ThreatQuotient

A Securonix Company

RansomLook CDF

Version 1.0.0

July 20, 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.

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	>= 6.5.0
Support Tier	ThreatQ Supported

Introduction

The RansomLook CDF integration enables ThreatQ to ingest ransomware victim intelligence from the RansomLook API. The integration creates Event objects for reported incidents and automatically associates related Identity and Adversary objects, providing analysts with timely visibility into ransomware activity and the threat groups responsible.

The integration provides the following feed:

- **RansomLook Victims** - retrieves recently reported ransomware victim intelligence from the RansomLook API and ingests related events, victims, and associated ransomware groups into ThreatQ.

The integration ingests the following system objects:

- Adversaries
- Event Attributes
- Events
- Identities
- Identity Attributes

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(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
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Ingest Victims As	Choose how victim names are ingested into ThreatQ. Options include: ◦ **Identities** *(default)* - ingests victims as STIX-aligned Identity objects, allowing additional context to be stored and managed within the associated Identity profile. ◦ **Attributes** - ingests victim names as attributes, making them available for use in attribute-based dashboard widgets. When this option is used, related victim context is stored in the description of the corresponding ransomware activity Event.

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

RansomLook Victims

The RansomLook Victims feed retrieves recently reported ransomware victim intelligence from the RansomLook API and ingests related events, victims, and associated ransomware groups into ThreatQ.

```
GET https://www.ransomlook.io/api/posts/period/{{ start }}/{{ end }}
```

Sample Response:


```
[
  {
    "post_title": "Techmar",
    "discovered": "2026-05-26 18:36:46.571699",
    "description": "techmar.com https://www.zoominfo.com/c/techmar-
inc/37699777 is a Dutch company specializing in 12 Volt outdoor
lighting solutions since 2002. Headquartered in Hengelo, Netherlands,
it designs, produces, and supplies lighting fixtures
globally.Products serve gardens, landscapes, and commercial
applications with a focus on quality and innovation.The brand
emphasizes in-house development, sustainability, and reliable low-
voltage technology",
    "link": null,
    "magnet": null,
    "screen": null,
    "group_name": "the gentlemen"
  },
  {
    "post_title": "Mayelia Automotive",
    "discovered": "2026-05-26 17:16:01.171191",
    "description": "mayelia.com zoominfo.com/c/mayelia-automotive/
480899337 is an Ivorian automotive company specializing in vehicle
technical inspections.Founded in 2019, it operates under Mayelia
Participations holding across multiple African sectors.Services
include technical checks, stickers, and corporate solutions for
drivers and businesses.The company emphasizes customer service,
modern equipment, and road safety education",
    "link": null,
    "magnet": null,
    "screen": null,
```

```
    "group_name": "the gentlemen"
  },
  {
    "post_title": "ctps.tp.edu.tw",
    "discovered": "2026-05-26 16:50:10.184074",
    "description": "ctps.tp.edu.tw – Taiwanese Public Elementary
School\n\nctps.tp.edu.tw is the official website of 臺北市南港區成...",
    "link": "/blog/
b4a7f8a258b93ba3de493134d47355ffb5b1247dc32f06d17d036c2fab17c457/",
    "magnet": null,
    "screen": "screenshots/krybit/ctpstpedutw.png",
    "group_name": "krybit"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.post_title, .group_name	Event Title	Ransomware Victim	.discovered	Victim: Acme | Group: the gentlemen	N/A
.post_title	Event Attribute	Victim	.discovered	Acme	If ingesting victims as attributes
.discovered	Event Attribute	Discovered Date	.discovered	March 26, 2026	Formatted into a more human-readable date.
.description, .screen, .link	Event Description	N/A	N/A	N/A	Concatenated into a rich text description.
.post_title	Identity Value	N/A	.discovered	Acme	If ingesting victims as Identity objects
N/A	Identity Attribute	Identity Class	.discovered	organization	Added to align with STIX 2.x data model.
.group_name	Adversary Name	N/A	.discovered	the gentlemen	N/A
N/A	Identity Tag	N/A	N/A	ransomware-victim	Added to all identities reported by this feed

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
Events	12
Event Attributes	12
Identities	12
Identity Attributes	12

Change Log

- **Version 1.0.0**
  - Initial release