

ThreatQuotient



Flashpoint Ignite Alerts CDF

Version 1.2.1

August 06, 2024

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

Support

Email: support@threatq.com

Web: 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

 Flashpoint Ignite Alerts 9

Average Feed Run..... 13

 Flashpoint Alerts 13

Change Log 14

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

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	1.2.1
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

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

The integration ingests threat intelligence data from the following endpoint:

- **Flashpoint Ignite Alerts** - ingests Ignite Alerts into the ThreatQ platform as Events.

The integration ingests the Event and Event Attribute type system 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 **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.

- Click on the integration entry to open its details page.
- Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Flashpoint Ignite Alerts API Key.
API Options	Optional - Enter a line-separated list of query IDs to filter alerts.
Enable SSL Verification	Enable this parameter to validate the host-provided SSL certificate. This parameter is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Flashpoint Ignite Alerts

Disabled

Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

Authentication

API Key

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.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuintent.

☒ Enable SSL Verification

Select indicator status to...

Active

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 Alerts into the ThreatQ platform as Events.

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=1717444021.230215",
  "first": "https://api.flashpoint.io/alert-management/v1/notifications?
created_after=now-7d&created_before=nowATsize=25&cursor=1717445812.558666"
}
}

```

```
}

```

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. names.handle, items[].resource.title[:147] + items[..id	Event.Title	Alert	.generat ed_at	Alert: Insider Threat Alerts...	Keys are used conditionally based on what's available
.items[].highlights, .items[].highlight_ text+.items[].id+ .items[].status+ items[].data_type+ .items[].source+ .items[].is_read+ .items[].created_at+ .items[].generated_at+ .items[].resource+ .items[].reason	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[].reason.name	Event.Attribute	Category	.generat ed_at	Insider Threat Alerts	N/A
.items[].reason.text	Event.Attribute	Search Text	.generat ed_at	(\ "I am an employee" OR \ "i'm an employee\ " OR \ "i can get access...	N/A
.items[].resource.basetypes	Event.Attribute	Base Type	.generat ed_at	chat, conversation	N/A
.items[].resource.container.titl e	Event.Attribute	Container Title	.generat ed_at	BIGFATCHAT™ 	N/A
.items[].soresource. container.container.title	Event.Attribute	Container Title	.generat ed_at	N/A	N/A
.items[].resource. container.name	Event.Attribute	Container Name	.generat ed_at	BIGFATCHAT™ 	N/A
.items[].resource. container.container.name	Event.Attribute	Container Name	.generat ed_at	N/A	N/A
.items[].resource.site.title	Event.Attribute	Site Title	.generat ed_at	Telegram	N/A
.items[].highlights[]. body.text/plain/.items[]. highlight_text	Event.Attribute	Alert Highlights	.generat ed_at	Nah I need 6 figs stims tho can fly you out where <mark>inny</ mark> at	.items[].highli ghts[].body.tex t/plain joined by < / br> or .items[].highli ght_text
.items[].resource.site _actor.names.handle	Event.Attribute/ Adversary Value	Site Actor	.generat ed_at	RISK	The actor is ingested both as an

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					event attribute and as an Adversary.
<code>.items[].resource.site_actor.names.aliases</code>	Event.Attribute/Adversary Value	Site Actor	<code>.generated_at</code>	N/A	The actor is ingested both as an event attribute and as an Adversary.

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.

Flashpoint Alerts

METRIC	RESULT
Run Time	1 minute
Events	507
Event Attributes	5380

Change Log

- **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