

# ThreatQuotient



## Tenable.io CDF Guide

**Version 1.0.0**

March 28, 2023

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147



ThreatQ Supported

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

- Integration Details..... 5
- Introduction ..... 6
- Prerequisites..... 7
  - Asset Object ..... 7
- Installation..... 9
- Configuration ..... 10
- ThreatQ Mapping..... 13
  - Tenable.io Vulnerable Assets ..... 13
  - Get Export Job Chunk (Supplemental) ..... 16
  - Get Export Job (Supplemental)..... 19
- Average Feed Run..... 20
- Change Log..... 21

# 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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto: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
----------------------------------	----------

Support Tier	ThreatQ Supported
--------------	-------------------

ThreatQ Marketplace	<a href="https://marketplace.threatq.com/details/tenable-io-cdf">https:// marketplace.threatq.com/ details/tenable-io-cdf</a>
---------------------	---

# Introduction

The Tenable.io CDF for ThreatQ enables analysts to automatically ingest vulnerability feeds from Tenable.io.

The integration provides the following feed:

- **Tenable.io Vulnerable Assets** - pulls vulnerable assets from Tenable.io including asset metadata, its vulnerabilities, and relevant CVEs.

The integration ingests the following system objects:

- Assets
  - Asset Attributes
- Indicators
- Vulnerabilities
  - Vulnerability Attributes


# Prerequisites

The CDF integration requires the following:


- A Tenable.io Cloud license
- Tenable.io API Credentials with `CAN_VIEW` permissions on `ASSETS`.
- The Asset Object type installed on your ThreatQ instance.

## Asset Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

 You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system 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_cdf
```

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

```
<> mkdir images
```

7. Upload the asset.svg.
8. Navigate to the `/tmp/tenable_cdf`.

The directory should resemble the following:

- tmp
  - `tenable_cdf`
    - `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.

```
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)
```

```
Application is now in maintenance mode.
```

```
Installing Custom Objects - Step 2 of 5 (Installing the Asset Custom Object)
```

```
Installing Custom Objects - Step 3 of 5 (Configuring image for Asset Custom Object)
```

```
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
```

```
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode)
```

```
Application is now live.
```


```
-
```

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf tenable_cdf
```



# Installation

 The CDF requires the installation of a custom object before installing the actual CDF if you are on ThreatQ version 5.9.0 or earlier. See the [Prerequisites](#) chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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 **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Access Key	Your Tenable.io Access Key to authenticate. <div> Your credentials must have the <code>CAN_VIEW</code> permission on <b>ASSETS</b>.</div>
Secret Key	Your Tenable.io Secret Key to authenticate. <div> Your credentials must have the <code>CAN_VIEW</code> permission on <b>ASSETS</b>.</div>
State Filter	Select one or more vulnerability states to include in the export.  Options include: <ul style="list-style-type: none"><li>◦ Open (default)</li><li>◦ Reopened (default)</li><li>◦ Fixed (default)</li></ul>

PARAMETER	DESCRIPTION
Severity Filter	Select one or more vulnerability severities to include in the export. <ul style="list-style-type: none"><li>◦ Info</li><li>◦ Low (default)</li><li>◦ Medium (default)</li><li>◦ High (default)</li><li>◦ Critical (default)</li></ul>
VPR Score Threshold	The minimum VPR score required to ingest a given vulnerability. If this value is set to 0.0, the default, a VPR score will not be required.
Require CVE	Enable this option to only ingest vulnerabilities that have at least one CVE associated with it. This option is disabled by default.
Include Unlicensed Assets	Enable this option to include assets that are unlicensed in the export. This option is enabled by default.
Export Timeout (Minutes)	The number of minutes to wait for the export to complete before timing out. The default value for this option is 30 (minutes).

## < Tenable.io Vulnerable Assets



Disabled ☐ Enabled

Uninstall

### Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Configuration Activity Log

Access Key

Enter your Tenable.io Access Key to authenticate. Your credentials must have the CAN\_VIEW permission on ASSETS.

Secret Key

Enter your Tenable.io Secret Key to authenticate. Your credentials must have the CAN\_VIEW permission on ASSETS.

#### State Filter

Select one or more vulnerability states to include in the export.

- ☒ Open
- ☒ Reopened
- ☒ Fixed

#### Severity Filter

Select one or more vulnerability severities to include in the export.

- ☐ Info
- ☒ Low
- ☒ Medium
- ☒ High
- ☒ Critical

VPR Score Threshold

0.0

The minimum VPR score (0-100) required to ingest a given vulnerability. If 0, a VPR score will not be required.

☐ Require CVE

Only ingest vulnerabilities that have at least one CVE associated with it.

☒ Include Unlicensed Assets

Include assets that are unlicensed in the export.

Export Timeout (Minutes)

30

Enter a number representing the amount of minutes to wait for the export to complete before timing out.

Set Indicator status to...

Active

Run Frequency

Hourly

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

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.

# ThreatQ Mapping

## Tenable.io Vulnerable Assets

The Tenable.io Vulnerable Assets feed periodically pulls vulnerable assets from Tenable.io, including metadata for the assets themselves, their vulnerabilities, and relevant CVEs.

POST `https://cloud.tenable.com/vulns/export`

### Sample Request Body:

```
{
  "filters": {
    "state": ["<selected state filters>"],
    "severity": ["<selected severity filters>"],
    "since": "<feed last run timestamp>"
  },
  "num_assets": 500,
  "include_unlicensed": true
}
```

### Sample Response:

```
{
  "export_uuid": "<UUID>"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].asset.fqdn, [].asset.ipv4	Asset.Value	N/A	.first_found	localhost.localdomain (10.13.0.163)	Selected keys are formatted into a description template
[].plugin.name	Vulnerability.Value	N/A	.plugin.publication_date	SSH Server CBC Mode Ciphers Enabled	N/A
[].plugin.description	Vulnerability.Description	N/A	N/A	N/A	N/A
[].plugin.cve[]	Indicator.Value	CVE	N/A	CVE-2022-12312	N/A
[].asset.fqdn	Asset.Attribute	FQDN	N/A	N/A	N/A
[].asset.ipv4	Asset.Attribute	IP Address	N/A	N/A	N/A
[].asset.device_type	Asset.Attribute	Device Type	N/A	general-purpose	N/A
[].asset.uuid	Asset.Attribute	Tenable.io UUID	N/A	N/A	N/A
[].asset.mac_address	Asset.Attribute	MAC Address	N/A	N/A	N/A
[].asset.operating_system[]	Asset.Attribute	Operating System	N/A	Linux Kernel 3.10.0-1160.76.1.el7.x86_64 on CentOS Linux release 7.9.2009 (Core)	N/A
[].state	Asset.Attribute	Vulnerable State	N/A	OPEN	N/A
[].port.service	Asset.Attribute	Tested Service	N/A	www	N/A
[].severity	Vulnerability.Attribute	Severity	N/A	Medium	N/A
[].last_found	Vulnerability.Attribute	Last Found	N/A	N/A	timestamp
[].plugin.family	Vulnerability.Attribute	Family	N/A	Misc.	N/A
[].plugin.type	Vulnerability.Attribute	Vulnerability Type	N/A	remote	N/A
[].plugin.has_patch	Vulnerability.Attribute	Has Patch	N/A	False	Bool -> True/False
[].plugin.exploit_availability	Vulnerability.Attribute	Exploit Available	N/A	False	Bool -> True/False
[].plugin.exploited_by_malware	Vulnerability.Attribute	Exploited by Malware	N/A	False	Bool -> True/False
[].plugin.exploitability_ease	Vulnerability.Attribute	Exploitability Ease	N/A	Medium	N/A
[].plugin.in_the_news	Vulnerability.Attribute	In News	N/A	False	Bool -> True/False
[].plugin.risk_factor	Vulnerability.Attribute	Risk Factor	N/A	Low	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].plugin.synopsis	Vulnerability.Attribute	Synopsis	N/A	N/A	N/A
[].plugin.solution	Vulnerability.Attribute	Solution	N/A	N/A	N/A
[].plugin.unsupported_by_vendor	Vulnerability.Attribute	Unsupported by Vendor	N/A	False	Bool -> True/False
[].plugin.vuln_publication_date	Vulnerability.Attribute	Publication Date	N/A	N/A	N/A
[].plugin.vpr.score	Vulnerability.Attribute	VPR Score	N/A	2.1	N/A
[].plugin.vpr.drivers.product_coverage	Vulnerability.Attribute	VPR Product Coverage	N/A	HIGH	N/A
[].plugin.xrefs[]	Vulnerability.Attribute	CWE	N/A	CWE-200	Where type == 'CWE'
[].plugin.vpr.drivers.threat_intensity_last28	Vulnerability.Attribute	VPR Threat Intensity	N/A	VERY_LOW	N/A
[].plugin.vpr.drivers.exploit_code_maturity	Vulnerability.Attribute	VPR Exploit Code Maturity	N/A	VERY_LOW	N/A
[].plugin.see_also[]	Vulnerability.Attribute	External Reference	N/A	N/A	N/A

## Get Export Job Chunk (Supplemental)

The Get Export Job Chunk supplemental feed fetches a specific chunk of the export job's results.

GET <https://cloud.tenable.com/vulns/export/{{ uuid }}/chunks/{{ chunk }}>

### Sample Response:

```
[
  {
    "asset": {
      "agent_uuid": "7640d8143c5f4830834fd4128697cd45",
      "bios_uuid": "53e22042-a344-ae31-0b79-0a58ab414826",
      "device_type": "general-purpose",
      "fqdn": "localhost.localdomain",
      "hostname": "10.13.0.163",
      "uuid": "caa34c9e-a1de-4ea3-9d91-90387b0965d1",
      "ipv4": "10.13.0.102",
      "last_authenticated_results": "2022-11-28T19:16:16Z",
      "mac_address": "02:42:59:E1:E1:C9",
      "operating_system": [
        "Linux Kernel 3.10.0-1160.76.1.el7.x86_64 on CentOS Linux release 7.9.2009 (Core)"
      ],
      "network_id": "00000000-0000-0000-0000-000000000000",
      "tracked": true
    },
    "output": "\n\nThe following client-to-server Cipher Block Chaining (CBC) algorithms\nare supported : \n\n3des-cbc\n aes128-cbc\n aes192-cbc\n aes256-cbc\n blowfish-cbc\n cast128-cbc\n\nThe following server-to-client\nCipher Block Chaining (CBC) algorithms\nare supported : \n\n 3des-cbc\n aes128-cbc\n aes192-cbc\n aes256-cbc\n\nblowfish-cbc\n cast128-cbc\n",
    "plugin": {
      "bid": [
        32319
      ],
      "checks_for_default_account": false,
      "checks_for_malware": false,
      "cve": [
        "CVE-2008-5161"
      ],
      "cvss3_base_score": 0,
      "cvss3_temporal_score": 0,
      "cvss_base_score": 2.6,
      "cvss_temporal_score": 1.9,
      "cvss_temporal_vector": {
        "exploitability": "Unproven",
        "remediation_level": "Official-fix",
        "report_confidence": "Confirmed",
        "raw": "E:U/RL:OF/RC:C"
      },
      "cvss_vector": {
        "access_complexity": "High",
        "access_vector": "Network",
        "authentication": "None required",
        "availability_impact": "None",
        "confidentiality_impact": "Partial",

```



```
    "integrity_impact": "None",
    "raw": "AV:N/AC:H/Au:N/C:P/I:N/A:N"
  },
  "description": "The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may
allow an attacker to recover the plaintext message from the ciphertext. \n\nNote that this plugin only checks for the
options of the SSH server and does not check for vulnerable software versions.",
  "exploit_available": false,
  "exploit_framework_canvas": false,
  "exploit_framework_core": false,
  "exploit_framework_d2_elliot": false,
  "exploit_framework_exploitHub": false,
  "exploit_framework_metasploit": false,
  "exploitability_ease": "No known exploits are available",
  "exploited_by_malware": false,
  "exploited_by_nessus": false,
  "family": "Misc.",
  "family_id": 23,
  "has_patch": false,
  "id": 70658,
  "in_the_news": false,
  "name": "SSH Server CBC Mode Ciphers Enabled",
  "modification_date": "2018-07-30T00:00:00Z",
  "publication_date": "2013-10-28T00:00:00Z",
  "risk_factor": "Low",
  "see_also": [
    ""
  ],
  "solution": "Contact the vendor or consult product documentation to disable CBC mode cipher encryption,
and enable CTR or GCM cipher mode encryption.",
  "synopsis": "The SSH server is configured to use Cipher Block Chaining.",
  "type": "remote",
  "unsupported_by_vendor": false,
  "version": "1.4",
  "vuln_publication_date": "2008-11-24T00:00:00Z",
  "xrefs": [
    {
      "type": "CERT",
      "id": "958563"
    },
    {
      "type": "CWE",
      "id": "200"
    }
  ],
  "vpr": {
    "score": 2.5,
    "drivers": {
      "age_of_vuln": {
        "lower_bound": 731
      },
      "exploit_code_maturity": "UNPROVEN",
      "cvss_impact_score_predicted": true,
      "cvss3_impact_score": 2.5,
      "threat_intensity_last28": "VERY_LOW",
      "threat_sources_last28": [
        "No recorded events"
      ],
      "product_coverage": "HIGH"
    },
    "updated": "2020-12-30T05:20:01Z"
  }
}
```

```
    },
    "port": {
      "port": 22,
      "protocol": "TCP",
      "service": "ssh"
    },
    "scan": {
      "completed_at": "2022-11-28T19:16:27.855Z",
      "schedule_uuid": "template-ac0f7c9e-1ee4-4040-a156-72682dc7a9991b8279485af00a75",
      "started_at": "2022-11-28T18:51:49.270Z",
      "uuid": "93b6356d-ba19-42f8-bda9-e1bebe363783"
    },
    "severity": "low",
    "severity_id": 1,
    "severity_default_id": 1,
    "severity_modification_type": "NONE",
    "first_found": "2022-11-28T19:16:27.855Z",
    "last_found": "2022-11-28T19:16:27.855Z",
    "state": "OPEN",
    "indexed": "2022-11-28T19:17:05.003Z"
  }
]
```

## Get Export Job (Supplemental)

The Get Export Job supplemental feed finds a given job by its UUID.

GET <https://cloud.tenable.com/vulns/export/status>

### Sample Response:

```
{
  "exports": [
    {
      "uuid": "8184a7f2-3038-445f-8c77-727551a464d5",
      "status": "FINISHED",
      "total_chunks": 0,
      "chunks_available_count": 0,
      "empty_chunks_count": 0,
      "finished_chunks": 0,
      "filters": {
        "severity": [
          "INFO",
          "LOW",
          "MEDIUM",
          "HIGH",
          "CRITICAL"
        ],
        "state": [
          "OPEN",
          "REOPENED"
        ],
        "tags": {},
        "since": 1669828186,
        "first_found": 0,
        "last_found": 0,
        "last_fixed": 0,
        "first_seen": 0,
        "last_seen": 0,
        "indexed_at": 0
      },
      "num_assets_per_chunk": 500,
      "created": 1669914589334
    }
  ]
}
```

# Average Feed Run



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

METRIC	RESULT
Run Time	1 minute
Assets	6
Asset Attributes	44
Indicators	1
Vulnerabilities	76
Vulnerability Attributes	960

# Change Log

- Version 1.0.0
  - Initial release