ThreatQuotient

A Securonix Company

Barracuda Research Blog CDF

Version 1.0.0

July 15, 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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Barracuda Research Blog CDF enables analysts to automatically ingest blog posts from the Barracuda blog website allowing them to stay up-to-date on advisories, bulletins, and analyses from the Barracuda team.

The integration provides the following feed:

- **Barracuda Research Blog** - pulls threat intel blog posts from the Barracuda website and ingests them into ThreatQ as report objects.

The integration ingests the following system object types:

- Indicators
- Reports
- Vulnerabilities

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.

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.

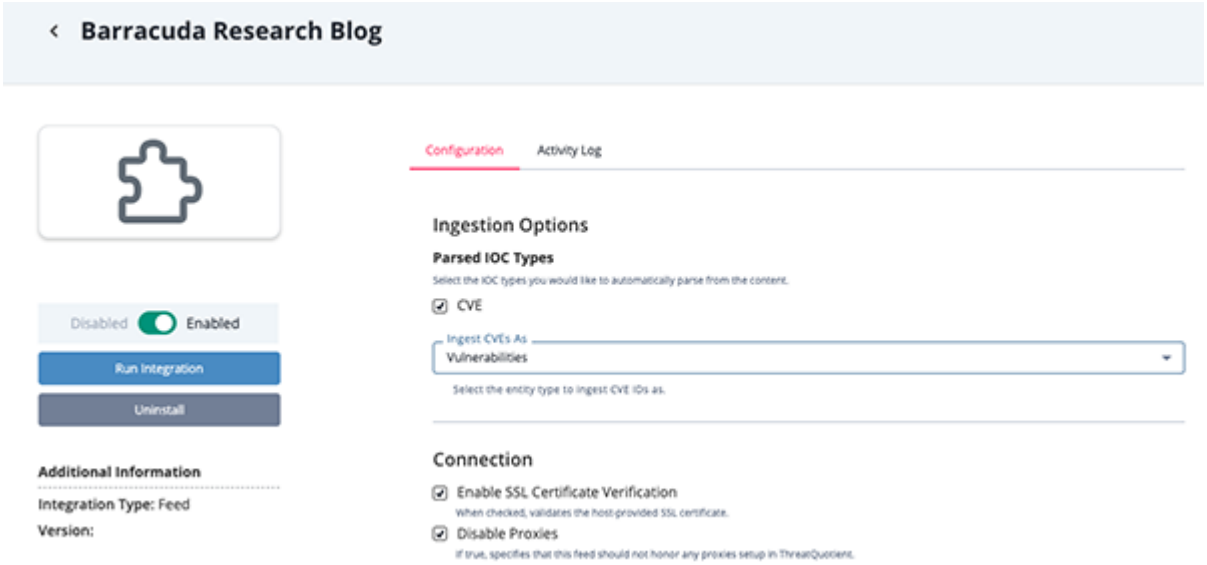
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **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
Parsed IOC Types	Select the IOC types you would like to automatically parse from the content. The only option available at this time is `CVE`.
Ingest CVEs As	Select the entity type to ingest CVE IDs as into the ThreatQ platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators > This parameter is only accessible if the `CVE` option is selected for the **Parsed IOC Types** parameter.
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

Barracuda Research Blog

The Barracuda Research Blog feed pulls threat intel blog posts from the Barracuda website and ingests them into ThreatQ as report objects.

`GET https://blog.barracuda.com/content/barracuda-blog/us/en/category/research/jcr:content/root/container_1/column_control/col_1/blog_list.list.json`

Sample Response:


```
{
  "totalMatches": 111,
  "blogs": [
    {
      "title": " Cybersecurity Threat Advisory: Microsoft Outlook elevation of privilege vulnerability",
      "description": "Microsoft Threat Intelligence discovered a critical EoP vulnerability (CVE-2023-23397) in Microsoft Outlook that allows for NTLM credentials to be stolen. ",
      "image": "/content/dam/barracuda-blog/images/2023/03/Generic_Featured_Datacenter_1200x628.jpg",
      "publicationDate": "Mar 22, 2023, 8:28:24 PM",
      "tags": ["barracuda-blog:categories/research/threat-advisory"],
      "formattedPublicationDate": "March 22, 2023",
      "authorName": "Matthew Russo",
      "link": "https://blog.barracuda.com/articles/2023/03/22/-cybersecurity-threat-advisory--microsoft-outlook-elevation-of-p",
      "authorPageLink": "https://blog.barracuda.com/author/matthew-russo"
    },
    {
      "title": "Cybersecurity Threat Advisory: New phishing campaigns related to recent bank failures ",
      "description": "Cybercriminals have started new phishing campaigns that targets organizations and individuals who were members of affected banks.",
      "image": "/content/dam/barracuda-blog/images/2023/03/Generic_Featured_BuildingTunnelUrban_1200x628.jpg",
      "publicationDate": "Mar 16, 2023, 2:20:04 PM",
      "tags": [
        "barracuda-blog:categories/research/threat-advisory",
        "barracuda-blog:categories/email-protection/phishing-and-impersonation",
        "barracuda-blog:categories/solutions/technologies/ransomware-protection",
        "barracuda-blog:categories/solutions/technologies/13-email-threat-types"
      ],
```

```
      "formattedPublicationDate": "March 16, 2023",
      "authorName": "Anika Jishan",
      "link": "https://blog.barracuda.com/articles/2023/03/16/cybersecurity-
threat-advisory--new-phishing-campaigns-related-to",
      "authorPageLink": "https://blog.barracuda.com/author/anika-jishan"
    }
  ],
  "pagination": {
    "pages": [
      {
        "index": 1
      },
      {
        "index": 2
      }
    ]
  }
}
```


The corresponding blog posts are fetched for each post returned.

`GET https://blog.barracuda.com/articles/{{ uri }}`

> Only blog posts marked as `Threat Research` will be ingested.

ThreatQuotient provides the following default mapping for this feed based on the `.blogs[]` array returned by the API:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report.Title	N/A	`.formattedPublicationDate`	`Cybersecurity Threat Advisory: Microsoft Outlook elevation of privilege vulnerability`	N/A
`{HTML}`	Report.Description	N/A	N/A	N/A	Parsed from the HTML
`.link`	Report.Attribute	External Reference	`.formattedPublicationDate`	`https://blog.barracuda.com/articles/2023/03/22/-cybersecurity-threat-advisory--microsoft-outlook-elevation-of-p`	N/A
`.formattedPublicationDate`	Report.Attribute	Published At	`.formattedPublicationDate`	`March 22, 2023`	N/A
`.tags[]`	Report.Tag	N/A	N/A	`threat-advisory`	The full "tag" is not used, but rather just the final part.
`.authorName`	Report.Attribute	Author	`.formattedPublicationDate`	`Matthew Russo`	N/A
`{HTML}`	Related Indicator/ Vulnerability	CVE/Vulnerability	`.formattedPublicationDate`	`CVE-2023-41232`	Parsed from HTML, Ingested according

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					to `Ingest CVEs As`

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	5
Report Attributes	15
Vulnerability	10

Known Issues / Limitations

- ThreatQuotient recommends running this integration every 7 days based on the publication pace of the Barracuda site.
- The feed utilizes **since** and **until** dates to make sure entries are not re-ingested if they haven't been updated.
- If you need to ingest historical blog posts, run the feed manually by setting the **since** date back.
- The integration can fetch a maximum of 16 of the most recent blog posts.

Change Log

- **Version 1.0.0**
  - Initial release