ThreatQuotient

MITRE Mapper 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	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Mitre Mapper Action can be used to relate MITRE ATT&CK techniques to ThreatQ objects in a Threat Library data collection.

The integration provides the following action:

- **Mitre Mapper** - relates MITRE ATT&CK techniques to the submitted ThreatQ Objects.

The action is compatible with and enriches the following object types:

- Adversaries
- Assets
- Campaigns
- Courses Of Action
- Events
- Exploits
- Files
- Target Identities
- Indicators
- Incidents
- Intrusion Sets
- Malware
- Notes
- Reports
- Signatures
- Tools
- TTPs
- Vulnerabilities

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

Prerequisites

- The ThreatQ MITRE ATT&CK CDF integration.

  > The CDF must be run, prior to running the action, in order to load all MITRE ATT&CK data.

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
  - Adversaries
  - Assets
  - Campaigns
  - Courses Of Action
  - Events
  - Exploits
  - Files
  - Target Identities
  - Indicators
  - Incidents
  - Intrusion Sets
  - Malware
  - Notes
  - Reports
  - Signatures
  - Tools
  - TTPs
  - Vulnerabilities

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

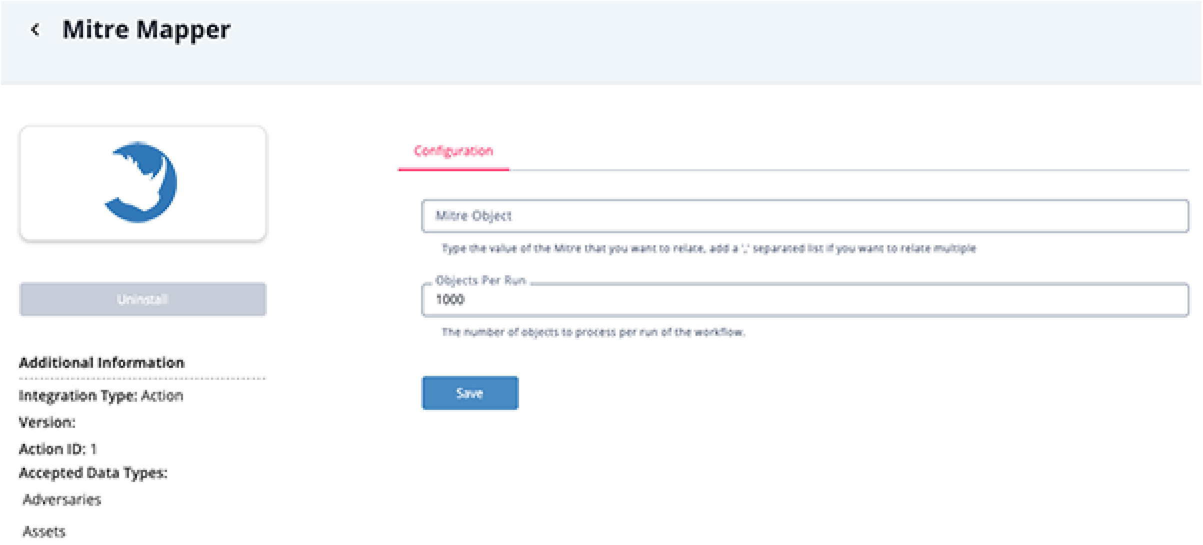
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
Mitre Object	Enter the value of the Mitre that you want to relate. Use a comma delimited format to list for multiple values.
Objects Per Run	The number of objects to process per workflow run. The default value is set to 1,000.



Mitre Object

Type the value of the Mitre that you want to relate, add a ',' separated list if you want to relate multiple

Objects Per Run: 1000

The number of objects to process per run of the workflow.

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

Adversaries

Assets

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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Mitre Mapper	Relates MITRE ATT&CK techniques to selected ThreatQ objects.	Adversaries, Assets, Campaigns, Courses Of Action, Events, Exploits, Files, Target Identities, Indicators, Incidents, Intrusion Sets, Malware, Notes, Reports, Signatures, Tools, TTPs, Vulnerabilities,	N/A

Known Issues / Limitations

- You will need to load all MITRE ATT&CK using the CDF prior to running the Mitre Mapping action.
- The MITRE filter uses cache memory to load all MITRE ATT&CK data, with the cache being refreshed every 24 hours.

Change Log

- **Version 1.0.0**
    - Initial release