

ThreatQuotient



The Hacker News CDF

Version 1.0.0

July 22, 2024

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

 The Hacker News 10

Average Feed Run..... 11

Known Issues / Limitations 12

Change Log 13

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 © 2024 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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The The Hacker News CDF enables analysts to automatically ingest posts from the "The Hacker News" blog. This allows analysts to stay up-to-date on data breaches, vulnerabilities, and cyber-attacks via the published articles.

The integration provides the following feed:

- **The Hacker News** - ingests posts from the Hacker news blog in the form of reports.

The integration ingests report and report attribute type 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
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
Post Categories	Select the categories of posts to pull from. Options include: ◦ Data Breaches (default) ◦ Cyber Attacks (default) ◦ Vulnerabilities (default)
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

< The Hacker News



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration **Activity Log**

Overview

This feed pulls posts from The Hacker News blog. Just note, this feed will only pull the latest page of posts for each category.

Post Categories

Select the categories of posts you would like to pull.

☒ Data Breaches

☒ Cyber Attacks

☒ Vulnerabilities

☒ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

☐ Enable SSL Verification

Set indicator status to...

Review

Run Frequency

Every 24 Hours

Next scheduled run:
07/23/2024 11:48am

☒ Send a notification when this feed encounters issues.

☒ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

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

The Hacker News

The Hacker News CDF periodically pulls threat research posts from the The Hacker News blog, and ingests them into ThreatQ as Report Objects.

GET `https://thehackernews.com/{{ category }}`

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

GET `https://thehackernews.com/{{ uri }}`

The mapping for this feed is 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.Value	N/A	N/A	Iranian Hackers Deploy New BugSleep Backdoor in Middle East Cyber Attacks	Parsed from HTML
N/A	Report.Description	N/A	N/A	N/A	Parsed from HTML
N/A	Report.Description	N/A	N/A	<code>https://thehackernews.com/2024/07/iranian-hackers-deploy-new-bugsleep.html</code>	Parsed from HTML
N/A	Report.Tag	N/A	N/A	Vulnerability	Parsed from HTML
N/A	Report.Attribute	Published At	N/A	Jul 17, 2024	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	10

Known Issues / Limitations

- The feed utilizes `since` and `until` dates to ensure entries are not re-ingested if they haven't been updated.
- If you nrrf to ingest historical blog posts, run the feed manually by setting the `since` date back.
- This feed will only pull at maximum, the latest page of blog posts for each category.

Change Log

- Version 1.0.0
 - Initial release