

ThreatQuotient

A Securonix Company



Flashpoint Adversary Forum CDF

Version 1.0.0

October 05, 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..... 3

Support..... 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation 8

Configuration 9

ThreatQ Mapping.....10

 Flashpoint Adversary Forum10

Average Feed Run.....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 © 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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Flashpoint Adversary Forum CDF retrieves community posts published by configured Flashpoint adversaries or authors and ingests them into ThreatQ.

The integration provides the following feed:

- **Flashpoint Adversary Forum** - retrieves posts from Flashpoint Communities for configured authors and ingests them into ThreatQ as events with associated adversaries.

The integration ingests adversary and event type objects into the ThreatQ platform.

Prerequisites

The following is required to run the integration:

- A Flashpoint API key.
- One or more Flashpoint author names to query.

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 **Commercial** 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
API Key	Enter a Flashpoint bearer token authorized to access the Communities endpoint. The value is masked in the ThreatQ user interface.
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.
Adversaries	Enter a comma-separated list of Flashpoint author names without quotation marks. Empty and duplicate entries are removed before the request is sent.

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

Flashpoint Adversary Forum

The Flashpoint Adversary Forum CDF retrieves community posts published by configured Flashpoint adversaries or authors and ingests them into ThreatQ as Event objects. The feed also creates or updates associated Adversary objects, providing context on relevant forum activity.

POST <https://app.flashpoint.io/api/v1/communities>

Sample Request:

```
{
  "include": {
    "date": {
      "label": "ThreatQ feed window",
      "start": "2026-09-20T00:00:00Z",
      "end": "2026-09-21T00:00:00Z"
    },
    "author": ["APT32", "ShinyHunters"]
  },
  "dedupe": true,
  "highlight": {
    "enabled": false
  }
}
```

Sample Response:

```
{
  "items": [
    {
      "id": "fp-community-post-001",
      "author": "APT32",
      "author_id": "author-001",
      "author_internal_id": "internal-author-001",
      "created_at": "2026-09-20T08:15:00Z",
      "container_id": "thread-001",
      "container_name": "restricted-access-forum",
      "container_external_uri": "https://example.invalid/forum/thread-001",
      "container_title": "Initial access offerings",

```

```

    "date": "2026-09-20T08:10:00Z",
    "first_observed_at": "2026-09-20T08:16:00Z",
    "indexed_at": "2026-09-20T08:17:00Z",
    "last_observed_at": "2026-09-20T09:30:00Z",
    "message": "Synthetic sample post for offline CDF validation.",
    "message_id": "message-001",
    "native_id": "native-message-001",
    "native_url": "https://example.invalid/forum/thread-001/
message-001",
    "site": "Example Forum",
    "site_actor_alias": "APT32",
    "site_actor_handle": "apt32_sample",
    "site_source_uri": "https://example.invalid/forum",
    "site_title": "Example Forum",
    "sort_date": "2026-09-20T08:10:00Z",
    "source_uri": "https://example.invalid/source/message-001",
    "title": "Sample forum post",
    "title_id": "title-001",
    "type": "post"
  }
],
"total": 1
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.items[]</code>	Event.value	Social Network Post	<code>.items[].date</code>	APT32 posted in Example Forum: Initial access offerings (message-001)	Creates one Event per returned post.
<code>.items[].message</code>	Event.Description	Description	<code>.items[].date</code>	Synthetic sample post...	Stores the forum-post content.
<code>.items[].date</code>	Event.date	Happened At	<code>.items[].date</code>	2026-09-20T08:10:00Z	Sets the Event occurrence time. The test sample exposes the same value as <code>.items[].happened_at</code> .
<code>.items[].author</code>	Adversary.value	Name	<code>.items[].date</code>	APT32	Creates or updates the Adversary and relates it to the Event.
<code>.items[].author</code>	Event.Tag	Name	<code>.items[].date</code>	APT32	Applied to the Event when the author is non-empty.
<code>.items[].id</code>	Event.Attribute	ID	<code>.items[].date</code>	fp-community-post-001	Also used as the Event-title identifier when <code>message_id</code> is empty.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].author_id	Event.Attribute	Author ID	.items[].date	author-001	Added to the Event when non-empty.
.items[].author_internal_id	Event.Attribute	Author Internal ID	.items[].date	internal-author-001	Added to the Event when non-empty.
.items[].created_at	Event.Attribute	Created At	.items[].date	2026-09-20T08:15:00Z	Added to the Event when non-empty.
.items[].container_id	Event.Attribute	Container ID	.items[].date	thread-001	Added to the Event when non-empty.
.items[].container_name	Event.Attribute	Container Name	.items[].date	restricted-access-forum	Added to the Event when non-empty.
.items[].container_external_uri	Event.Attribute	Container External URI	.items[].date	https://example.invalid/forum/thread-001	Added to the Event when non-empty.
.items[].first_observed_at	Event.Attribute	First Observed At	.items[].date	2026-09-20T08:16:00Z	Added to the Event when non-empty.
.items[].indexed_at	Event.Attribute	Indexed At	.items[].date	2026-09-20T08:17:00Z	Added to the Event when non-empty.
.items[].last_observed_at	Event.Attribute	Last Observed At	.items[].date	2026-09-20T09:30:00Z	Added to the Event when non-empty.
.items[].message_id	Event.Attribute	Message ID	.items[].date	message-001	Preferred identifier in the generated Event title.
.items[].native_id	Event.Attribute	Native ID	.items[].date	native-message-001	Added to the Event when non-empty.
.items[].native_url	Event.Attribute	Native URL	.items[].date	https://example.invalid/forum/thread-001/message-001	Added to the Event when non-empty.
.items[].site	Event.Attribute	Site	.items[].date	Example Forum	Also used in the generated Event title.
.items[].site_actor_alias	Event.Attribute	Site Actor Alias	.items[].date	APT32	Added to the Event when non-empty.
.items[].site_actor_handle	Event.Attribute	Site Actor Handle	.items[].date	apt32_sample	Added to the Event when non-empty.
.items[].site_source_uri	Event.Attribute	Site Source URI	.items[].date	https://example.invalid/forum	Added to the Event when non-empty.
.items[].site_title	Event.Attribute	Site Title	.items[].date	Example Forum	Added to the Event when non-empty.
.items[].sort_date	Event.Attribute	Sort Date	.items[].date	2026-09-20T08:10:00Z	Added to the Event when non-empty.
.items[].source_uri	Event.Attribute	Source URI	.items[].date	https://example.invalid/source/message-001	Added to the Event when non-empty.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].title	Event.Attribute	Title	.items[].date	Sample forum post	Used as the Event-title fallback when container_title is empty.
.items[].title_id	Event.Attribute	Title ID	.items[].date	title-001	Added to the Event when non-empty.
.items[].type	Event.Attribute	Message Type	.items[].date	post	Does not change the ThreatQ Event type.

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	2 minutes
Events	2
Events Attribute	24
Adversaries	2

Change Log

- **Version 1.0.0**
 - Initial release