

ThreatQuotient



Tenable.sc CDF

Version 1.0.1

November 18, 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 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

ThreatQ Mapping..... 11

 Tenable.sc Vulnerabilities 11

 Get Tenable.sc IP Assets (Supplemental) 16

 Get Tenable.sc CVEs (Supplemental) 19

Average Feed Run..... 21

Known Issues / Limitations 22

Change Log 23

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 © 2024 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

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	1.0.1
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Tenable.SC CDF captures vulnerability data from Tenable.sc and ingests it into the ThreatQ platform. Additionally, users have the option to configure the integration to ingest IP Addresses from Tenable.sc as Assets in ThreatQ and relate them back to the relevant vulnerabilities.

The integration provides the following feeds:

- **Tenable.sc Vulnerabilities** - Collects vulnerabilities from Tenable.sc from a specific historical period.
- **Get Tenable.sc IP Assets (Supplemental)** - Collects IP Addresses Assets from Tenable.sc from a specific historical period.
- **Get Tenable.sc CVEs (Supplemental)** - Collects CVEs from Tenable.sc and ingests them into ThreatQ as Vulnerabilities or Indicators, based on user selection.

The integration ingests the following object types:

- Assets
- Indicators
- Vulnerabilities

Prerequisites

You will need the following to run the integration:

- API access and secret keys for a Tenable.sc account with the privileges to see vulnerability scans.

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 integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the 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. 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
Tenable.sc Host	The hostname or IP address for the Tenable.sc server. The scheme is not required.
API Access Key	The API access key for the user that has privileges to access scan result and vulnerability data.
API Secret Key	The secret key associated with the API access key above.
Enable Capture of Asset Information	Enable this parameter to ingest all the related alerts even if they do not satisfy the previously configured filters.
Severity Selection	Select Minimum Severity for search filters. Options: • Critical • High • Medium • Low • Info
Exploitability	Select whether to search for exploitable in search filters.
Ingest CVEs As	Select the ThreatQ object type to ingest the CVEs into ThreatQ. Options include Indicators and Vulnerabilities (default).

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.



Disabled
Enabled

Uninstall

Additional Information

Integration Type: Feed
Version:

Configuration
Activity Log

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

Data Filtering

☐ Enable Capture of Asset Information
When enabled the feed ingests all the related alerts even if they do not satisfy the previously configured filters.

Severity Selection
Low

Select Minimum Severity for search filters

Exploitability Selection
Both

Select to search for Exploitable in search filters

Ingest CVEs As...
Vulnerabilities

Select the ThreatQ object type to ingest the CVEs into ThreatQ as.

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Tenable.sc Vulnerabilities

The Tenable.sc Vulnerabilities feed collects vulnerabilities from Tenable.sc from a specific historical period.

POST {host}/rest/analysis

Sample Request:

```
{
  "query": {
    "filters": [
      {
        "filterName": "lastSeen",
        "operator": "=",
        "value": "1716460215-1716892215"
      },
      {
        "filterName": "severity",
        "operator": "=",
        "value": "0,1,2,3,4"
      }
    ],
    "tool": "vulndetails",
    "type": "vuln"
  },
  "sourceType": "cumulative",
  "type": "vuln",
  "startOffset": "0",
  "endOffset": "100"
}
```

Sample Response:

```
{
  "type": "regular",
  "response": {
    "totalRecords": "1474560",
    "returnedRecords": 50,
    "startOffset": "0",
    "endOffset": "50",
    "matchingDataElementCount": "-1",
    "results": [
      {
        "pluginID": "145570",
        "severity": {
          "id": "3",

```

```

    "name": "High",
    "description": "High Severity"
  },
  "hasBeenMitigated": "0",
  "acceptRisk": "0",
  "recastRisk": "0",
  "ip": "0.0.137.85",
  "uuid": "11060ddf-bf0c-44a3-a240-09b0fe187433",
  "port": "0",
  "protocol": "TCP",
  "pluginName": "CentOS 8 : sudo (CESA-2021:0218)",
  "firstSeen": "1685505909",
  "lastSeen": "1716537289",
  "exploitAvailable": "Yes",
  "exploitEase": "Exploits are available",
  "exploitFrameworks": "Canvas (CANVAS), Metasploit (Sudo Heap-Based
Buffer Overflow), Core Impact, malware",
  "synopsis": "The remote CentOS host is missing a security update.",
  "description": "The remote CentOS Linux 8 host has a package
installed that is affected by a vulnerability as referenced in the
CESA-2021:0218 advisory.\n\n - sudo: Heap buffer overflow in argument parsing
(CVE-2021-3156)\n\nNote that Nessus has not tested for this issue but has
instead relied only on the application's self-reported version number.",
  "solution": "Update the affected sudo package.",
  "seeAlso": "https://access.redhat.com/errata/RHSA-2021:0218",
  "riskFactor": "High",
  "stigSeverity": "I",
  "vprScore": "9.7",
  "vprContext": "[{"id": "age_of_vuln", "name": "Vulnerability
Age", "type": "string", "value": "730 days +"}, {"id":
"cvssV3_impactScore", "name": "CVSS v3 Impact Score", "type": "number",
"value": 5.9}, {"id": "exploit_code_maturity", "name": "Exploit Code
Maturity", "type": "string", "value": "High"}, {"id":
"product_coverage", "name": "Product Coverage", "type": "string",
"value": "Very High"}, {"id": "threat_intensity_last_28", "name": "Threat
Intensity", "type": "string", "value": "Very Low"}, {"id":
"threat_recency", "name": "Threat Recency", "type": "string", "value":
"No recorded events"}, {"id": "threat_sources_last_28", "name": "Threat
Sources", "type": "string", "value": "Security Research"}]",
  "baseScore": "7.2",
  "temporalScore": "6.3",
  "cvssVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C",
  "cvssV3BaseScore": "7.8",
  "cvssV3TemporalScore": "7.5",
  "cvssV3Vector": "AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C",
  "cpe": "cpe:/o:centos:centos:8<br/>cpe:/o:centos:centos:8-stream<br/>
p-cpe:/a:centos:centos:sudo",
  "vulnPubDate": "1611576000",
  "patchPubDate": "1611662400",
  "pluginPubDate": "1611921600",

```

```

        "pluginModDate": "1674043200",
        "checkType": "local",
        "version": "1.11",
        "cve": "CVE-2021-3156",
        "bid": "",
        "xref": "RHSAs #2021:0218, IAVAs #2021-A-0053, CISA-KNOWN-EXPLOITED
#2022/04/27",
        "seolDate": "-1",
        "pluginText": "<plugin_output>\nRemote package installed :
sudo-1.8.25p1-4.el8\nShould be                               : sudo-1.8.29-6.el8_3.1\n\n</
plugin_output>",
        "dnsName": "",
        "macAddress": "00:00:00:7e:3e:0f",
        "netbiosName": "",
        "operatingSystem": "Linux Kernel 4.18.0-80.11.2.el8_0.x86_64 on
CentOS Linux release 8.0.1905 (Core)",
        "ips": "0.0.137.85",
        "recastRiskRuleComment": "",
        "acceptRiskRuleComment": "",
        "hostUniqueness": "repositoryID,ip,dnsName",
        "hostUUID": "",
        "acrScore": "4.0",
        "keyDrivers": "{\n  \"internet exposure\": \"internal\", \"device
capability\": \"\", \"device type\": \"general_purpose\"",
        "assetExposureScore": "619",
        "vulnUniqueness": "repositoryID,ip,port,protocol,pluginID",
        "vulnUUID": "",
        "uniqueness": "repositoryID,ip,dnsName",
        "family": {
          "id": "18",
          "name": "CentOS Local Security Checks",
          "type": "active"
        },
        "repository": {
          "id": "2",
          "name": "Staged-Large",
          "description": "",
          "dataFormat": "IPv4"
        },
        "pluginInfo": "145570 (0/6) CentOS 8 : sudo (CESA-2021:0218)"
      }
    ],
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1716810557
  }

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.pluginName	Vulnerability Value	N/A	pluginPubDate	CentOS 8 : sudo (CESA-2021:0218)	N/A
.synopsis+.description+.solution	Vulnerability Description	N/A	pluginPubDate	The remote CentOS host is missing a security update....	N/A
.cve	Related Vulnerability/ Related Indicator	N/A	pluginPubDate	CVE-2021-3156	Object type is based on Ingest CVEs As.. selection
.riskFactor	Vulnerability Attribute	Risk Factor	pluginPubDate	High	Updates at ingestion.
.vprScore	Vulnerability Attribute	Vulnerability Priority Rating	pluginPubDate	9.7	Updates at ingestion.
.baseScore	Vulnerability Attribute	CVSS v2 Base Score	pluginPubDate	7.2	Updates at ingestion.
.cvssV3BaseScore	Vulnerability Attribute	CVSS v3 Base Score	pluginPubDate	7.8	Updates at ingestion.
.temporalScore	Vulnerability Attribute	CVSS v2 Temporal Score	pluginPubDate	7.5	Updates at ingestion.
.severity.name	Vulnerability Attribute	Severity	pluginPubDate	High	Updates at ingestion.
.cvssVector	Vulnerability Attribute	CVSS v2 Vector	pluginPubDate	AV:L/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C	N/A
.cvssV3Vector	Vulnerability Attribute	CVSS v3 Vector	pluginPubDate	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	N/A
.firstSeen	Vulnerability Attribute	First Seen	pluginPubDate	1685505909	Timestamp formatted.
.lastSeen	Vulnerability Attribute	Last Seen	pluginPubDate	1716537289	Timestamp formatted.
.pluginModDate	Vulnerability Attribute	Last Modified	pluginPubDate	1674043200	Timestamp formatted.
.pluginInfo	Vulnerability Attribute	Plugin Information	pluginPubDate	145570 (0/6) CentOS 8 : sudo (CESA-2021:0218)	N/A
.pluginID	Vulnerability Attribute	Plugin ID	pluginPubDate	145570	N/A
.family.name	Vulnerability Attribute	Family	pluginPubDate	CentOS Local Security Checks	N/A
.version	Vulnerability Attribute	Version	pluginPubDate	1.11	N/A
.checkType	Vulnerability Attribute	Type	pluginPubDate	local	Updates at ingestion.
.patchPubDate	Vulnerability Attribute	Patch Published Date	pluginPubDate	1611662400	Timestamp formatted. Updates at ingestion.
.exploitAvailable	Vulnerability Attribute	Exploit Available	pluginPubDate	Yes	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.exploitEase	Vulnerability Attribute	Exploitability Ease	pluginPubDate	Exploits are available	N/A
.vulnPubDate	Vulnerability Attribute	Vulnerability Publish Date	pluginPubDate	1611576000	If value is greater than 0. Timestamp formatted. Updates at ingestion.
.cpe	Vulnerability Attribute	CPE	pluginPubDate	1611662400	Timestamp formatted. Updates at ingestion.

Get Tenable.sc IP Assets (Supplemental)

The Get Tenable.sc IP Assets supplemental feed collects IP Address Assets from Tenable.sc from a specific historical period.

GET {host}/rest/analysis

Sample Request:

```
{
  "type": "vuln",
  "sourceType": "cumulative",
  "query": {
    "tool": "vulnipdetail",
    "type": "vuln",
    "filters": [
      {
        "filterName": "lastSeen",
        "operator": "=",
        "value": "1716368655-1716455055"
      }
    ],
    "startOffset": 0,
    "endOffset": 100
  }
}
```

Sample Response:

```
{
  "type": "regular",
  "response": {
    "totalRecords": "1321",
    "returnedRecords": 50,
    "startOffset": "0",
    "endOffset": "50",
    "matchingDataElementCount": "4374",
    "results": [
      {
        "pluginID": "10107",
        "total": "14",
        "severity": {
          "id": "0",
          "name": "Info",
          "description": "Informative"
        },
        "name": "HTTP Server Type and Version",
        "pluginDescription": "This plugin attempts to determine the type and the version of the remote web server.",
        "hosts": [
          {
```

```

    "iplist": [
      {
        "ip": "10.238.64.1",
        "uuid": "",
        "hostUUID": "",
        "macAddress": "00:16:3e:a1:12:f7",
        "netbiosName": "",
        "dnsName": "_gateway.incus",
        "acrScore": "6.0",
        "assetExposureScore": "497"
      }
    ],
    "repository": {
      "id": "1",
      "name": "Live",
      "description": "",
      "dataFormat": "IPv4"
    }
  },
  "family": {
    "id": "11",
    "name": "Web Servers",
    "type": "active"
  }
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1716897653
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Vulnerability Value	N/A	N/A	HTTP Server Type and Version	N/A
.hosts.iplist.ip	Related Asset Value	N/A	N/A	10.238.64.1	N/A
.hosts.iplist.netbiosName	Related Asset Attribute	NetBIOS Name	N/A	N/A	N/A
.hosts.iplist.dnsName	Related Asset Attribute	DNS	N/A	_gateway.incus	N/A
.hosts.iplist.macAddress	Asset Attribute	MAC Address	N/A	00:16:3e:a1:12:f7	N/A

Get Tenable.sc CVEs (Supplemental)

The Get Tenable.sc CVEs supplemental feed collects CVEs from Tenable.sc and ingests them into ThreatQ as Vulnerabilities or Indicators, based on user selection.

GET {host}/rest/analysis

Sample Request:

```
{
  "type": "vuln",
  "sourceType": "cumulative",
  "query": {
    "tool": "cveipdetail",
    "type": "vuln",
    "filters": [
      {
        "filterName": "lastSeen",
        "operator": "=",
        "value": "1211241600-1716336000"
      }
    ],
    "startOffset": 0,
    "endOffset": 100
  }
}
```

Sample Response:

```
{
  "type": "regular",
  "response": {
    "totalRecords": "788",
    "returnedRecords": 788,
    "startOffset": "0",
    "endOffset": "1000",
    "matchingDataElementCount": "788",
    "results": [
      {
        "cveID": "CVE-1999-0524",
        "total": "52",
        "hosts": [
          {
            "repositoryID": "1",
            "iplist": [
              {
                "ip": "10.238.64.1",
                "uuid": "",
                "hostUUID": "",
                "macAddress": "00:16:3e:a1:12:f7",
                "netbiosName": ""
              }
            ]
          }
        ]
      }
    ]
  }
}
```

```

        "dnsName": "_gateway.incus"
      }
    ]
  },
],
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1716894002
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cveID	Vulnerability Value	N/A	N/A	CVE-1999-0524	N/A
.hosts.iplist.ip	Related Asset Value	N/A	N/A	10.238.64.1	N/A
.hosts.iplist.netbiosName	Related Asset Attribute	NetBIOS Name	N/A	N/A	N/A
.hosts.iplist.dnsName	Related Asset Attribute	DNS	N/A	_gateway.incus	N/A
.hosts.iplist.macAddress	Asset Attribute	MAC Address	N/A	00:16:3e:a1:12:f7	N/A

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	2 min
Assets	28
Asset Attributes	57
Indicators	100
Vulnerabilities	114
Vulnerability Attributes	668

Known Issues / Limitations

- The initial run of the feed will retrieve data last discovered today. Because of the way the historical filtering is done, the minimum time interval of the requests is 1 day. ThreatQuotient advises scheduling the feed for a minimum of 24 hours.

Change Log

- **Version 1.0.1**
 - Added two new configuration options:
 - Enable SSL Verification
 - Disable Proxies
- **Version 1.0.0**
 - Initial release