ThreatQuotient

MITRE ATT&CK Navigator Operation User Guide

Version 1.0.1

October 30, 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	>= 4.30.0
Support Tier	ThreatQ Supported

Introduction

The MITRE ATT&CK Navigator Operation for ThreatQ allows an analyst to export an Adversary, and its related Attack Patterns, for use in the MITRE ATT&CK Navigator.

The operation provides the following action:

- **Generate Layer** - export Adversary and related Attack Patterns as JSON following the MITRE ATT&CK Navigator 4.2 specification.

The operation is compatible with the following system objects:

- Adversaries
- Campaigns
- Events
- Malware
- Reports
- Tools

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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Generate Layer	Export Adversary and related Attack Patterns as JSON following the MITRE ATTACK Navigator 4.2 specification.	Adversaries, Events, Tools, Malware, Campaigns	N/A

Generate Layer

The Generate Layer action exports Adversary and related Attack Patterns as JSON following the MITRE ATTACK Navigator 4.2 specification.

Action Parameters

The following configuration parameters are available for this action:

PARAMETER	DESCRIPTION
Layer Name	Name for this layer. If left blank, the name will be the object's value.
Description	Description for the layer.
Use the description in ThreatQ instead of the providing one	Use the checkbox to enable/disable this option.
MITRE Domain	Select the MITRE Domain for the layer. Options include **Enterprise** and **Mobile**.
Show techniques by default in Navigator	Use the checkbox to enable/disable this option.
Include object attributes as metadata	Use the checkbox to enable/disable this option.

Change Log

- **Version 1.0.1**
    - The operation is now compatible with Tools and Events object types.
- **Version 1.0.0**
    - Initial release