

# ThreatQuotient



## Board Cybersecurity CDF

Version 1.0.0

June 03, 2024

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://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..... 9

    Board Cybersecurity Incident Tracker ..... 9

Average Feed Run..... 10

Known Issues / Limitations ..... 11

Change Log ..... 12

# 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](mailto: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	>= 5.18.0
Support Tier	ThreatQ Supported

# Introduction

The Board Cybersecurity CDF enables analysts to automatically ingest incidents from Board Cybersecurity's Incident Tracker. Ingested incidents will be brought into ThreatQ as Report objects, and will include the affected company, disclosure date, and full content of the incident.

The integration provides the following feed:

- **Board Cybersecurity Incident Tracker** - pulls incidents from the Board Cybersecurity Incident Tracker.

The integration ingests Report type objects into the ThreatQ platform.

# 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.

6. 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. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.



# ThreatQ Mapping

## Board Cybersecurity Incident Tracker

The Board Cybersecurity Incident Tracker feed periodically pulls incidents from the Board Cybersecurity Incident Tracker.

GET <https://www.board-cybersecurity.com/incidents/tracker/>

This request returns HTML, which is parsed for the data, links etc. The post itself is then fetched:

GET <https://www.board-cybersecurity.com/incidents/tracker/{{ uri }}>

ThreatQuotient provides the following default mapping for the information parsed from the post's HTML content:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Value	N/A	Last Update	2024-03-12 MARINEMAX INC Cybersecurity Incident	Parsed from the HTML
N/A	Report.Description	N/A	N/A	N/A	Parsed from the HTML
N/A	Report.Attribute	External Reference	Last Update	<a href="https://www.board-cybersecurity.com/incidents/tracker/20240312-marinemax-inc-cybersecurity-incident/">https://www.board-cybersecurity.com/incidents/tracker/20240312-marinemax-inc-cybersecurity-incident/</a>	Parsed from the HTML
N/A	Report.Attribute	Disclosed At	Last Update	2024-03-12	Parsed from the HTML. Updated at ingestion
N/A	Report.Attribute	Affected Company	Last Update	MARINEMAX INC	Parsed from the 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	8
Report Attributes	24

---

## 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.

# Change Log

- Version 1.0.0
  - Initial release