ThreatQuotient

First EPSS CDF User Guide

Version 1.0.1

June 22, 2023

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	>= 4.45.0
Support Tier	ThreatQ Supported

Introduction

The First EPSS CDF for ThreatQ enables analysts to automatically ingest the EPSS (Exploit Prediction Scoring System) scores and the EPSS percentiles for a list of CVEs. The EPSS score represents the probability [0-1] of exploitation in the wild in the next 30 days. The percentile of the score represents the proportion of all scored vulnerabilities with the same or a lower EPSS score. The EPSS score and percentile are computed by FIRST, the global Forum of Incident Response and Security Teams.

The integration provides the following feeds:

- **First EPSS Scores** - ingests the EPSS scores and percentiles for a list of given CVEs.

The integration ingests indicators and indicator attributes.

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.

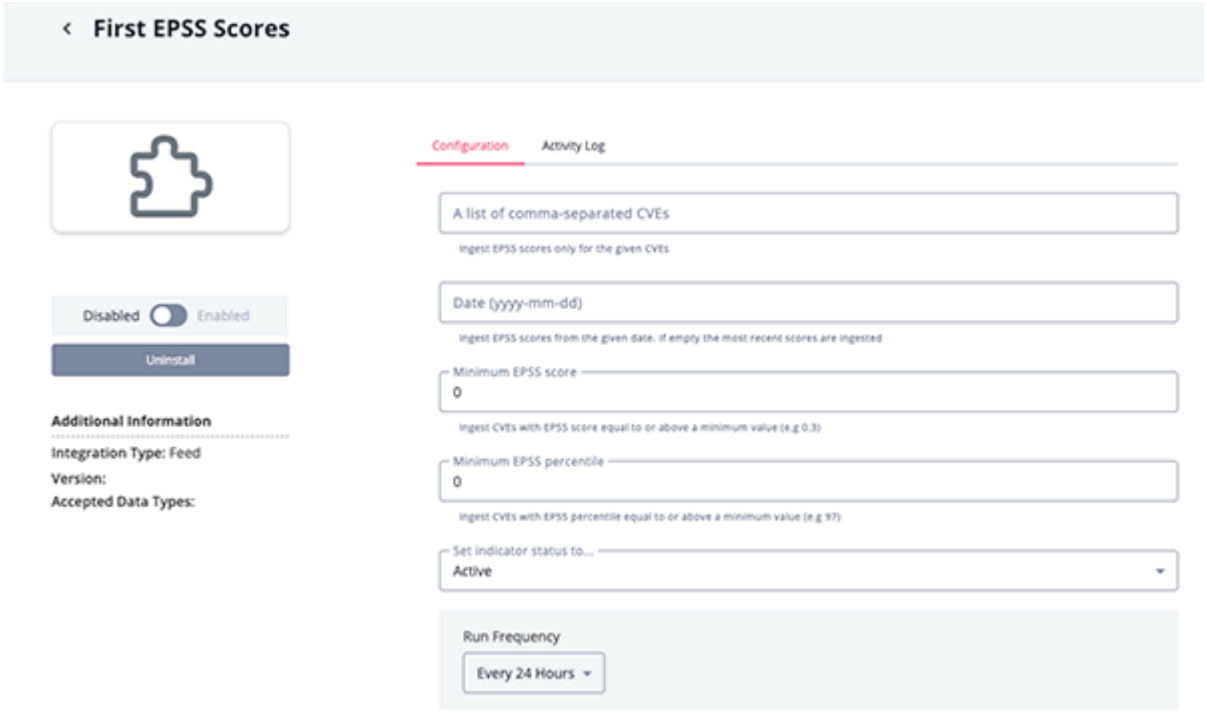
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** 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
A List of Comma-separated CVEs	The CVEs for which the EPSS score and percentile should be ingested.
Date	Set the date to from which to ingest the scores and percentiles. If this value is empty, the most recent values are ingested. The format should be as follows: `yyyy-mm-dd`
Minimum EPSS Score	Optional - Enter the minimum EPSS score to ingest the CVE. Only CVEs with the minimum score or greater will be ingested.
Minimum EPSS Percentile	Optional - Enter the minimum EPSS percentile to ingest the CVE. Only CVEs with the minimum percentile or greater will be ingested.



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

First EPSS Scores

The First EPSS Scores feed ingests the EPSS scores and the corresponding percentiles for a list of given CVEs. It is mandatory to provide the list, because only the specified CVEs the scores will be ingested.

```
GET https://api.first.org/data/v1/epss?
cve=CVE-2022-26332,CVE-2022-26315,CVE-2022-26181&offset=0
```

Sample Response:

```
{
    "status": "OK",
    "status-code": 200,
    "version": "1.0",
    "access": "public",
    "total": 3,
    "offset": 0,
    "limit": 100,
    "data": [
        {
            "cve": "CVE-2022-26332",
            "epss": "0.000720000",
            "percentile": "0.294870000",
            "date": "2023-04-09"
        },
        {
            "cve": "CVE-2022-26315",
            "epss": "0.000860000",
            "percentile": "0.349110000",
            "date": "2023-04-09"
        },
        {
            "cve": "CVE-2022-26181",
            "epss": "0.000560000",
            "percentile": "0.215250000",
            "date": "2023-04-09"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].cve	Indicator.Value	N/A	.data[].date	CVE-2022-26332	N/A
.data[].epss	Indicator.Attribute	EPSS Score	.data[].date	0.000720000	The value is converted into a percentage.
.data[].percentile	Indicator.Attribute	EPSS Score Percentile	.data[].date	29.487	The value is converted into a percentage.

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
Indicators	3
Indicator Attributes	6

Change Log

- **Version 1.0.1**
  - Updated the attributes ingested to be displayed as percentages.
- **Version 1.0.0**
  - Initial release