ThreatQuotient

First EPSS Action Guide

Version 1.0.0

February 14, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/first-epss-action

Introduction

The First EPSS action submits a data collection containing CVE IOCs to First EPSS and returns enriched IOCs and relevant attributes.

The action can perform the following function:

- **First EPSS** - Submits indicators to First EPSS API to be enriched with related threat intelligence.

The action is compatible with CVE indicator types.

The action returns enriched indicator and indicator attributes.

> 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 CVE indicator objects.

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 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

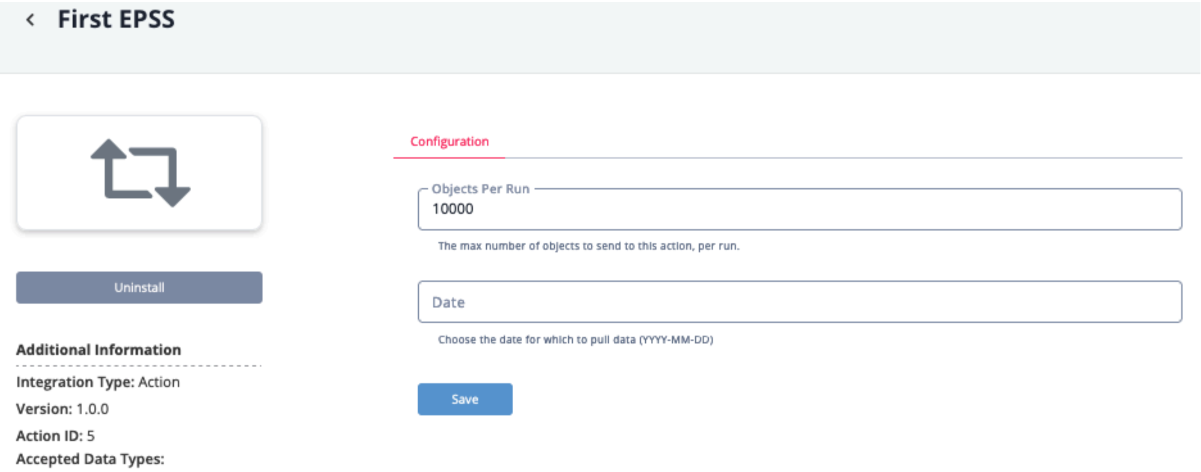
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
Objects Per Run	The max number of objects per run to send to this action. The max value for this parameter is 50,000.
Date	Select the date for which to pull data. The format is as follows: **YYYY-MM-DD**.



First EPSS

Additional Information

Integration Type: Action

Version: 1.0.0

Action ID: 5

Accepted Data Types:

Objects Per Run: 10000

The max number of objects to send to this action, per run.

Date

Choose the date for which to pull data (YYYY-MM-DD)

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

Action Functions

The action provides the following function:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
First EPSS	Enriches IOCs using First EPSS API.	Indicators	CVE

First EPSS

The First EPSS function enriches CVEs using the First EPSS API and returns indicators and indicator attributes.

`GET https://api.first.org/data/v1/epss`

Sample Response

```
{
    "status": "OK",
    "status-code": 200,
    "version": "1.0",
    "access": "public",
    "total": 1,
    "offset": 0,
    "limit": 100,
    "data": [
        {
            "cve": "CVE-2023-25193",
            "epss": "0.008900000",
            "percentile": "0.297670000",
            "date": "2023-02-06"
        }
    ]
}
```

ThreatQ provides the following default mapping for this workflow:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[0].epss`	Indicator.Attribute	EPSS Score	`.data[0].date`	`0.008900000`	The value is transformed in percentage
`.data[0].percentile`	Indicator.Attribute	EPSS Percentile	`.data[0].date`	`0.297670000`	The value is transformed in percentage

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	150
Indicator Attributes	300

Known Issues / Limitations

- The attributes value will be based on the configuration parameter: **Date**. Example: if you select a date of **2023-01-01**, the attributes values will be from that day.

Change Log

- **Version 1.0.0**
    - Initial release