ThreatQuotient

A Securonix Company

G Data Blog CDF

Version 1.0.0

August 29, 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 G Data Blog CDF enables analysts to automatically ingest blog posts from the G Data Blog, https://www.gdatasoftware.com/blog/, providing timely access to advisories, bulletins, and in-depth analyses published by the G Data team. By automating this process, analysts can ensure they remain informed of the latest security updates and research without manual effort.

The integration provides the following feed:

- **G Data Blog** - pulls threat intel blog posts from the G Data blog website as Report objects.

The integration ingests the following system object types:

- Attack Patterns
- Indicators (CVE)
- Reports
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns ingested by the G Data Blog feed to be related correctly. MITRE ATT&CK attack patterns are ingested from the following feeds:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE ICS ATT&CK

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:

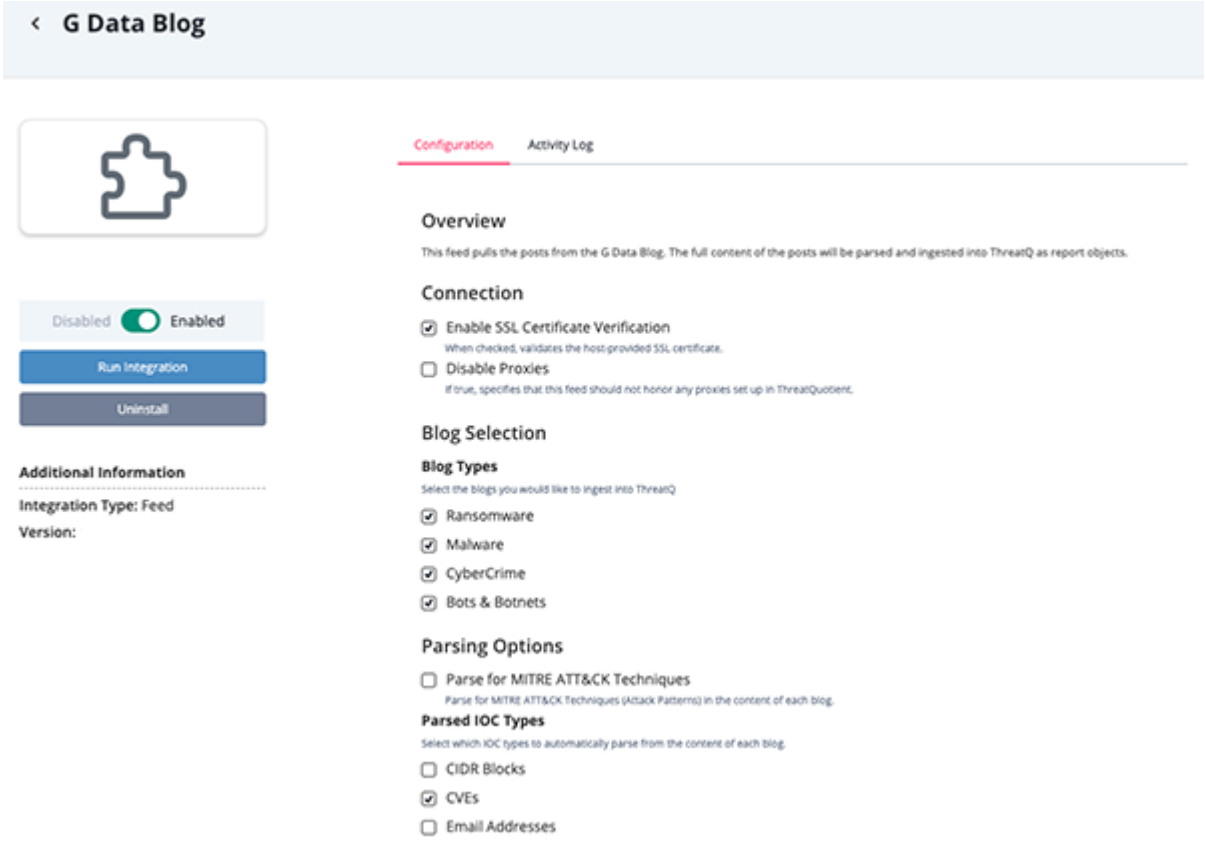
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   > 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.
Blog Types	Select the blog types to ingest into ThreatQ. Options include: ◦ Ransomware *(default)* ◦ Malware *(default)* ◦ CyberCrime *(default)* ◦ Bots & Botnets *(default)*
Parse for MITRE ATT&CK Techniques	Enable this parameter to parse for MITRE ATT&CK Techniques (Attack Patterns) in the content of each blog. This parameter is enabled by default.
Parsed IOC Types	Select the IOC types you would like to automatically parse from the content. Options include: ◦ CIDR Blocks ◦ CVEs *(default)* ◦ MD5 ◦ SHA-1

PARAMETER	DESCRIPTION
	◦ Email Addresses ◦ Filenames ◦ File Paths ◦ FQDNs ◦ IP Addresses ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 ◦ URLs
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.



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

G Data Blog

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

```
GET https://www.gdatasoftware.com/blog/{{ blog type }}
```

This request returns HTML. The HTML is parsed for the title, author, date, links, etc. The blog itself is then fetched.

```
GET https://www.gdatasoftware.com/blog/{{ uri }}
```

ThreatQuotient provides the following default mapping for this feed based on the information parsed out of the blog's HTML content.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Title	Report	Parsed from html	`Verdict-as-a-Service moves malware scanning from the endpoint to the cloud`	Parsed from the HTML
N/A	Report.Description	N/A	Parsed from html	N/A	Parsed from the HTML
N/A	Report.Attribute	External Reference	Parsed from html	`https://www.gdatasoftware.com/blog/2023/03/37714-verdict-as-a-service-moves-malware-scanning-from-the-endpoint-to-the-cloud`	Parsed from HTML
N/A	Report.Attribute	Published At	Parsed from html	`03/03/2023`	Parsed from the HTML
N/A	Report.Tag	N/A	Parsed from html	`Malware`	User-configurable.Parsed from the HTML. Reports are filtered by user selected categories.
N/A	Report.Attribute	Author	Parsed from html	`Kathrin Beckert-Plewka`	Parsed from the HTML
N/A	Report.Indicator/ Report Vulnerability	CVE	Parsed from html	`CVE-2023-41232`	User-configurable.Parsed from HTML
N/A	Report.Indicator	See `Parsed IOC Types` user field	Parsed from html	N/A	User-configurable.Parsed from HTML, based on user selection in `Parsed IOC Types`
N/A	Report.Attack Pattern	Attack Pattern	Parsed from html	N/A	User-configurable.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	5
Report Attributes	15

Known Issues / Limitations

- ThreatQuotient recommends running this integration monthly based on the publication pace of the G Data 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.

Change Log

- **Version 1.0.0**
  - Initial release