

ThreatQuotient



Broadcom Security Advisories CDF

Version 1.0.0

July 01, 2025

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

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

 Broadcom Security Advisories 10

Average Feed Run..... 12

Known Issues / Limitations 13

Change Log 14

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 © 2025 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	1.0.0
Compatible with ThreatQ Versions	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Broadcom Security Advisories CDF enables analysts to ingest security advisories from the Broadcom website in order to stay up-to-date on software updates and patched vulnerabilities for VMware products.

The integration provides the following feed:

- **Broadcom Security Advisories** - ingests Broadcom Security Advisories.

The integration ingests the following system object types:

- Event
- Incident
- Indicator
- Report
- Vulnerability

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
6. Select the individual feeds to install, when prompted and click **Install**.



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.

The feed(s) 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 **OSINT** 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
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Product Areas	<p>Select which products to fetch security advisories for with the feed.</p> <ul style="list-style-type: none"> ◦ VMware Cloud Foundation (<i>default</i>) ◦ Tanzu ◦ Application Networking and Security (<i>default</i>) ◦ Software Defined Edge (<i>default</i>)
Ingest Advisories As	<p>Select the object type to ingest the security advisories as in the ThreatQ platform. Options include:</p> <ul style="list-style-type: none"> ◦ Reports (<i>default</i>) ◦ Vulnerabilities ◦ Events ◦ Incidents
Severity Filter	<p>Select the advisory severities you want to ingest into ThreatQ. Options include:</p> <ul style="list-style-type: none"> ◦ Low Medium (<i>default</i>)

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ High (<i>default</i>) ◦ Critical (<i>default</i>)
Ingest CVEs as	Select the entity type to ingest CVE IDs as in ThreatQ. Options include: <ul style="list-style-type: none"> ◦ Indicators ◦ Vulnerabilities

[< Broadcom Security Advisories](#)



Disabled
Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed
Version:

Configuration
Activity Log

Connection

- ☒ Enable SSL Certificate Verification
When checked, validates the host-provided SSL certificate.
- ☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Ingestion Options

Product Areas
 Select which products you want to fetch security advisories for.

- ☒ VMware Cloud Foundation
- ☒ Tanzu
- ☒ Application Networking and Security
- ☒ Software Defined Edge

Ingest Advisories As
 Incidents

Select the object type to ingest the security advisories as.

Severity Filter
 Select the advisory severities you want to ingest into ThreatQ.

- ☒ Low
- ☒ Medium
- ☒ High
- ☒ Critical

Ingest CVEs As
 Vulnerabilities

- 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

Broadcom Security Advisories

The Broadcom Security Advisories feed periodically pulls security advisories from the Broadcom website and ingests them into ThreatQ.

GET <https://support.broadcom.com/web/ecx/security-advisory/-/securityadvisory/getSecurityAdvisoryList>

Sample Request Body:

```
{
  "pageNumber": 0,
  "pageSize": 20,
  "searchVal": "",
  "segment": "VC",
  "sortInfo": {
    "column": "",
    "order": ""
  }
}
```

Sample Response:

```
{
  "success": true,
  "data": {
    "list": [
      {
        "documentId": "VCDSA35843",
        "notificationId": 35843,
        "published": "18 June 2025",
        "status": "CLOSED",
        "title": "Product Release Advisory - VMware Tanzu Greenplum 7.5.0",
        "updated": "2025-06-18 23:43:48.549",
        "totalRecords": null,
        "notificationUrl": "https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35843",
        "alertType": "S",
        "severity": "CRITICAL",
        "supportProducts": "VMware Tanzu Data Suite,V...",
        "affectedCve": "CVE-2025-22243, CVE-2025-22244",
        "workAround": ""
      }
    ]
  }
}
```



In addition, the HTML content for each security advisory is also fetched and imported as the description for the Report/Vulnerability/Event/Incident Object. The HTML content is fetched using `.notificationUrl` key.

ThreatQuotient provides the following default mapping for this feed based on each dictionary within the data key in the JSON response and HTML content.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.affectedCve</code>	Indicator/Vulnerability.Value	CVE/Vulnerability	<code>.published</code>	CVE-2025-22243, CVE-2025-22244	Split by a comma. Ingested according to Ingest CVEs As.
<code>{HTML}</code>	Indicator/Vulnerability.Value	CVE/Vulnerability	<code>.published</code>	N/A	Parsed from HTML. Ingested according to Ingest CVEs As.
<code>.title</code>	Report/Vulnerability/Event/Incident.Value	Report/Vulnerability/Event/Incident	<code>.published</code>	Product Release Advisory - VMware Tanzu Greenplum 7.5.0	Ingested according to Ingest Advisories As.
N/A	Report/Vulnerability/Event/Incident.Tag	N/A	N/A	advisory	Static Tag.
<code>.{HTML}</code>	Report/Vulnerability/Event/Incident.Description	N/A	N/A	<HTML content>	N/A
<code>.Severity</code>	Report/Vulnerability/Event/Incident.Attribute, Indicator/Vulnerability.Attribute	Severity	<code>.published</code>	Critical	Title cased. Updatable.
<code>{HTML}</code>	Report/Vulnerability/Event/Incident.Attribute, Indicator/Vulnerability.Attribute	Affected Product	<code>.published</code>	VMware Tanzu Data Suite	Parsed from HTML.
<code>{HTML}</code>	Report/Vulnerability/Event/Incident.Attribute	CVSSv3 Base Score	<code>.published</code>	9.8	Parsed from HTML. Updatable.
<code>.N/A</code>	Report/Vulnerability/Event/Incident.Attribute, Indicator/Vulnerability.Attribute	Affected Vendor	<code>.published</code>	VMware	Static Attribute.
<code>.status</code>	Report/Vulnerability/Event/Incident.Attribute	Status	<code>.published</code>	Closed	Title cased. Updatable.
<code>.documentId</code>	Report/Vulnerability/Event/Incident.Attribute	Notification ID	<code>.published</code>	VCDSA35843	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	1 minute
Reports	12
Report Attributes	48
Indicators	27
Indicator Attributes	81

Known Issues / Limitations

- It is highly recommended to run this integration every 5 days based on the average publication rate for article updates and new content.
- The feed utilizes `since` and `until` dates to avoid reingesting entries that haven't been updated.

Change Log

- Version 1.0.0
 - Initial release