ThreatQuotient

IBM Security Bulletins 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

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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The IBM Security Bulletins CDF enables analysts to automatically ingest bulletins such as vulnerability advisories from IBM's support site, into ThreatQ.

The integration provides the following feeds:

- **IBM Security Bulletins -** pulls security bulletins from IBM.

The integration ingests the following object types:

- 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(s).

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:

IBM Security Bulletin Parameters

PARAMETER	DESCRIPTION
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Ingest CVEs As	Select which entity type to ingest relevant CVEs as: Vulnerabilities (default) or Indicators (Type: CVE).

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

IBM Security Bulletins

This feed periodically pulls security security bulletins from IBM as Report Objects.

`GET https://www.ibm.com/support/pages/securityapp/api/site/datalist`

In addition, the HTML content for each security bulletin is also fetched and imported as the description for the Report Object. The HTML content is fetched using `https://www.ibm.com/support/pages/node/{{.NID}}`.

Sample Response:

```
{
  "isCountNearLimit": false,
  "results": {
    "product_names": [
      {
        "": ""
      },
      {
        "SSYMXC": ""
      },
      {
        "SWG10": "AIX"
      },
      {
        "SG11S": "AIX 7.2 HIPERS, APARs & Fixes"
      },
      {
        "OE609": "AIX-&gt;AIX 7.1"
      },
      {
        "SSNLSG": "Algo Audit & Compliance"
      },
      {
        "SS9TEA": "Algo Credit Administrator"
      }
    ],
    "cve_ids": [
      "CVE-2022-46771",
      "CVE-2022-45421",
      "CVE-2022-45418",
      "CVE-2022-45416",
      "CVE-2022-45412",
      "CVE-2022-45411"
    ],
    "top_records": [
      {
        "nid": "6849101",
        "title": "Multiple vulnerabilities of Mozilla Firefox (less than
Firefox 102.5ESR) have affected Synthetic Playback Agent 8.1.4.0-8.1.4 IF16",
        "field_cve_id": "CVE-2022-45403",
        "field_oc_code": "SSVJUL",
        "field_offering_pid_number": "5725V19",
        "field_product": "IBM Application Performance Management",
        "field_cvss_base_score": "Medium",
        "field_cvss_base_score_color": "sev_medium",
        "field_cvss_desc": "Mozilla Firefox could allow a remote attacker to
obtain sensitive information, caused by a flaw in the Service Workers
component. By persuading a victim to visit a specially-crafted Web site, an
attacker could exploit this vulnerability to determine the presence or length
of a media file, and use this information to launch further attacks against the
affected system",
        "field_reported_date": "2022-11-15",
        "field_pub_date": "2022-12-20",
        "field_x_force_url": "https://exchange.xforce.ibmcloud.com/
vulnerabilities/240123",
        "field_section_id": "240123"
      }
    ],
    "alerts": []
  }
}
```

ThreatQuotient provides the following default mapping for this feed based on each item within the API's response `.data` array.

> The following fields are added to the description for each CVE: `.timeline[].first_exploit_published, .timeline[].most_recent_exploit_published, .counts.exploits, .counts.threat_actors, .counts.ransomware_families, .counts.botnets, .reported_exploitation[].name, .reported_exploitation[].url, .reported_exploitation[].date_added, .exploits[].name, .exploits[].exploit_maturity, .exploits[].exploit_availability, .exploits[].exploit_type, exploits[].date_added`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report.Value	Report	`.field_pub_date`	`Multiple vulnerabilities of Mozilla Firefox (less than Firefox 102.5ESR)...`	N/A
`.{HTML}`	Report.Description	N/A	N/A	`<HTML content>`	N/A
`.field.cve.id`	Indicator/ Vulnerability.Value	CVE/Vulnerability	`.field_pub_date`	`CVE-2022-45412`	Ingested according to `Ingest CVEs As`.
`.field_cvss_desc`	Indicator/ Vulnerability.Description	N/A	N/A	`Mozilla Firefox could allow a remote attacker to obtain sensitive...`	N/A
`.field_x_force_url`	Report/Indicator/ Vulnerability.Attribute	External Reference	`.field_pub_date`	`https://exchange.xforce.ibmcloud.com/vulnerabilities/240123`	N/A
`.field_cvss_base_score`	Report/Indicator/ Vulnerability.Attribute	Severity	`.field_pub_date`	`High`	Updatable
`.field_reported_date`	Report/Indicator/ Vulnerability.Attribute	First Reported	`.field_pub_date`	`2022-11-15`	Updatable
`.field_product`	Report/Indicator/ Vulnerability.Attribute	Affected Product	`.field_pub_date`	`IBM Application Performance Management`	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.

IBM Security Bulletins

METRIC	RESULT
Run Time	1 minute
Reports	7
Report Attributes	33
Indicators	26
Indicator Attributes	104

Known Issues / Limitations

- This feed uses "since" and "until" dates to make sure entries are not re-ingested if they have not been updated. Use the Run Integration button to ingest historical entries from feeds.

Change Log

- **Version 1.0.0**
    - Initial release