ThreatQuotient

Flashpoint Ignite Vulnerabilities CDF

Version 1.0.1

October 07, 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

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	1.0.1
Compatible with ThreatQ Versions	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

The Flashpoint Ignite Vulnerabilities CDF ingests threat intelligence data from the Flashpoint Ignite API as either indicators or vulnerabilities based on user settings.

The integration provides the following feed:

- **Flashpoint Ignite Vulnerabilities** - ingests vulnerabilities and indicators from the Flashpoint Ignite API.

The integration ingests ether indicators or vulnerabilities system object based on user settings.

Prerequisites

The following is required to run the integration:

- A Flashpoint Ignite API Token.

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 yaml file into the dialog box
   - Select **Click to Browse** to locate the integration yaml 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.

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.

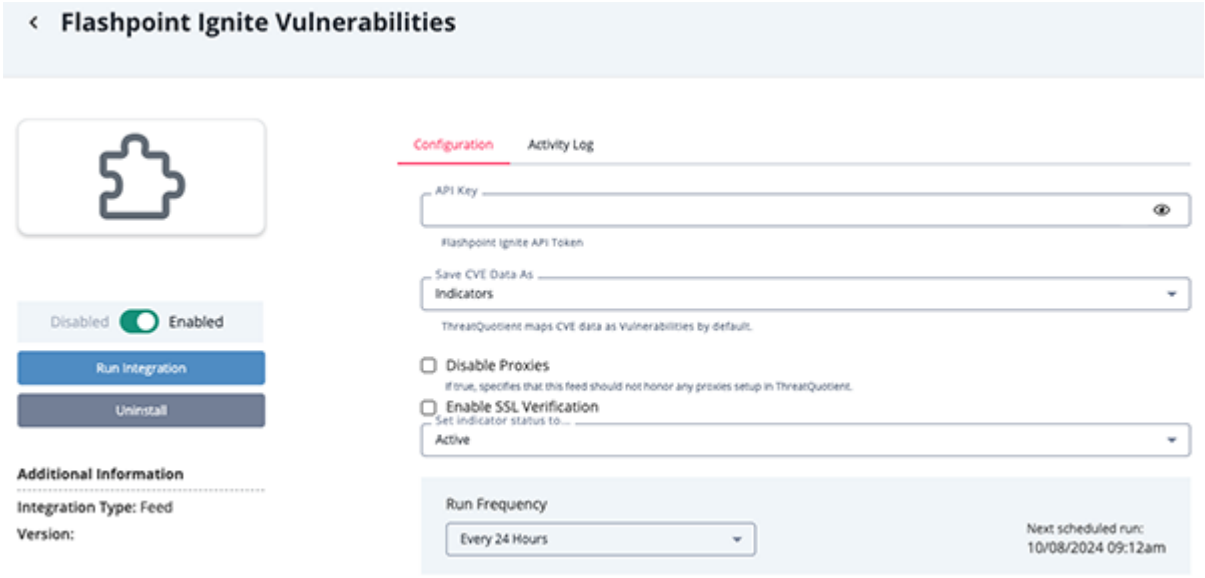
To configure the integration:

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 your Flashpoint Ignite API token.
Save CVE Data As	Select how to ingest the threat data into the platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this option if the feed should verify the SSL certificate.



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 Vulnerabilities

The Flashpoint Ignite Vulnerabilities feeds ingests threat intelligence data from the Flashpoint Ignite API. This data is saved in the form of vulnerabilities or indicators based on the feed configurations.

`GET https://api.flashpoint.io/vuln/vulnerabilities/v1/vulnerabilities/`

Sample Response:


```
{
  "total": 246673,
  "next": "https://api.flashpoint.io/api/v1/vulnerabilities/?from=20size=20",
  "previous": null,
  "size": 20,
  "from": 0,
  "results": [
    {
      "id": 351481,
      "title": "pdfmake dev-playground/server.js createPdfBinary() Function /
pdf Endpoint content Parameter Handling Remote Code Execution",
      "keywords": "",
      "description": "pdfmake contains a flaw in the createPdfBinary() function
in dev-playground/server.js that is triggered as user-supplied input in the
'content' parameter is used with the Function class. With a specially crafted
POST request to the /pdf endpoint, a remote attacker can execute arbitrary
code.",
      "solution": "We are not currently aware of a solution for this
vulnerability.",
      "timelines": {
        "disclosed_at": "2024-02-27T00:00:00Z",
        "published_at": "2024-03-05T08:35:30Z",
        "last_modified_at": "2024-03-05T08:35:30Z"
      },
      "scores": {
        "epss_score": 0.00043,
        "severity": "Critical"
      },
      "vuln_status": "Active",
      "cwes": [],
      "ext_references": [
        {
          "value": "2024-25180",
          "type": "CVE ID",
          "created_at": "2024-02-29T19:33:53Z"
        },
        {
```

```
          "value": "https://github.com/joaoviictorti/My-CVES/blob/main/
CVE-2024-25180/README.md",
          "type": "Other Advisory URL",
          "created_at": "2024-02-29T19:33:53Z"
        }
      ],
      "classifications": [
        {
          "name": "location_remote",
          "longname": "Remote / Network Access",
          "description": "This vulnerability can be exploited over a wired
network (e.g., LAN, WAN, Internet)."
        }
      ],
      "cvss_v2s": [
        {
          "access_vector": "NETWORK",
          "access_complexity": "LOW",
          "authentication": "NONE",
          "confidentiality_impact": "COMPLETE",
          "integrity_impact": "COMPLETE",
          "availability_impact": "COMPLETE",
          "source": "Flashpoint",
          "generated_on": "2024-03-05T08:30:56Z",
          "cve_id": null,
          "score": 10,
          "calculated_cvss_base_score": null
        }
      ],
      "cvss_v3s": [
        {
          "attack_vector": "NETWORK",
          "attack_complexity": "LOW",
          "privileges_required": "NONE",
          "user_interaction": "NONE",
          "scope": "UNCHANGED",
          "confidentiality_impact": "HIGH",
          "integrity_impact": "HIGH",
          "availability_impact": "HIGH",
          "source": "Flashpoint",
          "generated_on": "2024-03-05T08:30:56Z",
          "cve_id": null,
          "score": 9.8,
          "calculated_cvss_base_score": null,
          "vector_string": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/
RL:U/RC:U",
          "version": "3.1"
        }
      ],
      "nvd_additional_information": [],
```

```
      "products": [
        {
          "id": 13058826,
          "name": "pdfmake"
        }
      ],
      "vendors": [
        {
          "id": 12436653,
          "name": "Bartek Pampuch"
        }
      ]
    }
]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
CVE-(.results[].ext_references[].value)	Indicator.Value/ Vulnerability.Value	CVE (for Indicators)	.results[].timelines.published_at	CVE-2024-25180	If `.results[].ext_references[].type` is "CVE ID"
.results[].description	indicator.description/ vulnerability.description	N/A	.results[].timelines.published_at	pdfmake contains a flaw in the createPdfBinary() function in dev-playground/server.js...	
.results[].solution	Indicator.Attribute/ Vulnerability.Attribute	Summary	.results[].timelines.published_at	We are not currently aware of a solution for this vulnerability.	
.results[].scores.severity	Indicator.Attribute/ Vulnerability.Attribute	Severity	.results[].timelines.published_at	Critical	It gets updated at ingestion.
.results[].scores.epss_score	Indicator.Attribute/ Vulnerability.Attribute	EPSS Score	.results[].timelines.published_at	0.00043	It gets updated at ingestion.
.results[].cvss_v2s[].access_complexity	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Access Complexity	.results[].timelines.published_at	LOW	It gets updated at ingestion.
.results[].cvss_v2s[].access_vector	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Access Vector	.results[].timelines.published_at	NETWORK	It gets updated at ingestion.
.results[].cvss_v2s[].authentication	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Authentication	.results[].timelines.published_at	NONE	
.results[].cvss_v2s[].availability_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Availability Impact	.results[].timelines.published_at	COMPLETE	It gets updated at ingestion.
.results[].cvss_v2s[].score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Score	.results[].timelines.published_at	10	It gets updated at ingestion.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].cvss_v2s[].confidentiality_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Confidentiality Impact	.results[].timelines.published_at	COMPLETE	It gets updated at ingestion.
.results[].cvss_v2s[].calculated_cvss_base_score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Calculated CVSS Base Score	.results[].timelines.published_at	10	It gets updated at ingestion.
.result[].cvss_v2s[].integrity_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Integrity Impact	.results[].timelines.published_at	COMPLETE	It gets updated at ingestion.
.results[].cvss_v3s[].attack_complexity	Indicator Attribute/ Vulnerability.Attribute	CVSSV3 Attack Complexity	.results[].timelines.published_at	LOW	It gets updated at ingestion.
.results[].cvss_v3s[].attack_vector	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Attack Vector	.results[].timelines.published_at	NETWORK	It gets updated at ingestion.
.results[].cvss_v3s[].privileges_required	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Privileges Required	.results[].timelines.published_at	NONE	
.results[].cvss_v3s[].availability_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Availability Impact	.results[].timelines.published_at	HIGH	It gets updated at ingestion.
.results[].cvss_v3s[].score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Score	.results[].timelines.published_at	9.8	It gets updated at ingestion.
.results[].cvss_v3s[].confidentiality_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Confidentiality Impact	.results[].timelines.published_at	HIGH	It gets updated at ingestion.
.results[].cvss_v3s[].calculated_cvss_base_score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Calculated CVSS Base Score	.results[].timelines.published_at	9.8	It gets updated at ingestion.
.results[].cvss_v3s[].integrity_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Integrity Impact	.results[].timelines.published_at	HIGH	It gets updated at ingestion.
.results[].cvss_v3s[].scope	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Scope	.results[].timelines.published_at	UNCHANGED	It gets updated at ingestion.
.results[].cvss_v3s[].vector_string	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Vector String	.results[].timelines.published_at	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:U	
.results[].cvss_v3s[].user_interaction	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 User Interaction	.results[].timelines.published_at	NONE	
.results[].products[].name	Indicator.Attribute/ Vulnerability.Attribute	Product Name	.results[].timelines.published_at	pdfmake	
.results[].vendors[].name	Indicator.Attribute/ Vulnerability.Attribute	Product Vendor	.results[].timelines.published_at	Bartek Pampuch	
.results[].classifications.longname	Indicator.Attribute/ Vulnerability.Attribute	Classification Name	.results[].timelines.published_at	Remote / Network Access	
.results[].classifications.description	Indicator.Attribute/ Vulnerability.Attribute	Classification Description	.results[].timelines.published_at	This vulnerability can be exploited over a wired network (e.g., LAN, WAN, Internet).	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].timelines.last_modified_at	Indicator.Attribute/ Vulnerability.Attribute	Last Modified At	.results[].timelines.published_at	2024-03-05T08:45:32Z	Timestamp. It gets updated at ingestion.
.results[].ext_references.value	Indicator.Attribute/ Vulnerability.Attribute	.results[].ext_references.type(Other Advisory URL)	.results[].timelines.published_at	https://github.com/joaoviictorti/My-CVES/blob/main/CVE-2024-25180/README.md	

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.

With the **Save CVE Data As** parameter set to **Vulnerabilities**.

METRIC	RESULT
Run Time	3 minutes
Vulnerabilities	451
Vulnerability Attributes	49,350

Change Log

- **Version 1.0.1**
  - Added the following configuration options:
    - **Enable SSL Verification**
    - **Disable Proxies**
  - Resolved an issue where the fetching data from the provider would trigger an API timeout.
- **Version 1.0.0 rev-a**
  - Updated Integration name from **Flashpoint Ignite CDF** to **Flashpoint Ignite Vulnerabilities CDF**.
- **Version 1.0.0**
  - Initial release