ThreatQuotient

A Securonix Company

IBM Security Blogs CDF

Version 1.0.0

March 09, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email:	tq-support@securonix.com
Web:	https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 6.5.0
Support Tier	ThreatQ Supported

Introduction

The IBM Security Blogs CDF enables organizations to automatically ingest security-related blog content from IBM into ThreatQ as report objects, providing analysts with timely insights from IBM’s research and thought leadership. By leveraging the IBM Search API, the integration collects report metadata and supplements it by retrieving and parsing full HTML content from each report URL to enrich report descriptions.

The integration provides the following feeds:

- **IBM Security Blogs -** ingests report metadata from IBM Search API.
    - **IBM Security Blogs Download** (supplemental) **-** fetches each report URL and extracts HTML content for report description.

The integration ingests report and report attributes into the ThreatQ platform.

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
API Host	Enter the IBM API host name. The default is `www-api.ibm.com`.
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.

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 Blogs

The IBM Security Blogs feed pulls blog posts from IBM's blog website and ingests them into ThreatQ as report objects.

`POST https://www-api.ibm.com/search/api/v2`

Sample Response Body:

```
{
  "appId": "thinkhub",
  "scopes": ["thinkhub"],
  "query": {
    "bool": {
      "must": [],
      "filter": [
        {
          "nested": {
            "path": "field_hierarchy_01",
            "query": {
              "term": {
                "field_hierarchy_01.@id": "Cybersecurity"
              }
            }
          }
        }
      ]
    }
  },
  "from": 0,
  "size": 100,
  "sort": [
    { "dcdate": "desc" },
    { "_score": "desc" }
  ],
  "lang": "en",
  "cc": "us",
  "localeSelector": {},
  "_source": [
    "_id",
    "title",
    "url",
    "description",
    "dcdate",
    "field_hierarchy_01",
    "field_hierarchy_02",
    "field_hierarchy_03",
    "field_hierarchy_04",
    "field_keyword_01",
    "field_keyword_09",
    "field_keyword_14",
    "field_text_01"
  ]
}
```

Sample Response:

```
{
  "hits": {
    "total": { "value": 750, "relation": "eq" },
    "hits": [
      {
        "_source": {
          "title": "Cyber Frontlines: Mark Hughes",
          "description": "Learn more about IBM's team of experts...",
          "field_keyword_01": "Threat intelligence",
          "field_keyword_14": "",
          "url": "https://www.ibm.com/think/x-force/cyber-frontlines-mark-hughes",
          "dcdate": "2025-07-28T00:00:00Z"
        }
      }
    ]
  }
}
```

The integration uses each `_source.url` to fetch article page HTML.

```
GET https://www.ibm.com/think/x-force/cyber-frontlines-mark-hughes
```

Sample Response:

```
<div class="table-of-contents container responsivegrid">
  ...
  <div class="cms-richtext" data-dynamic-inner-content="description">
    <p>As new technologies advance, so too do the cybersecurity threats...</p>
  </div>
  <div class="cms-richtext" data-dynamic-inner-content="description">
    <p>In this first edition of Cyber Frontlines, meet Mark Hughes...</p>
  </div>
  ...
</div>
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.hits.hits[]._source.title`	Report value	N/A	`.hits.hits[]._source.dcdate`	`Cyber Frontlines: Mark Hughes`	N/A
`extracted HTML from GET(_source.url)`	Report description	N/A	N/A	`<div class="cms-richtext" ...><p>...</p></div>`	Primary description source
`.hits.hits[]._source.url`	Report attribute	`URL`	`.hits.hits[]._source.dcdate`	`https://www.ibm.com/think/x-force/...`	N/A
`.hits.hits[]._source.field_keyword_01`, `.hits.hits[]._source.field_keyword_14`	Report tags	N/A	N/A	`Threat intelligence`	Empty values removed and values deduplicated
`.hits.hits[]._source.field_keyword_01`, `.hits.hits[]._source.field_keyword_14`	Report attribute	`Tag`	`.hits.hits[]._source.dcdate`	`Threat intelligence`	Same tag values are also mapped as report attributes

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	13
Reports	745
Reports Attributes	1,491

Change Log

- **Version 1.0.0**
  - Initial release