ThreatQuotient

Flashpoint Alerts CDF Guide

Version 1.1.1

August 08, 2022

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

Integration Details 5
Introduction 6
Installation 7
Configuration 8
ThreatQ Mapping 9
    Flashpoint Alerts 9
Average Feed Run 14
    Flashpoint Alerts 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.

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	1.1.1
Compatible with ThreatQ Versions	>= 4.38.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/flashpoint-alerts-cdf

Introduction

The Flashpoint Alerts CDF for ThreatQ enables the automatic ingestion of an organization's keyword alerts within Flashpoint.

The integration ingests threat intelligence data from the following endpoint:

- **Flashpoint Alerts** - enables the automatic ingestion of an organization's keyword alerts within Flashpoint.

The integration ingests the following system object types:

- Adversaries
- Events

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration 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. If prompted, select the individual feeds to install and click **Install**. 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 API Key.

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 Alerts

The Flashpoint Alerts feed for ThreatQ enables the automatic ingestion of an organization's keyword alerts within Flashpoint.

```
GET https://fp.tools/api/alerting/v1/alerts
```

Sample Response:


```
{
    "data": [
        {
            "alert_id": "16582e98-f2b6-47d7-af1a-1fe8ca598830",
            "fpid": "0a3bc228-6b1b-50e7-b29e-acaa4edfd477",
            "keyword": {
                "keyword_id": "5aa6a7e6-a58e-4c84-830a-eb0b65302052",
                "keyword_text": "threatq"
            },
            "highlights": [
                "FIT50 HEPA Air Purifier - HEPA-Pure\t1\t588\r\nAlen BreatheSmart FIT50 HEPA Air Purifier - HEPA-
Pure / White\t1\t588\r\nAlen BreatheSmart FIT50 HEPA Air Purifier - HEPA-Pure\t1\t588\r\niRobot - Roomba 690 App-
Controlled Robot Vacuum - Black/Silver (15lb)\t1\t350\r\n<x-fp-highlight>ThreatQ</x-fp-highlight>"
            ],
            "basetypes": [
                "paste",
                "post"
            ],
            "ts": 1627390806.591999,
            "tags": {},
            "source": {
                "basetypes": [
                    "paste",
                    "post"
                ],
                "body": {
                    "text/plain": "Delta 9659T-DST Trinsic Single Handle Pull-Down Spring Spout Kitchen Faucet With
Touch2O Technology\t1\t554\r\nDelta 9959T-DST Trinsic Single Handle Pull-Down Bar/Prep Faucet with Touch2O Technology
Chrome\t1\t488\r\nDelta 9181-DS\t1\t310\r\nDelta 3597LF-MPU\t1\t295\r\nDelta 9659-DST\t1\t554\r\nDelta 4159-
DST\t1\t246\r\nGrohe 23 868\t1\t266\r\nDelta 9659T-DST Trinsic Single Handle Pull-Down Spring Spout Kitchen Faucet
With Touch2O Technology Chrome B01JBTLKFY\t1\t554\r\nDelta 9659-DST\t1\t554\r\nPS4 1TB Pro Console with Dual Charging
Dock\r\nHome Cinema LS100 Full HD 3LCD Ultra Short-throw Laser Projector\t1\t2450\r\nAKG C214 Professional Large-
Diaphragm Condenser Microphone\t1\t495\r\nBOSCH 11264EVS 1-5/8\" SDS-Max Combination Hammer\t1\t599\r\nGarmin
Forerunner 235 Gps Runners Watch NEW\t1\t249\r\nGarmin Forerunner 235 GPS Sport Watch - Black Gray\t1\t249\r\nRachio
16 Zone 2nd Generation Smart Sprinkler Controller\t1\t229\r\nRachio 8 Zone 2nd Gen Smart Sprinkler
Controller\t1\t182\r\nPolar V800 GPS Sports Watch With HR Monitor\t1\t439\r\nAlen BreatheSmart FIT50 HEPA Air
Purifier - HEPA-Pure / White\t1\t588\r\nAlen BreatheSmart FIT50 HEPA Air Purifier - HEPA-Pure\t1\t588\r\nAlen
BreatheSmart FIT50 HEPA Air Purifier - HEPA-Pure / White\t1\t588\r\nAlen BreatheSmart FIT50 HEPA Air Purifier - HEPA-
Pure\t1\t588\r\niRobot - Roomba 690 App-Controlled Robot Vacuum - Black/Silver (15lb)\t1\t350\r\nThreatQ - HC1450
1080p Smart 3LCD Projector - Gray/white (16lb)\t1\t1499\r\nDyson - Cyclone V10 Animal Cord-Free Stick Vacuum (14lb)
\t1\t499\r\nDyson Cyclone V10 Absolute (Black)\t1\t729\r\nDyson Ball Mulitfloor 2 Upright Vacuum\t1\t389\r\nDyson
Cyclone V10 Absolute (Black)\t1\t729\r\nAlen BreatheSmart 75i Air Purifier - HEPA-Pure\t1\t759\r\nLuna Optics LN-NVB3
```

```
3x42 Gen1 Hi-Grade Night Vision Binoculars\t1\t300\r\nShimano XTR PD-M9020 Pedals\t1\t179\r\nShimano Thunnus CI4
Saltwater Spinning Reel 1-B0044ZSZOU(this)Â + 1-B0006781N0\t2\t500\r\nShimano Stradic CI4+ Spinning Reel
1000FB\t1\t229\r\nNorth 760008A Silicone Full Facepiece Respirators 7600 Series\t2\t460"
                },
                "created_at": {
                    "date-time": "2021-07-27T12:54:49+00:00",
                    "raw": "1627390489",
                    "timestamp": 1627390489
                },
                "first_observed_at": {
                    "date-time": "2021-07-27T12:59:57+00:00",
                    "raw": "1627390797.394061",
                    "timestamp": 1627390797
                },
                "fpid": "CjvCKGsbUOeynqyqTt_Udw",
                "last_observed_at": {
                    "date-time": "2021-07-27T12:59:57+00:00",
                    "raw": "1627390797.394061",
                    "timestamp": 1627390797
                },
                "native_id": "i1MmWbda",
                "site": {
                    "title": "pastebin.com"
                },
                "site_actor": {
                    "names": {
                        "handle": "anonymous"
                    }
                },
                "sort_date": "2021-07-27T12:54:49Z",
                "title": "n/a"
            }
        },
        {
            "alert_id": "9699a800-3495-4e97-84de-c3d64584eafc",
            "fpid": "a5413cd1-b1cd-5243-9fdd-ca8fb93685db",
            "keyword": {
                "keyword_id": "5aa6a7e6-a58e-4c84-830a-eb0b65302052",
                "keyword_text": "threatq"
            },
            "highlights": [
                "Kamo 603XL Cartucce Multipack Compatibile con <x-fp-highlight>ThreatQ</x-fp-highlight> 603 603XL
Cartuccia d'inchiostro; Expression Home XP-2100 XP-3100 XP-2105 XP-3105 XP-4100 XP-4105; Workforce WF-2810 WF-2830
WF-2835 WF-2850\n\n A soli 25.13€\n Invece di 32.96€\n Risparmi 7.83€ ("
            ],
            "basetypes": [
                "chat",
                "conversation",
                "message",
                "telegram"
            ],
            "ts": 1627326572.087766,
            "tags": {},
            "source": {
                "basetypes": [
                    "conversation",
                    "chat",
                    "telegram",
                    "message"
                ],
                "body": {
                    "text/plain": " Kamo 603XL Cartucce Multipack Compatibile con ThreatQ 603 603XL Cartuccia
```

```
d'inchiostro; Expression Home XP-2100 XP-3100 XP-2105 XP-3105 XP-4100 XP-4105; Workforce WF-2810 WF-2830 WF-2835
WF-2850\n\n A soli 25.13€\n Invece di 32.96€\n Risparmi 7.83€ (-24%)\n\n 4.0/5 (63)\nPrime: "
                },
                "container": {
                    "basetypes": [
                        "conversation",
                        "chat",
                        "telegram",
                        "container"
                    ],
                    "fpid": "ztO9fSo4W5qh17-AZ6ymXA",
                    "name": "STREAM TV - FILM - SERIE TV - CANALI TV",
                    "title": "STREAM TV - FILM - SERIE TV - CANALI TV"
                },
                "created_at": {
                    "date-time": "2021-07-26T17:44:41+00:00",
                    "raw": "1627321481",
                    "timestamp": 1627321481
                },
                "first_observed_at": {
                    "date-time": "2021-07-26T17:44:41.935925+00:00",
                    "raw": "1627321481.935925",
                    "timestamp": 1627321481
                },
                "fpid": "pUE80bHNUkOf3cqPuTaF2w",
                "last_observed_at": {
                    "date-time": "2021-07-26T17:44:41.935925+00:00",
                    "raw": "1627321481.935925",
                    "timestamp": 1627321481
                },
                "media": {
                    "basetypes": [
                        "telegram",
                        "media"
                    ],
                    "caption": " Kamo 603XL Cartucce Multipack Compatibile con ThreatQ 603 603XL Cartuccia
d'inchiostro; Expression Home XP-2100 XP-3100 XP-2105 XP-3105 XP-4100 XP-4105; Workforce WF-2810 WF-2830 WF-2835
WF-2850\n\n A soli 25.13€\n Invece di 32.96€\n Risparmi 7.83€ (-24%)\n\n 4.0/5 (63)\nPrime: ",
                    "crc32c": "656e9edd",
                    "fpid": "vAJSpbOUXcOSWxM4QVwoLg",
                    "last_observed_at": {
                        "date-time": "2021-07-26T19:02:22+00:00",
                        "raw": "1627326142",
                        "timestamp": 1627326142
                    },
                    "md5": "84a48425a61609fb9cfabfa9f982a696",
                    "media_type": "image",
                    "mime_type": "image/jpeg",
                    "native_id": "6004701426607041462",
                    "orig_media_type": "photo",
                    "phash": "ba3bc4c4c5683a3b",
                    "sha1": "97721442648e3eb6d0c8838580a71f7fc536ff4b",
                    "sha256": "348d1022522bedbdee55ace758c9dbccdc710c6cd3b32c8cb7308d6335d8ea1b",
                    "sha512":
"30a11189d4ce72bc192ea644a16b9c8666cf776c8fc4329bb83e7cba225cac35e89ad1d4bae0e6990de7fb181ab2229be26d4b09f1c42d40db91
20f25a0d2436",
                    "size": 40874,
                    "storage_uri": "gs://navajo-media/97721442648e3eb6d0c8838580a71f7fc536ff4b.jpg",
                    "stored_at": 1627326195,
                    "type": "image"
                },
                "native_id": "135806",
```

```
                "site": {
                    "title": "Telegram"
                },
                "site_actor": {
                    "names": {
                        "aliases": [
                            "[AMZ] DealsManager ",
                            "amzdealsmanagerbot",
                            "[AMZ] DealsManager "
                        ],
                        "handle": "[AMZ] DealsManager "
                    }
                },
                "sort_date": "2021-07-26T17:44:41Z"
            }
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.highlights[0]`, `.keyword.keyword_text`, `.alert_id`	Event Title	Keyword Alert	`.ts`	N/A	Keys are used conditionally based on what's available
`.source.body['text/plain']`	Event Description	N/A	N/A	N/A	Descriptions are formatted/ santized
`.source.site_actor.names.handle`, `.source.site_actor.names.aliases[]`	Attribute	Site Actor	`.ts`	anonymous	Keys are concatenated into a list
`.keyword.keyword_text`	Attribute	Keyword	`.ts`	N/A	N/A
`.source.basetypes`	Attribute	Base Type	`.ts`	paste	N/A
`.source.container.title`	Attribute	Container Title	`.ts`	`STREAM TV - FILM - SERIE TV - CANALI TV`	N/A
`.source.container.container.title`	Attribute	Container Title	`.ts`	`/p/ - Photography`	N/A
`.source.container.container.name`	Attribute	Container Name	`.ts`	DataHoarder	N/A
`.source.site.title`	Attribute	Site Title	`.ts`	reddit	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.

Flashpoint Alerts

METRIC	RESULT
Run Time	2 minutes
Events	25
Event Attributes	188
Adversaries	20

Change Log

- **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