ThreatQuotient

A Securonix Company

Gen Digital Blog CDF

Version 1.0.0

June 15, 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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Gen Digital Blog integration enables ThreatQ users to ingest cybersecurity research, threat intelligence insights, and security-focused articles published through the Gen Digital Insights RSS feed. The integration periodically retrieves new RSS entries and ingests them as ThreatQ Report objects. To provide additional context for analysis, each report is enriched by retrieving the associated article content and incorporating it into the report description.

By centralizing Gen Digital research within ThreatQ, analysts can efficiently monitor emerging threats, industry trends, and security developments without leaving their threat intelligence workflow.

The integration provides the following feed:

- **Gen Digital Blog Insights** - retrieves posts from the Gen Digital Insights RSS feed and ingests them as enriched ThreatQ Report objects.

The integration ingests Report and Report Attribute type system objects.

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.

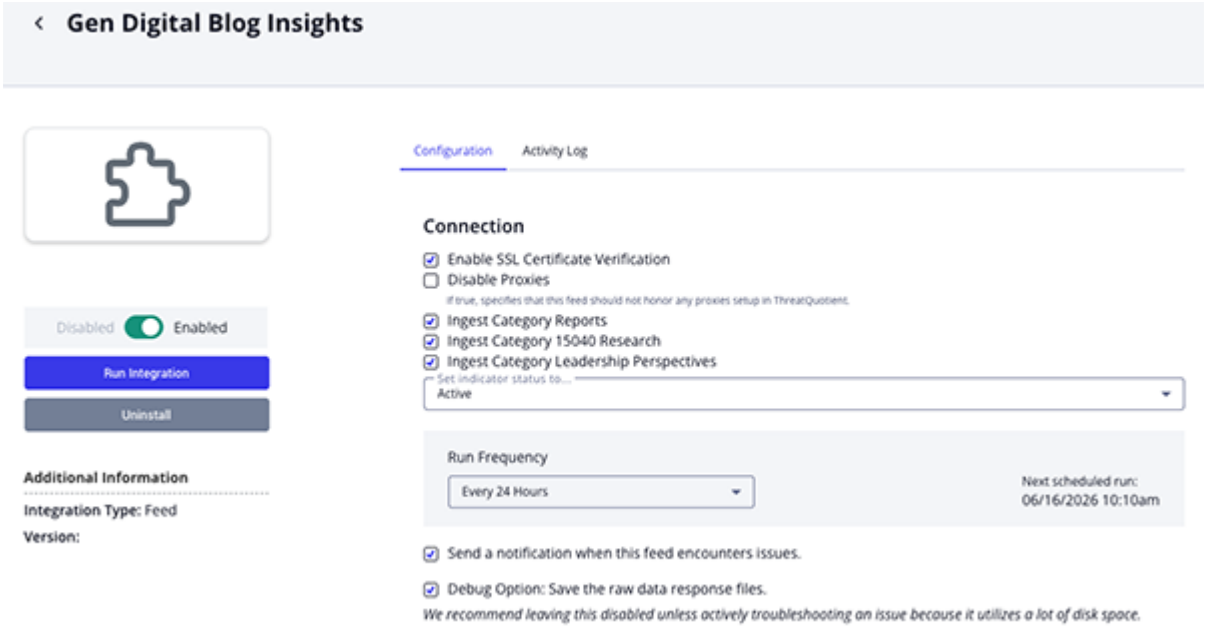
To configure the integration:

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
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.
Ingest Category Reports	Enable this parameter to ingest RSS items from the Reports category.
Ingest Category Research	Enable this parameter to ingest RSS items from the Research category.
Ingest Category Leadership Perspectives	Enable this parameter to ingest RSS items from the Leadership Perspectives category.



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

Gen Digital Blog Insights

The Gen Digital Blog Insights feed retrieves blog posts directly from the Gen Digital Insights RSS feed and ingests them as ThreatQ Report objects. Each report is enriched by retrieving the associated article content from the RSS item link, providing analysts with additional context and visibility into the published research.

The feed can be configured to request one or more RSS categories:

```
GET https://www.gendigital.com/blog/rss/v1/blogs/rss.xml/
15299,15040,15041
```

CATEGORY	RSS ID
Reports	`15299`
Research	`15040`
Leadership Perspectives	`15041`

Sample Response:

```
{
  "title": "Inside the JDownloader Supply-Chain Attack: An r77
Rootkit Bot That Kills Your Antivirus",
  "subtitle": "Malware that hid itself on infected systems and
disabled antivirus protection.",
  "createdYmd": "2026-05-11",
  "timeToRead": "20",
  "authors": [
    {
      "displayName": "Threat Research Team"
    }
  ],
  "paragraphs": [
    {
      "bundle": "rich_text",
      "content": "
```

```
  Attackers replaced selected official download links...
" } ] }
```

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	`Report.Value`	`N/A`	`N/A`	`When Hotel Scams Know Your Booking: 350 Compromised Accommodations Across 50 Countries`	`Article page title .`
`.link`	`Report.Attribute`	`Source URL`	`N/A`	`https://www.gendigital.com/blog/insights/research/reservation-hijack-scams-target-travelers`	`Used to fetch the full article content and stored as the report source URL.`
`.guid`	`Report.Attribute`	`GUID`	`N/A`	`https://www.gendigital.com/blog/insights/research/reservation-hijack-scams-target-travelers`	`RSS GUID is used when available; otherwise the source URL is used.`
`.pubDate`	`Report.Attribute`	`Blog Published Date`	`published_date`	`2026-05-28`	`RSS publication date is converted to YYYY-MM-DD.`
`.dc:creator, .authors[].displayName`	`Report.Attribute`	`Author`	`N/A`	`Luis Corrons, Martin Chlumecký`	`Article page authors are preferred; RSS creator is used as fallback.`
`.description`	`Report.Description`	`N/A`	`N/A`	`After our first report, Booking.com began warning customers...`	`Included as the RSS summary and fallback when article content is unavailable.`
`.paragraphs[].content`	`Report.Description`	`N/A`	`N/A`	`N/A`	`Article paragraphs are fetched from the source URL and rendered into the report description.`
`.timeToRead`	`Report.Description`	`N/A`	`N/A`	`20`	`Included in the report description when available.`

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	2 minutes
Reports	10
Report Attributes	40

Known Issues / Limitations

- The Gen Digital RSS endpoint returns a maximum of 10 reports, even when all three categories are selected.

Change Log

- **Version 1.0.0**
  - Initial release