

ThreatQuotient

A Securonix Company



Flashpoint Ignite Alerts CDF

Version 1.3.1

May 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 | 3 |
| Support | 4 |
| Integration Details | 5 |
| Introduction | 6 |
| Prerequisites | 7 |
| Installation | 8 |
| Configuration | 9 |
| ThreatQ Mapping | 11 |
| Flashpoint Ignite Alerts | 11 |
| Average Feed Run | 15 |
| Change Log | 16 |

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 1.3.1

Compatible with ThreatQ Versions $\geq 5.12.1$

Support Tier ThreatQ Supported

Introduction

The Flashpoint Ignite Alerts CDF for ThreatQ enables the automatic ingestion of an alert within Flashpoint.

The integration ingests threat intelligence data from the following endpoint:

- **Flashpoint Ignite Alerts** - ingests Ignite Alert data into the ThreatQ platform.

The integration ingests following object types:

- Adversaries
- Events
 - Event Attributes
- Indicators
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A Flashpoint Ignite API Key.

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 **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 parameter under the **Configuration** tab:

| PARAMETER | DESCRIPTION |
|-----------------------------------|------------------------------------------------------------------------------------------------------------|
| API Key | Your Flashpoint Ignite Alerts API Key. |
| Disable Proxies | Enable this option if the feed should not honor proxies set in the ThreatQ UI. |
| Enable SSL Verification | Enable this parameter to validate the host-provided SSL certificate. This parameter is enabled by default. |
| Query IDs | Optional - Enter a line-separated list of query IDs to filter alerts. |
| Ingest Highlights | Enable this parameter to ingest highlights. |
| Link Adversaries to Alerts | Enable this parameter to link ingested adversaries to alerts. This parameter is disabled by default. |
| Save CVE Data as | Select how to ingest CVEs as into the ThreatQ platform. Options include: |

PARAMETER

DESCRIPTION

- Indicators
- Vulnerabilities

Only Ingest Curated Alerts

When enabled, only curated alerts will be ingested. Curated reports are those reviewed by Flashpoint analysts and identified as having higher relevance or significance. This parameter is disabled by default.

< Flashpoint Ignite Alerts



Disabled Enabled

Uninstall

Additional Information
 Integration Type: Feed
 Version:

Configuration Activity Log

Connection & Authentication

API Key

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

Enable SSL Verification

API Options

Query IDs (Optional)

(Optional) Enter a line-separated list of query IDs to filter alerts by. You can obtain these IDs from the Flashpoint Ignite Notifications page. Select a Saved Search, and copy the ID from your browser's URL bar.

Ingestion Options

Ingest Highlights
If true, highlights will be ingested.

Link Adversaries to Alerts
If true, Adversaries will be ingested and linked to Alerts.

Save CVE Data As
 Vulnerabilities

Select which entity types you'd like CVEs to be ingested as into ThreatQ

Only Ingest Curated Alerts
If true, only curated alerts will be ingested. Curated reports are those that have been reviewed by Flashpoint analysts and deemed to be of higher relevance or importance.

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 Ignite Alerts

The Flashpoint Ignite Alerts feed enables the automatic ingestion Ignite Alert data into the ThreatQ platform as Events, Indicators, and Vulnerabilities.

GET <https://api.flashpoint.io/alert-management/v1/notifications>

Sample Response:

```
{
  "items": [
    {
      "id": "8a45bd35-1fac-4b35-aa27-630ab3821507",
      "resource": {
        "id": "LIjNc-xrVUynzUwsoqPfVw",
        "basetypes": [
          "chat",
          "conversation",
          "message",
          "telegram"
        ],
        "title": "BIGFATCHAT™",
        "sort_date": "2024-06-03T20:15:07Z",
        "site": {
          "title": "Telegram"
        },
        "container": {
          "name": "BIGFATCHAT™",
          "native_id": "1213408970",
          "title": "BIGFATCHAT™"
        },
        "site_actor": {
          "names": {
            "handle": "RISK"
          },
          "native_id": "5375938422"
        },
        "created_at": {
          "date-time": "2024-06-03T20:15:07+00:00",
          "raw": "1717445707",

```

```

        "timestamp": 1717445707
    }
},
"reason": {
    "id": "218f7b12-8c85-474e-8013-98d014e99c8c",
    "name": "Insider Threat Alerts",
    "text": "(\"I am an employee\" OR \"i'm an employee\" OR \"i
can get access\" OR \"i have access to\" OR \"i work at\" OR \"i work
for\" OR inny OR \"i'm employed at\" OR \"my occupation is\") NOT
arsenal",
    "origin": "two-face",
    "details": {
        "sources": [
            "communities"
        ],
        "params": {
            "sort": "relevancy",
            "exclude": {},
            "include": {
                "date": {
                    "end": "now",
                    "label": "Last 7 Days",
                    "start": "now-7d"
                }
            }
        }
    }
},
"entity": {
    "id": "001o000000igOLYAA2",
    "name": "ThreatQ",
    "type": "organization"
}
},
"status": null,
"generated_at": "2024-06-03T20:16:12.875144Z",
"created_at": "2024-06-03T20:16:14.716472Z",
"tags": {},
"highlights": {
    "body.text/plain": [
        "Nah I need 6 figs stims tho can fly you out where inny at"
    ]
}
},

```

```

    "highlight_text": "Nah I need 6 figs stims tho can fly you out
where inny at",
    "data_type": "chat",
    "parent_data_type": null,
    "source": "communities",
    "is_read": false
  }
],
"pagination": {
  "next": "https://api.flashpoint.io/alert-management/v1/
notifications?
created_after=now-7d&created_before=nowATsize=25&cursor=1717444021.23
0215",
  "first": "https://api.flashpoint.io/alert-management/v1/
notifications?
created_after=now-7d&created_before=nowATsize=25&cursor=1717445812.55
8666"
}
}

```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------------------|----------------|---------------------------------------------------------------------------|-------------------------------------------------------|
| Alert: .items[].reason.name + .items[].resource.site.title, .items[].resource.section, .items[].resource.site_actor.name s.handle, items[].resource.title[:147] + items[..id | Event.Title | Alert | .generate_d_at | Alert: Insider Threat Alerts... | Keys are used conditionally based on what's available |
| .items[].highlights | Event.Description | N/A | N/A | Nah I need 6 figs stims tho can fly you out where <mark>inny</mark> at... | Description is html formatted with available data |
| .items[].tags | Event.Attribute | Status | .generate_d_at | In Progress | Updatable |
| .items[].status | Event.Attribute | Is Flagged | .generate_d_at | false | Updatable |
| .items[].created_at | Event.Attribute | Created At | .generate_d_at | 2024-06-03T20:16:14.716472Z | |
| .items[].data_type | Event.Attribute | Data Type | .generate_d_at | chat | N/A |
| .items[].source | Event.Attribute | Source | .generate_d_at | communities | N/A |
| .items[].is_read | Event.Attribute | Is Read | .generate_d_at | False | Updatable |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|------------------------------------------------------------------------------|---------------------------------|--------------------------------------|----------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <code>.items[].reason.entity.name</code> | Event.Attribute | Entity | <code>.generated_at</code> | ThreatQ | N/A |
| <code>.items[].reason.name</code> | Event.Attribute | Category | <code>.generated_at</code> | Insider Threat Alerts | Updatable |
| <code>.items[].reason.text</code> | Event.Attribute | Search Text | <code>.generated_at</code> | (\ "I am an employee\ " OR \ "i'm an employee\ " OR \ "i can get access... | N/A |
| <code>.items[].resource.basetypes</code> | Event.Attribute | Base Type | <code>.generated_at</code> | chat, conversation | N/A |
| <code>.items[].resource.container.title</code> | Event.Attribute | Container Title | <code>.generated_at</code> | BIGFATCHAT™ | N/A |
| <code>.items[].resource.container.title</code> | Event.Attribute | Container Title | <code>.generated_at</code> | N/A | N/A |
| <code>.items[].resource.container.name</code> | Event.Attribute | Container Name | <code>.generated_at</code> | BIGFATCHAT™ | N/A |
| <code>.items[].resource.container.name</code> | Event.Attribute | Container Name | <code>.generated_at</code> | N/A | N/A |
| <code>.items[].resource.site.title</code> | Event.Attribute | Site Title | <code>.generated_at</code> | Telegram | N/A |
| <code>.items[].highlights[].body.text/plain / .items[].highlight_text</code> | Event.Attribute | Alert Highlights | <code>.generated_at</code> | Nah I need 6 figs stims tho can fly you out where <mark>inny</mark> at | <code>.items[].highlights[].body.text/plain</code> joined by < / br> or <code>.items[].highlight_text</code> , User-configurable |
| <code>.items[].highlights[].body.text/plain / .items[].highlight_text</code> | Related Vulnerability/Indicator | CVE | <code>.generated_at</code> | CVE-2025-12389 | CVE values mentioned in <code>.items[].highlights[].body.text/plain</code> or <code>.items[].highlight_text</code> , User-configurable |
| <code>.items[].resource.site_actor.name.s.handle</code> | Event.Attribute | Site Actor | <code>.generated_at</code> | RISK | N/A |
| <code>.items[].resource.site_actor.name.s.aliases[]</code> | Event.Attribute | Site Actor | <code>.generated_at</code> | N/A | N/A |
| <code>.items[].resource.site_actor.name.s.handle</code> | Adversary .Value | Adversary | <code>.generated_at</code> | RISK | User-configurable |
| <code>.items[].resource.site_actor.name.s.aliases[]</code> | Adversary .Value | Adversary | <code>.generated_at</code> | N/A | User-configurable |

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 |
| Adversaries | 24 |
| Events | 25 |
| Event Attributes | 442 |
| Vulnerabilities | 3 |

Change Log

- **Version 1.3.1**
 - Resolved an issue affecting the parsing and ingestion of key/value tags as attributes.
- **Version 1.3.0**
 - Added a new configuration parameter: **Only Ingest Curated Alerts**. When enabled, the feed ingests only Flashpoint alerts that have been reviewed and curated by Flashpoint analysts for higher relevance and significance.
 - Updated the **Status** attribute to reflect the Flashpoint Alert label (for example, In Progress or Actioned). Previously, this field reflected only whether the alert was flagged in Flashpoint.
 - Added a new **Is Flagged** attribute to indicate whether a Flashpoint alert has been flagged (starred).
- **Version 1.2.7**
 - Resolved an issue where missing container and title information would cause feed runs to fail with an `error applying filter` error message.
- **Version 1.2.6**
 - The integration now ingests adversary object types.
 - Added a new configuration parameter:
 - **Link Adversaries to Alerts** - link ingested adversaries to alerts.
- **Version 1.2.5**
 - Resolved an issue with incorrect Flashpoint Ignite links for Media type events.
- **Version 1.2.4**
 - Flashpoint Ignite links to alert descriptions are now ingested as descriptions in ThreatQ.
- **Version 1.2.3**
 - Site Actors are no longer ingested as related Adversaries.
 - Context information will no longer be included in the description and will now be saved as attributes.
 - Added a new configuration parameter:

-
- **Save CVE Data As** - select if CVEs should be ingested as Indicators or Vulnerabilities.
 - **Version 1.2.2**
 - Added a new configuration parameter: **Ingest Highlights**. Users can use this setting to control if the feed will ingest **Alert Highlights** attribute.
 - Removed HTML tags from the **Alert Highlights** attribute.
 - **Version 1.2.1**
 - Updated the style for Event descriptions.
 - Added **Search Text** and **Alert Highlights** attributes to Events.
 - Added Actors as related Adversaries.
 - Added two new configuration parameters: **Disable Proxies** and **Enable SSL Verification**.
 - **Version 1.2.0**
 - Updated the feed to use Flashpoint Ignite Alerts endpoint.
 - Alerts now include rich text descriptions containing alert highlights and metadata.
 - Alert Titles have been improved.
 - The Flashpoint Link attribute has been replaced with a link within the description.
 - Rebranded the integration to FlashPoint Ignite Alerts CDF.
 - Updated the minimum ThreatQ version to v5.12.1.
 - **Version 1.1.1**
 - Long alert bodies, which would trigger feed errors, are now truncated.
 - **Version 1.1.0**
 - Optimized integration code to improve overall performance and upgraded support tier from Not Supported to ThreatQ Supported.
 - **Version 1.0.0**
 - Initial Release