ThreatQuotient

MISP Operation Guide

Version 1.0.0

December 13, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Not Supported

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 **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The MISP Operation for ThreatQ enables analysts to export Events from ThreatQ into MISP, along with related context.

The operation provides the following action:

- **Share** - Exports a ThreatQ Event to MISP, with related contex.

The operation is compatible with Event object types.

See the Actions chapter for more information on the action listed above.

The operation is compatible with Event object types.

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 feed 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.
6. 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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
MISP Host	Your MISP Hostname or IP.
MISP API Key	Your MISP API Key.
Verify SSL Certificate	Select this checkbox to validate/verify the SSL certification. ⚠ Leave this parameter unchecked if you are using a self-signed certificate.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The MISP Operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPES
Share	Exports a ThreatQ event to MISP, with related context	Event

Share

The Share action allows you to share an event from ThreatQ to MISP, along with related context such as MISP Galaxies, indicators, and attributes.

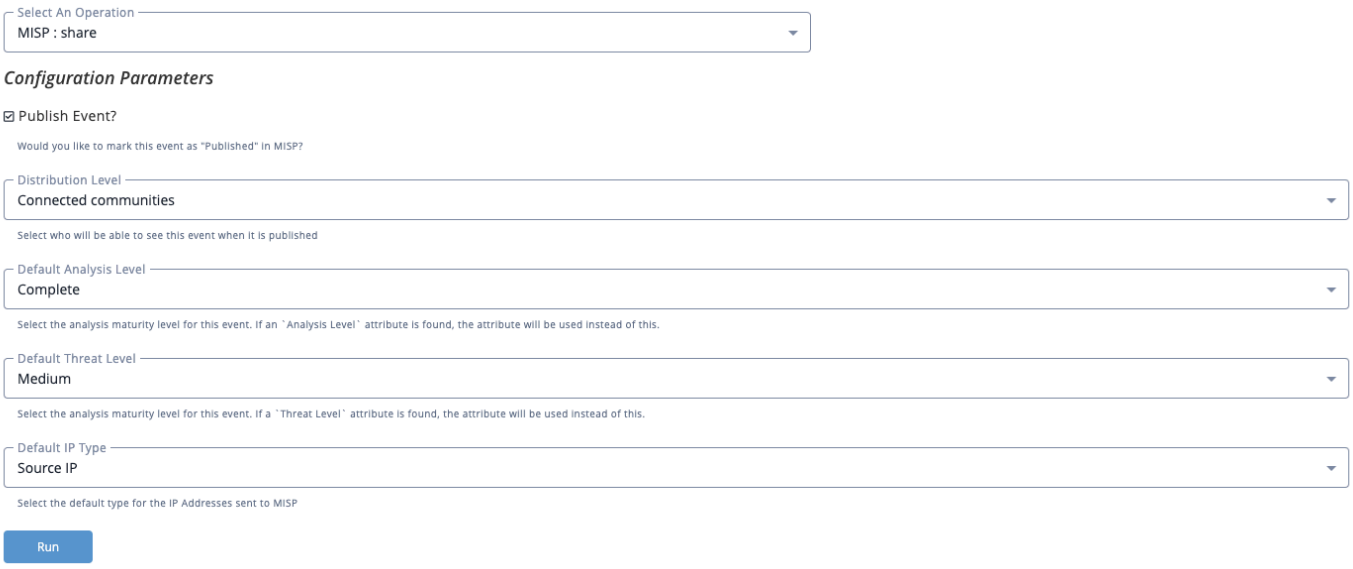
There is no API response data or mappings for this action.

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Publish Event	Use this checkbox to mark the event as `Published` in MISP. This parameter is selected by default.
Distribution Level	Select who will be able to see this event when it is published. Options include: • Connected communities (Default) • Your organization only • This community only • All communities • Sharing group
Default Analysis Level	Select the analysis maturity level for this event. If an `Analysis Level` attribute is found, the attribute will be used instead of this value. Options include: • Initial • Ongoing • Complete (Default)
Default Threat Level	Select the analysis maturity level for this event. If a `Threat Level` attribute is found, the attribute will be used instead of this value. Options include:

PARAMETER	DESCRIPTION
	• High • Medium (Default) • Low • Undefined
Default IP Type	Select the default type for the IP Addresses sent to MISP. Options include: • Source IP (Default) • Destination IP



Known Issues / Limitations

- Not all relationships will be transferred over as `Galaxies`. MISP only supports a handful of Galaxies and we may not be able to "match up" ThreatQ relationships with MISP Galaxies. As a result, all relationships will be transferred over using Attribution, and if Galaxies are found, they will also be used.

Change Log

- **Version 1.0.0**
  - Initial Release