ThreatQuotient

A Securonix Company

Abnormal Security Threat Intel Blog CDF

Version 1.0.1

June 23, 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	1.0.1
Compatible with ThreatQ Versions	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Abnormal Security Threat Intel Blog CDF enables analysts to ingest the latest security news and research from the Abnormal Security team in the form of advisories, bulletins, and analyses posted on the Abnormal Security blog .

The integration provides the following feed:

- **Abnormal Security Threat Intel Blog** - ingests Abnormal Security Threat Intel blogs as ThreatQ reports and related CVEs.

The integration ingests the following 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:

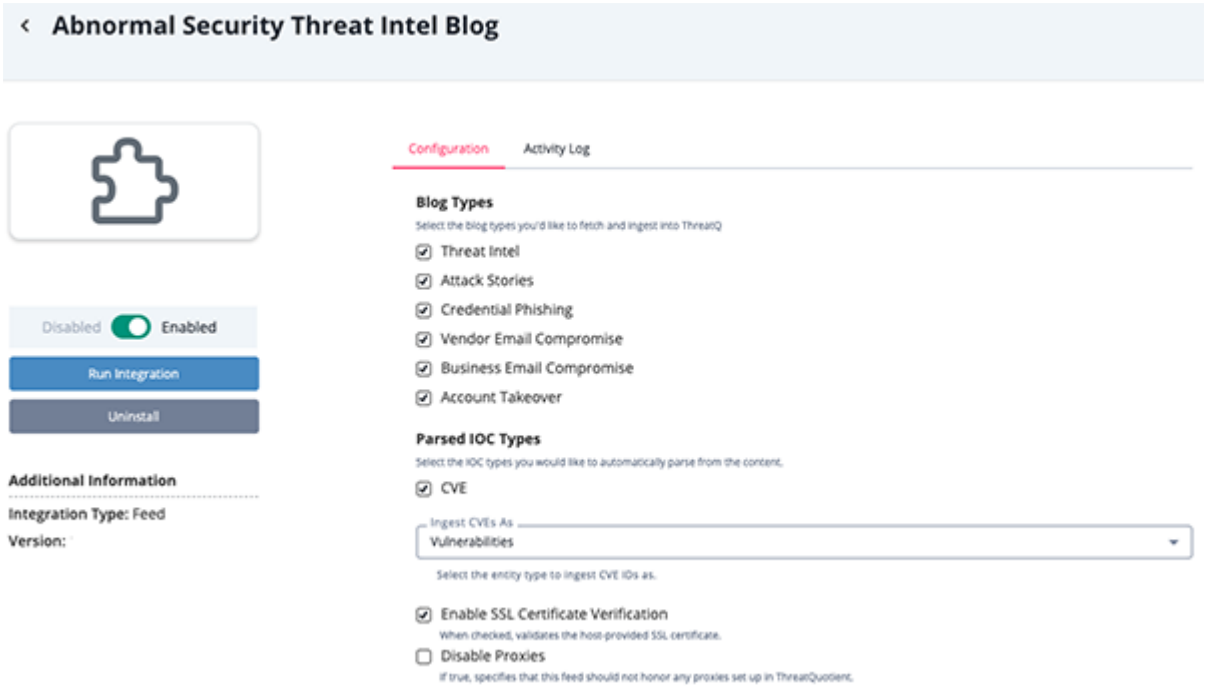
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   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
Blog Types	Select the blog types to fetch and ingest into ThreatQ. Options include: ◦ Threat Intel *(default)* ◦ Attack Stories *(default)* ◦ Credential Phishing *(default)* ◦ Vendor Email Compromise ◦ Business Email Compromise ◦ Account Takeover
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

PARAMETER	DESCRIPTION
	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

Abnormal Security Threat Intel Blog

The Abnormal Security Threat Intel Blog feed pulls blog posts from Abnormal Security's website and ingests them into ThreatQ as report objects.

`GET https://abnormalsecurity.com/blog`

The output of this request is HTML, which is parsed for a build ID that is used to fetch the blog posts.

`GET https://abnormalsecurity.com/_next/data/{{ build_id }}/blog/category/{{ type }}.json`

For each of the posts returned, fetch the corresponding blog post.

`GET https://abnormalsecurity.com/_next/data/{{ build_id }}/blog/{{ uri }}.json`

The detailed blog response returns the post data under the `.pageProps.blogPost` key.

Sample Request (truncated):


```
{
  "pageProps": {
    "navigation": {
      "primaryNavigation": [],
      "primaryCallToActions": [],
      "footerPrimaryNavigation": []
    },
    "pageEntry": {},
    "persistentNav": {},
    "blogPost": {
      "id": "129543",
      "title": "A Deep Dive into Active Ransomware Groups",
      "slug": "deep-dive-active-ransomware-groups",
      "uri": "blog/deep-dive-active-ransomware-groups",
      "url": "https://abnormalsecurity.com/blog/deep-dive-active-
ransomware-groups",
      "sectionHandle": "blog",
      "typeHandle": "default",
```

```
      "image": [
        {
          "title": "B 05 27 22 Active Ransomware Groups",
          "entryThumb": [
            {
              "width": 760,
              "height": 760,
              "url": "https://optimise2.assets-servd.host/.../
B-05.27.22-Active-"
                     "Ransomware-Groups.png"
            }
          ]
        }
      ],
      "postDate": "2022-05-27T10:30:00-07:00",
      "showSummary": true,
      "summary": "Here's an in-depth analysis of the 62 most
prominent ransomware "
                 "groups and their activities since January 2020.",
      ...
    }
  },
  "__N_SSG": true
}
```


ThreatQuotient provides the following default mapping for this feed based on the `.pageProps.blogPost` JSON keys:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	`Report.Title`	`N/A`	`.postDate`	`A Deep Dive into Active Ransomware Groups`	`N/A`
`.contentSections[]`	`Report.Description`	`N/A`	`N/A`	`N/A`	`Items are parsed into HTML`
`.url`	`Report.Attribute`	`External Reference`	`.postDate`	`https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups`	`N/A`
`.postDate`	`Report.Attribute`	`Published At`	`.postDate`	`2022-05-27T10:30:00-07:00`	`N/A`
`.blogCategory[].slug`	`Report.Tag`	`N/A`	`.postDate`	`threat-intel`	`N/A`
`.postAuthors[].title`	`Report.Attribute`	`Author`	`.postDate`	`threat-intel`	`N/A`
`N/A`	`Related Indicator/`	`CVE`	`.postDate`	`CVE-2023-41232`	`User-configurable.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
	Vulnerability				Parsed from HTML

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	3
Report Attributes	9
Vulnerabilities	1

Known Issues / Limitations

- 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 feed will only return at maximum, the most recent 24 posts.
- ThreatQuotient recommends running this integration every 7 days based on the publication pace of the site.

Change Log

- Version 1.0.1
  - Updated the feed to support the latest Abnormal Security Blog API structure.
  - Updated the build ID discovery source to `https://abnormal.ai/blog`.
  - Modified blog listing parsing to use the `blogPosts` object in place of `posts`.
  - Modified blog detail parsing to use the `blogPost` object in place of `post`.
  - Enhanced blog content parsing with additional validation and error-handling mechanisms to improve reliability and resilience.
- **Version 1.0.0**
  - Initial release