

ThreatQuotient

A Securonix Company



Bitdefender Labs Blog CDF

Version 1.0.0

August 12, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

 Bitdefender Labs Blog..... 10

Average Feed Run..... 13

Known Issues / Limitations 14

Change Log 15

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.

Copyright © 2025 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Bitdefender Labs Blog CDF enables security analysts to automatically ingest the latest threat intelligence articles directly from the Bitdefender Labs Blog into ThreatQ. By pulling advisories, bulletins, and in-depth analyses, it ensures teams remain informed about emerging cyber threats, newly discovered vulnerabilities, and available defensive tools.

The integration provides the following feed:

- **Bitdefender Labs Blog** - ingests blog posts from the Bitdefender blog website.

The integration ingests the following system object types:

- Indicator
- Report
- Vulnerability

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
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.
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: <ul style="list-style-type: none"> ◦ Vulnerabilities (<i>default</i>) ◦ Indicators <div>  This parameter is only accessible if the CVE option is selected for the Parsed IOC Types parameter. </div>

< Bitdefender Labs Blog



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.0

Configuration Activity Log

Connection

- ☒ Enable SSL Certificate Verification
When checked, validates the host-provided SSL certificate.
- ☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Ingestion Options

Parsed IOC Types

Select the IOC types you would like to automatically parse from the content.

- ☒ CVE

Ingest CVEs As _____
Indicators (Type: CVE)

Select the entity type to ingest CVE IDs as.

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

Bitdefender Labs Blog

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

GET <https://www.bitdefender.com/nuxt/api/get/en/labs/posts>

Sample JSON Response:

```
{
  "posts": [
    {
      "id": "63fcc772c645650631a4767a",
      "title": "Bitdefender Releases Decryptor for MortalKombat Ransomware",
      "slug": "bitdefender-releases-decryptor-for-mortalcombat-ransomware",
      "feature_image": "https://blogapp.bitdefender.com/labs/content/images/2023/02/decryptors.jpeg",
      "featured": true,
      "published_at": "2023-02-28T17:00:00.000+03:00",
      "html": "<p>A new decryptor for the MortalKombat ransomware is now available for download.<br>Bitdefender has been monitoring the MortalKombat ransomware family since it....",
      "authors": [
        {
          "id": "5f9c907adc5c7f0d91e240aa",
          "name": "Bitdefender",
          "slug": "bitdefenderteam",
          "profile_image": "https://blogapp.bitdefender.com/labs/content/images/2022/02/logo_bd_social.png",
          "cover_image": null,
          "bio": "The meaning of Bitdefenderâ€™s mascot, the Dacian Draco, a symbol that depicts a mythical animal with a wolfâ€™s head and a dragonâ€™s body, is â€œto watchâ€ and to â€œguard with a sharp eye.â€",
          "website": null,
          "location": null,
          "facebook": null,
          "twitter": null,
          "meta_title": null,
          "meta_description": null
        }
      ],
      "tags": [
        {
          "id": "60a41bee97ab4752cdb55530",
          "name": "EN",
          "slug": "en",
```

```

        "description": null,
        "feature_image": null,
        "visibility": "public",
        "og_image": null,
        "og_title": null,
        "og_description": null,
        "twitter_image": null,
        "twitter_title": null,
        "twitter_description": null,
        "meta_title": null,
        "meta_description": null,
        "codeinjection_head": null,
        "codeinjection_foot": null,
        "canonical_url": null,
        "accent_color": null
    },
    {
        "id": "60a41bee97ab4752cdb55531",
        "name": "Free Tools",
        "slug": "free-tools",
        "description": null,
        "feature_image": null,
        "visibility": "public",
        "og_image": null,
        "og_title": null,
        "og_description": null,
        "twitter_image": null,
        "twitter_title": null,
        "twitter_description": null,
        "meta_title": null,
        "meta_description": null,
        "codeinjection_head": null,
        "codeinjection_foot": null,
        "canonical_url": null,
        "accent_color": null
    }
],
    "excerpt": "A new decryptor for the MortalKombat ransomware is now
available for download.\nBitdefender has been monitoring the MortalKombat
ransomware family since it..."
}
],
    "meta": {
        "pagination": {
            "page": 1,
            "limit": 50,
            "pages": 6,
            "total": 267,
            "next": 2,
            "prev": null
        }
    }
}

```

```
}
}
}
```

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
<code>.title</code>	Report.Title	Report	<code>.published_at</code>	Bitdefender Releases Decryptor for MortalKombat Ransomware	N/A
<code>.html</code>	Report.Description	N/A	N/A	<p>A new decryptor for the MortalKombat ransomware...	N/A
<code>.slug</code>	Report.Attribute	External Reference	<code>.published_at</code>	https://www.bitdefender.com/blog/labs/bitdefender-releases-decryptor-for-mortalkombat-ransomware	Formatted into the URL
<code>.published_at</code>	Report.Attribute	Published At	<code>.published_at</code>	2023-02-22 14:00:00.000+00:00	Converted to GMT.
<code>.authors[].name</code>	Report.Attribute	Author	<code>.published_at</code>	Dăvid ACS	N/A
<code>.tags[].slug</code>	Report.Tag	N/A	N/A	antimalware-research	If <code>.visibility</code> is public and length > 2 characters
N/A	Indicator/Vulnerability.Value	CVE/Vulnerability	N/A	CVE-2023-41232	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	16
Indicators	2

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 6 pages of data.
- ThreatQuotient recommends running this integration every 2 days based on the publication pace of the site.

Change Log

- Version 1.0.0
 - Initial release