ThreatQuotient

ThreatQ Vulnerability Score Categorizer Action

Version 1.0.0

December 17, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Vulnerability Score Categorizer Action allows you to normalize CVSS and EPSS score attributes and add new attributes for a submitted object based on user configured Scoring Methodology and the numeric Score attribute data that already exists.

The integration provides the following action:

- **ThreatQ Vulnerability Score Categorizer -** normalizes numeric attributes into a string and saves it as a separate updatable attribute.

The action is compatible with the following system object types:

- Indicators (CVE)
- Vulnerabilities

The action returns enriched system objects based on the selected input objects.

> 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 object types:
    - Indicator
        - CVE
    - Vulnerability

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.

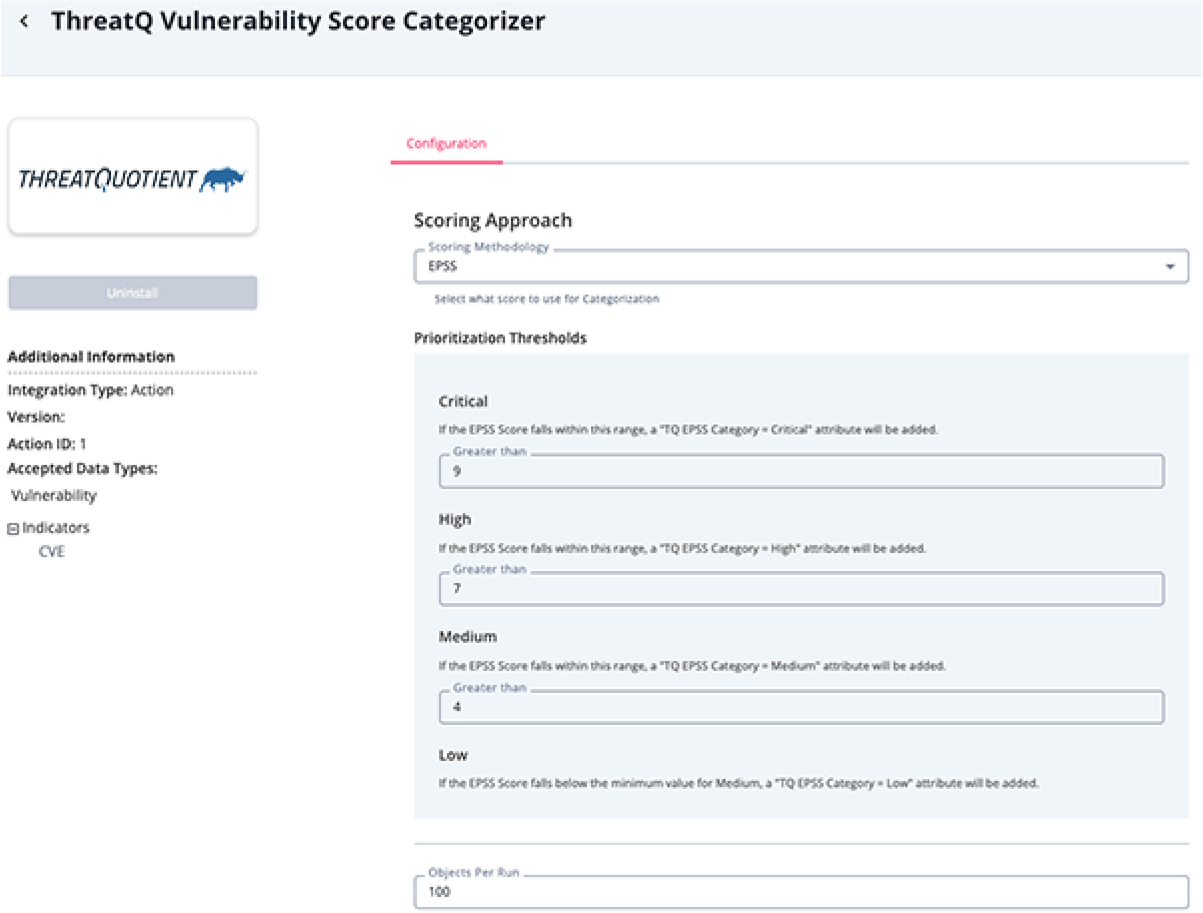
To configure the integration:

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
Scoring Methodology	Select what score to use for Categorization. Options include: ◦ CVSS ◦ EPSS
Prioritization Thresholds - Critical	Enter a critical score range value. A `TQ CVSS/EPSS Category: critical` attribute will be added if the score falls within this set range. The default value is 9.
Prioritization Thresholds - High	Enter a high score range value. A `TQ CVSS/EPSS Category: high` attribute will be added if the score falls within this set range. The default value is 7.
Prioritization Thresholds - Medium	Enter a medium score range value. A `TQ CVSS/EPSS Category: medium` attribute will be added if the score falls within this set range. The default value is 4. A `TQ CVSS/EPSS Category: low` attribute will be added if the score falls below the set medium range.

PARAMETER	DESCRIPTION
Objects Per Run	The number of objects to process per run of the workflow. *(default: 100)*



ThreatQ Vulnerability Score Categorizer

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

Vulnerability

⊟ Indicators

CVE

Scoring Approach

Scoring Methodology: EPSS

Select what score to use for Categorization

Prioritization Thresholds

Critical

If the EPSS Score falls within this range, a "TQ EPSS Category = Critical" attribute will be added.

Greater than: 9

High

If the EPSS Score falls within this range, a "TQ EPSS Category = High" attribute will be added.

Greater than: 7

Medium

If the EPSS Score falls within this range, a "TQ EPSS Category = Medium" attribute will be added.

Greater than: 4

Low

If the EPSS Score falls below the minimum value for Medium, a "TQ EPSS Category = Low" attribute will be added.

Objects Per Run: 100

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
ThreatQ Vulnerability Score Categorizer	Adds a normalized attribute based on CVSS or EPSS score.	Indicators, Vulnerabilities	Indicators - CVE

ThreatQ Vulnerability Score Categorizer

The ThreatQ Vulnerability Score Categorizer action will take a data collection and add a new attribute for each object in the collection based on user selection of Scoring Methodology and the numeric Score attribute data that already exists for the object.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Vulnerability/ Indicator Attribute	TQ CVSS Category	N/A	Medium	Calculated based on existing CVSS Score attribute and the interval defined in the UI Configuration
N/A	Vulnerability/ Indicator Attribute	TQ EPSS Category	N/A	Critical	Calculated based on existing EPSS Score attribute and the interval defined in the UI Configuration

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	5
Indicator Attributes	5

Use Case Example

1. A Threat Analyst is ingesting CVEs as Indicators into ThreatQ, via his commercial feeds. These feeds report CVEs with their CVSS Base Score.
2. The Threat Analyst creates a data collection containing the CVEs ingested from the commercial feeds.
3. The Threat Analyst creates a new TQO workflow using the ThreatQ Vulnerability Score Categorizer action configured with CVSS for Scoring Methodology. The workflow will now automatically normalize the CVSS Base Score for each CVE flowing into the configured data collection.
4. The Threat Analyst can now use their ThreatQ Priority to prioritize CVEs based on their Normalized CVSS Base Score attribute.

Change Log

- **Version 1.0.0**
  - Initial release