ThreatQuotient

Flashpoint Ignite Action

Version 1.0.0

May 27, 2025

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

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	1.0.0
Compatible with ThreatQ Versions	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Flashpoint Ignite Action integration enriches indicators ingested by the FlashPoint Ignite CDF. The action uses the `Flashpoint ID` to retrieve details and relates attack patterns and sighted related indicators based on user configuration.

The integration provides the following actions:

- **Flashpoint Ignite - IOC Enrichment** - enriches Flashpoint Ignite indicators with attack patterns and sighted related indicators.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- URL

The action returns the following enriched system objects:

- Indicators
  - Indicator Attributes
- Attack Patterns

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - IP Address
  - MD5
  - SHA-1
  - SHA-256
  - URL

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

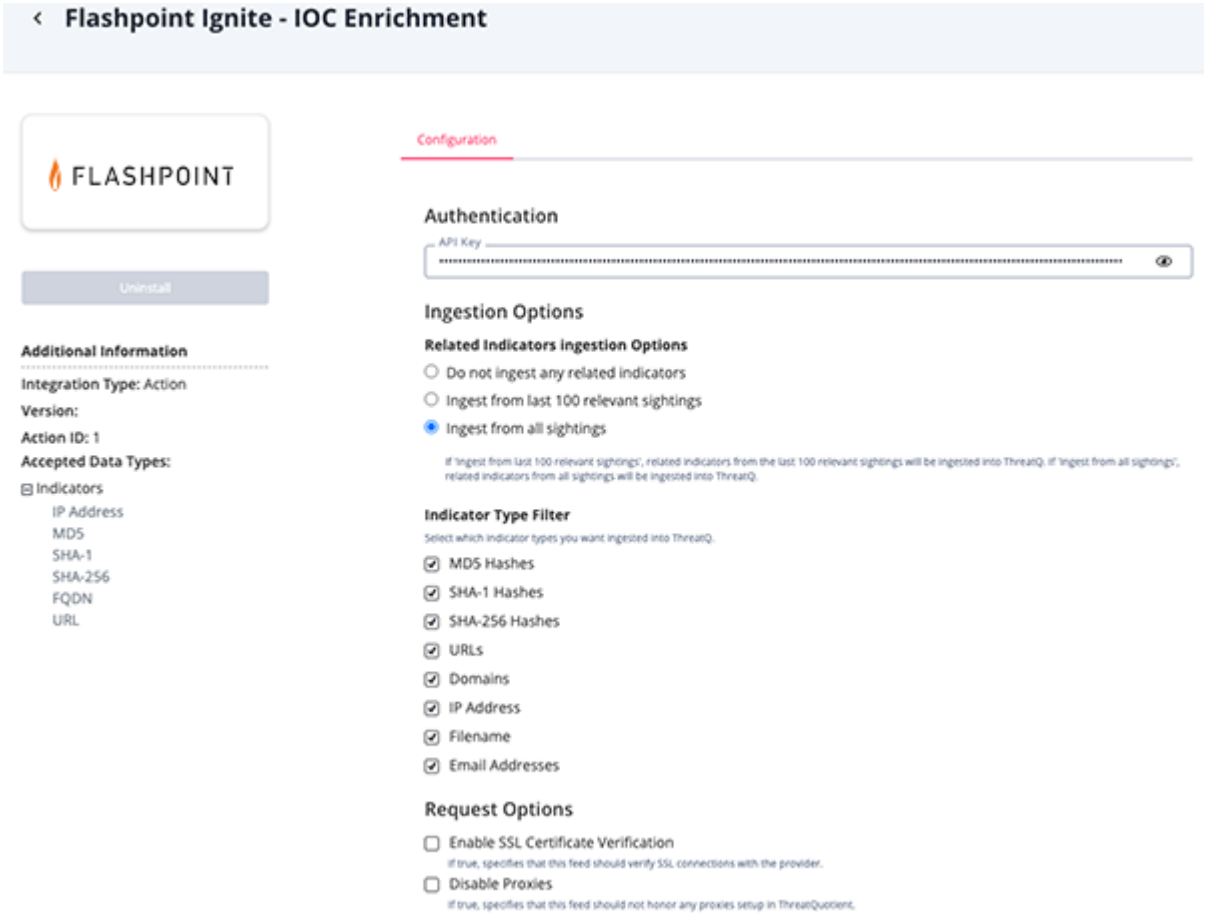
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Flashpoint Ignite API Key.
Related Indicators ingestion Options	Select how the action will handle related indicators. Options include: ◦ **Do not Ingest Any Related Indicators** - related indicators will not be ingested. ◦ **Ingest from Last 100 Relevant Sightings** - related indicators from the last 100 relevant sightings will be ingested into ThreatQ. ◦ **Ingest from All Sightings** - related indicators from all sightings will be ingested into ThreatQ
Indicator Type Filter	Select which indicator types to ingest into ThreatQ. Options include: ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ URLs ◦ Domains ◦ IP Address ◦ Filename ◦ Email Addresses

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The max number of objects to send to this action, per run.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Flashpoint Ignite - IOC Enrichment	Enriches Flashpoint Ignite indicators with attack patterns and sighted related indicators.	Indicators	IP Address, FQDN, URL, MD5, SHA-1, SHA-256

Flashpoint Ignite - IOC Enrichment

The Flashpoint Ignite - IOC Enrichment action enriches Flashpoint Ignite indicators with attack patterns and related indicators from the last 100 relevant sightings or from all the sightings (based on user configuration).

```
GET https://api.flashpoint.io/technical-intelligence/v2/indicators/
{{flashpoint_ID}}
```

Sample Response:


```
{
  "id": "jMXpz9FQXMyPM420kgLTAg",
  "type": "file",
  "value": "a885b1f5377c2a1cead4e2d7261fab6199f83610ffdd35d20c653d52279d4683",
  "href": "https://api.flashpoint.io/technical-intelligence/v2/indicators/
jMXpz9FQXMyPM420kgLTAg",
  "entity_type": "indicator",
  "score": {
    "value": "malicious",
    "last_scored_at": "2025-05-08T17:00:36.866000"
  },
  "modified_at": "2025-05-08T17:00:36.866000",
  "created_at": "2020-10-27T04:02:31",
  "last_seen_at": "2025-05-08T16:47:25.644000",
  "sort_date": "2025-05-08T16:47:25.644000",
  "platform_urls": {
    "ignite": "https://app.flashpoint.io/cti/malware/iocs/
jMXpz9FQXMyPM420kgLTAg"
  },
  "apt_description": "N/A",
  "external_references": [],
  "hashes": {
    "md5": null,
    "sha1": null,
    "sha256":
"a885b1f5377c2a1cead4e2d7261fab6199f83610ffdd35d20c653d52279d4683"
  },
  "malware_description": "<p style=\"\"><a href=\"https://fp.tools/home/
intelligence/reports/report/foL_uSViQMq2YDK6ut9CfA\" rel=\"noopener noreferrer
nofollow\">\"Lokibot\"</a> is a resident loader malware that downloads
additional payloads to the victim machine and provides an array of optional
modules from which potential buyers can select. It is written in C++ and works
on all versions of Windows between Windows XP and Windows 10, and all Windows
server versions. Depending on the number of modules purchased in conjunction
with the regular bot, the binary file size is between seventy and eighty KB,
which is relatively large for a loader, potentially making it easier to
detect.</p><p style=\"\"></p><p style=\"\"><strong>Type:</strong> Loader,
Infostealer</p><p style=\"\"><strong>Platform:</strong> Windows</p><p
style=\"\"><strong>Language:</strong> C/C++</p><p
```

```
style=\"\"><strong>Availability:</strong> <a href=\"https://app.flashpoint.io/
search/context/communities/6wsy7P8OWRuGLtNndksP7g?
page=11&amp;size=25&amp;sort=relevancy&amp;query=lokibot&amp;type=communities&a
mp;include.date=all+time&amp;include.site%5B%5D=Exploit&amp;include.site%5B%5D=
Damagelab+
(now+XSS)&amp;include.site%5B%5D=Hackforums.net&amp;include.site%5B%5D=DamageLa
b+
(Now+XSS)&amp;include.site%5B%5D=Sinister&amp;include.site%5B%5D=Raid+Forums&am
p;dedupe=false&amp;#6wsy7P8OWRuGLtNndksP7g\" rel=\"noopener noreferrer
nofollow\">Malware-as-a-Service (MaaS)</a></p>",
  "mitre_attack_ids": [
    {
      "id": "T1016",
      "name": "System Network Configuration Discovery",
      "tactics": [
        "Discovery"
      ],
      "tactic": "Discovery"
    }
  ],
  "sightings": [
    {
      "source": "flashpoint_detection",
      "sighted_at": "2020-10-27T04:02:31",
      "tags": [
        "malware:lokibot",
        "os:windows",
        "source:flashpoint_detection",
        "t1041",
        "type:stealer"
      ],
      "related_iocs": [
        {
          "id": "Je_c0xvXX9aBpoYH_owdUw",
          "type": "file",
          "value":
"f8d437977dab93e60ed0025422030dd46094873243a673d6dca1171d6d155b03",
          "href": "https://api.flashpoint.io/technical-intelligence/v2/
indicators/Je_c0xvXX9aBpoYH_owdUw"
        },
        {
          "id": "eIRcLxuzVaKl1knKtoIxdg",
          "type": "file",
          "value":
"6946eb1e9ba8405ddbc07bc2972dfeaa5b058847023f92758646b643fc8115de",
          "href": "https://api.flashpoint.io/technical-intelligence/v2/
indicators/eIRcLxuzVaKl1knKtoIxdg"
        },
        {
          "id": "y45w0G8JV6GH5em4kN5U4Q",
          "type": "file",
```

```
          "value":
"f8618a96eb9aaa3699f3045491059355e62b2156b95465cc2777c433c52054ce",
          "href": "https://api.flashpoint.io/technical-intelligence/v2/
indicators/y45w0G8JV6GH5em4kN5U4Q"
        }
      ]
    }
  ],
  "historical_tags": [
    "event:observation",
    "extracted_config:true",
    "malware:lokibot",
    "os:windows",
    "source:flashpoint_detection",
    "source:flashpoint_extraction",
    "t1041",
    "type:stealer"
  ],
  "reports": []
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.mitre_attack_ids.id`	Related Attack Pattern	Attack Pattern	N/A	`T1016`	ID is used to fetch ThreatQ attack pattern(`T1016 - System Network Configuration Discovery`) and relate it to the indicator.
`.sightings[].related_iocs[].value`	Related Indicator	`.sightings[].related_iocs[].type`	N/A	`f8d437977dab93e60ed0025422030dd46094873243a673d6dca1171d6d155b03`	Indicator type is extracted based on value length. See Indicator map below. No related indicator is ingested if `Related Indicators ingestion Options` user configuration field is `Do not ingest any related indicators`.
`.score.value`	Indicator.Attribute	Score	N/A	`malicious`	Updatable.
`.modified_at`	Indicator.Attribute	Modified At	N/A	`2025-05-08T17:00:36.866000`	Updatable.
`.last_seen_at`	Indicator.Attribute	Last Seen At	N/A	`2025-05-08T16:47:25.644000`	Updatable.
`.historical_tags`	Indicator.Tag	N/A	N/A	`[event:observation, extracted_config:true,...]`	N/A

A supplemental Feed is used to retrieve all the sightings and collect all the related indicators when the **Related Indicators ingestion Options** configuration parameter is set to `Ingest from all sightings.`

Get All Sighted Indicators

When selecting the `Ingest from All Sights` option for the **Related Indicators Ingestion Options** parameter, the action retrieves all the sightings of the Flashpoint indicators and collects and ingest all the related indicators.

`GET https://api.flashpoint.io/technical-intelligence/v2/indicators/{{flashpoint_ID}}/sightings`

Sample Response:


```
{
"items": [
    {
      "source": "flashpoint_extraction",
      "sighted_at": "2025-05-08T16:47:25.644000",
      "tags": [
        "extracted_config:true",
        "malware:lokibot",
        "source:flashpoint_extraction"
      ],
      "related_iocs": [
        {
          "id": "MpwgZ7csXPGtoI2FGjgnkw",
          "type": "extracted_config",
          "value": "{\"botnet_id\": \"\", \"campaign_id\": \"\", \"urls\":
[\"http://www.ibsensoftware.co1\"]}",
          "href": "https://api.flashpoint.io/technical-intelligence/v2/
indicators/jMXpz9FQXMyPM420kgLTAg/MpwgZ7csXPGtoI2FGjgnkw"
        },
        {
          "id": "jMXpz9FQXMyPM420kgLTAg",
          "type": "file",
          "value":
"a885b1f5377c2a1cead4e2d7261fab6199f83610ffdd35d20c653d52279d4683",
          "href": "https://api.flashpoint.io/technical-intelligence/v2/
indicators/jMXpz9FQXMyPM420kgLTAg/jMXpz9FQXMyPM420kgLTAg"
        }
      ]
    },
    {
      "source": "flashpoint_detection",
      "sighted_at": "2021-02-27T17:35:56",
      "tags": [
        "event:observation",
        "malware:lokibot",
        "os:windows",
        "source:flashpoint_detection",
        "t1041",
        "type:stealer"
      ],
```

```
      "related_iocs": [
        {
          "id": "jMXpz9FQXMyPM420kgLTAg",
          "type": "file",
          "value":
"a885b1f5377c2a1cead4e2d7261fab6199f83610ffdd35d20c653d52279d4683",
          "href": "https://api.flashpoint.io/technical-intelligence/v2/
indicators/jMXpz9FQXMyPM420kgLTAg/jMXpz9FQXMyPM420kgLTAg"
        }
      ]
    }
],
"total": null,
  "pagination": {
    "next": null,
    "prev": null
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.items[].related_iocs[].value`	Related Indicator	`.items[].related_iocs[].type`	N/A	`f8d437977dab93e60ed0025422030dd46094873243a673d6dca1171d6d155b03`	Indicator type is extracted based on value length. See Indicator map below. No related indicator is ingested if `Related Indicators ingestion Options` user configuration field is `Do not ingest any related indicators`.

Indicator Mapping

URL: URL domain: FQDN ipv4: IP Address file: Hash. See Hash map extracted_config: Filename, URL, FQDN, IP Addresses. See Extracted Config Note.

Hash Mapping

Time is determined based on the Hash length: 32: md5 40: sha-1 64: sha-256

Extracted Config Note

Extracted_config is a special Flashpoint indicator type, that might have the value in this format:


```
"{\"Port\": \"3000\", \"ServerID\": \"vagina\", \"Password\": \"1234\",
\"Install_Flag\": \"TRUE\", \"Install_Directory\": \"HostManager\",
\"Install_Name\": \"HostManager.exe\", \"ActiveX_Startup\":
\"{AL887A2X-5730-5620-121P-H80DXJR5ECUY}\", \"Enable_Message_Box\": \"FALSE\",
\"Activate_Keylogger\": \"TRUE\", \"Keylogger_Enable_FTP\": \"FALSE\",
\"FTP_Directory\": \"./logs/\", \"FTP_UserName\": \"ftp_user\",
\"FTP_Password\": \"none\", \"FTP Port\": \"21\", \"FTP_Interval\": \"30\",
\"Persistance\": \"TRUE\", \"Hide_File\": \"TRUE\", \"Change_CreationDate\":
\"TRUE\", \"Mutex\": \"UDPMQ83G21587O\", \"MeltFile\": \"TRUE\",
\"Startup_Policies\": \"Policies\", \"USB_Spread\": \"1000\", \"P2P_Spread\":
\"none\", \"GoogleChrome_Passwords\": \"http://www.server.com/sqlite3.dll\",
\"Domain\": [\"mw2jtag.no-ip.info\"]}"
```


The indicators are extracted by parsing this value such as: Filename, URL, FQDN, IP Addresses.

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	4
Indicator Attributes	6
Attack Pattern	54

Use Case Example

1. A user submits 5 indicators ingested by Flashpoint Ignite CDF, that have `Flashpoint ID` attribute, using the `Flashpoint Ignite – IOC Enrichment` action to the Flashpoint Ignite.
2. The action queries the Flashpoint Ignite for indicator details, based on the `Flashpoint ID`.
3. The action relates ThreatQ Attack Patterns that are matched based on details Attack Pattern IDs and ingests related indicators from sightings, based on user configuration.

Change Log

- **Version 1.0.0**
  - Initial release