ThreatQuotient

A Securonix Company

Recorded Future Threat Research CDF

Version 1.0.0

January 26, 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.

Copyright © 2026 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: 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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Recorded Future Threat Research CDF integration enables analysts to ingest the latest research published by the Recorded Future Insikt Group into ThreatQ as Report objects. These reports provide in-depth analysis of cybersecurity trends, threat actors, and emerging risks, delivering actionable intelligence to support proactive threat detection and informed decision-making.

The integration provides the following feed:

- **Recorded Future Threat Research** - fetches intelligence reports from Recorded Future's Threat Research team, Insikt.

The integration ingests report and report attribute 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.

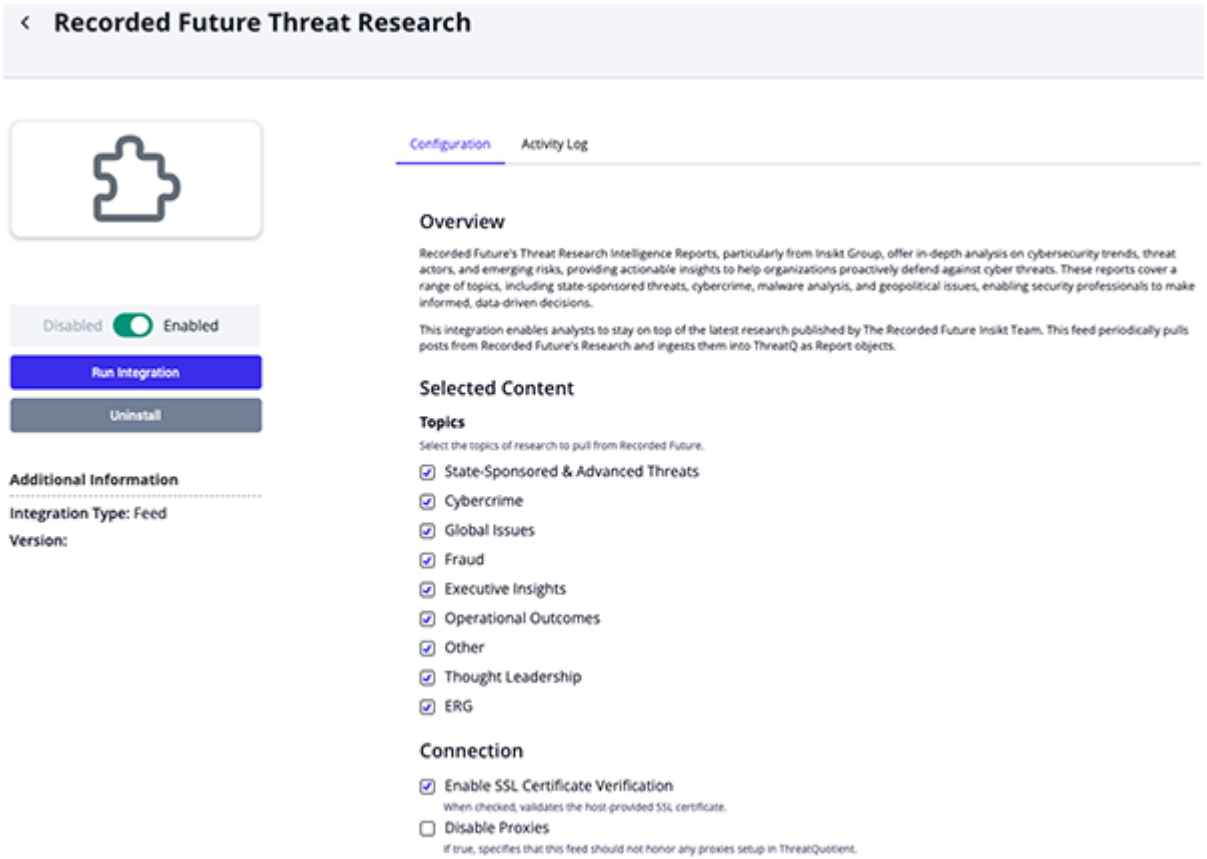
To configure the integration:

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
Topics	Select the categories of blog/news posts to pull from Recorded Future. Options include: ◦ State-Sponsored & Advanced Threats *(default)* ◦ Cybercrime *(default)* ◦ Global Issues *(default)* ◦ Fraud *(default)* ◦ Executive Insights *(default)* ◦ Operational Outcomes *(default)* ◦ Other ◦ Thought Leadership ◦ ERG *(default)*
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.



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

Recorded Future Threat Research

The Recorded Future Threat Research feed pulls posts from Recorded Future's Research and ingests them into ThreatQ as Report objects.

`GET https://www.recordedfuture.com/placeholders.json`

This request returns JSON data, which is used in the next request to pull the articles (index, App ID, API Key).

`GET https://an767qem3v-dsn.algolia.net/1/indexes/{INDEX}/query?x-algolia-api-key={API_KEY}&x-algolia-application-id={APP_ID}`

This request returns JSON data, which is parsed for tags, author, and the link to the underlying article. The full article content is then fetched.

Sample Response:


```
{
  "exhaustive": {
    "nbHits": true,
    "typo": true
  },
  "exhaustiveNbHits": true,
  "exhaustiveTypo": true,
  "hits": [
    {
      "altTitle": "",
      "author": [
        "Insikt Group\u00ae"
      ],
      "category": "",
      "countryTags": [
        "Russia"
      ],
      "date": 1767798016,
      "excerpt": "Insikt Group reveals how GRU-linked BlueDelta evolved credential-harvesting
campaigns targeting government, energy, and research organizations across Europe and Eurasia.",
      "image": "/research/media_13adafe204e74a6a3976247e1c12b0466f536b86e.gif?
width=1200&format=pjpg&optimize=medium",
      "industryTags": [
        "Software & Services"
      ],
      "lastModified": 1767737796,
      "objectID": "8cf135a5-0ddb-56cb-851e-c2da0944feca",
      "pillTag": "",
      "productTags": [
        "Malware Intelligence"
      ],
      "publishedDate": 1767744000,
      "resourceBlock": true,
      "resourceBlockTitle": "Related",
      "resourceType": "research",
      "sidebar": "",
      "slug": "/research/gru-linked-bluedelta-evolves-credential-harvesting",
      "source": "gdoc",
```

```
      "threatTags": [
        "Nation-State Attacks"
      ],
      "title": "GRU-Linked BlueDelta Evolves Credential Harvesting",
      "topicTags": [
        "State-Sponsored & Advanced Threats"
      ]
    }
  ],
  "hitsPerPage": 24,
  "nbHits": 278,
  "nbPages": 12,
  "page": 0,
  "params": "hitsPerPage=24&page=0&filters=resourceType%3Aresearch&facetFilters=%5B%5D",
  "processingTimeMS": 1,
  "processingTimingsMS": {
    "_request": {
      "roundTrip": 114
    },
    "total": 0
  },
  "query": "",
  "renderingContent": {},
  "serverTimeMS": 1
}
```


`GET https://recordedfuture.com/{SLUG}`

The mapping for this feed is based on the `.hits[]` array in the JSON data, as well as information parsed out of the article's HTML content.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report.Title	N/A	`.publishedAt`	`GRU-Linked BlueDelta Evolves Credential Harvesting`	N/A
N/A	Report.Description	N/A	N/A	N/A	Parsed from the HTML
`.publishedDate`	Report.Attribute	Published At	`.publishedAt`	`January 07, 2026`	Converted to human-readable format.
`.lastModified`	Report.Attribute	Updated At	`.publishedAt`	`January 07, 2026`	Updatable. Converted to human-readable format.
`.countryTags[]`	Report.Tag	N/A	N/A	`Russia`	N/A
`.countryTags[]`	Report.Attribute	Country	`.publishedAt`	`Russia`	N/A
`.industryTags[]`	Report.Tag	N/A	N/A	`Software & Services`	N/A
`.industryTags[]`	Report.Attribute	Industry	`.publishedAt`	`Software & Services`	N/A
`.productTags[]`	Report.Tag	N/A	N/A	`Malware Intelligence`	N/A
`.productTags[]`	Report.Attribute	Product	`.publishedAt`	`Malware Intelligence`	N/A
`.threatTags[]`	Report.Tag	N/A	N/A	`Nation-State Attacks`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.threatTags[]`	Report.Attribute	Threat	`.publishedAt`	`Nation-State Attacks`	N/A
`.topicTags[]`	Report.Tag	N/A	N/A	`State-Sponsored & Advanced Threats`	N/A
`.topicTags[]`	Report.Attribute	Topic	`.publishedAt`	`State-Sponsored & Advanced Threats`	N/A
`.author`	Report.Attribute	Author	`.publishedAt`	`Insikt Group`	N/A
`.resourceType`	Report.Attribute	Type	`.publishedAt`	`Research`	N/A

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	14
Report Attributes	83

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