": {
        "endOffset": 10,
        "filters": [
            {
                "filterName": "ip",
                "operator": "=",
                "value": "1.50.134.231"
            }
        ],
        "startOffset": 0,
        "tool": "cveipdetail",
        "type": "vuln"
    },
    "sourceType": "cumulative",
    "type": "vuln"
}
```

Sample Response:

```
{
  "type": "regular",
  "response": {
    "totalRecords": "84",
    "returnedRecords": 10,
    "startOffset": "0",
    "endOffset": "10",
    "matchingDataElementCount": "84",
    "results": [
      {
        "cveID": "CVE-1999-0632",
        "total": "1",
        "hosts": [
          {
            "repositoryID": "2",
            "iplist": [
              {
                "ip": "1.50.134.231",
                "uuid": "957d8559-504b-4337-a7b6-262bd85dab8e",
                "hostUUID": "",
                "macAddress": "",
                "netbiosName": "",
                "dnsName": "jaij320cpqbwvjh6.example.demo"
              }
            ]
          }
        ]
      }
    ]
  },
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1732529590
}
```

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`	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.

METRIC	RESULT
Run Time	1 min
Vulnerabilities	33
Vulnerability Attributes	33

Use Case Example

1. A user submits a collection of IP Address Assets to the Tenable.sc API using the **Tenable.sc Vulnerability Remediation** action.
2. The Tenable.sc API queries vulnerability data for the specified IP Address.
3. The action verifies if all the related Tenable.sc vulnerabilities existing in ThreatQ are still present in the Tenable response. If they are not present, it means that they have been remediated. The action will then unrelate the vulnerability and will set the vulnerability **Vulnerability State** attribute to **Fixed**.

Change Log

- **Version 1.0.0**
  - Initial release