

ThreatQuotient



MISP Operation Guide

Version 1.1.0

April 25, 2022

ThreatQuotient

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

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

- Support 4
- Versioning..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- Actions 9
 - Share..... 10
 - Parameters 10
 - Send Investigation..... 12
 - Parameters 12
- Known Issues / Limitations 13
- Change Log..... 14

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.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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.

Versioning

- Current integration version: 1.1.0
- Compatible with ThreatQ versions \geq 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 actions:



See the [Actions](#) chapter for more information on the actions listed above.

- **Share** - Exports a ThreatQ Event, and related content, to MISP.
- **Send Investigation** - Exports a ThreatQ Investigation, and related content, to MISP.

The operation is compatible with system object types:

- Event
- Files
- Indicators

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. <div> Leave this parameter unchecked if you are using a self-signed certificate.</div>

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, and related content, to MISP.	Events
Send Investigation	Exports a ThreatQ Investigation, along with related content, to MISP.	Events, Files, Indicators

Share

The Share action allows you to share an event from ThreatQ to MISP, along with related context such as MISP Galaxies, indicators, attachments, 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 <code>Published</code> 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: <ul style="list-style-type: none">• 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 <code>Analysis Level</code> attribute is found, the attribute will be used instead of this value. Options include: <ul style="list-style-type: none">• Initial• Ongoing• Complete (Default)
Default Threat Level	Select the analysis maturity level for this event. If a <code>Threat Level</code> attribute is found, the attribute will be used instead of this value. Options include:

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none">• High• Medium (Default)• Low• Undefined
Send IOCs/ Attachments to IDS	Send IOCs and attachments directly to the IDS (if applicable).
Default IP Type	Select the default type for the IP Addresses sent to MISP. Options include: <ul style="list-style-type: none">• Source IP (Default)• Destination IP
Include Unmapped Attribution	Add attribution that doesn't have a mapped Category/Type.

Send Investigation

The Send Investigation action allows you to export an Investigation from ThreatQ to MISP, along with related content such as indicators, attachments, tasks, and events.

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Investigation to send to MISP	The name of the Investigation you want to send to MISP

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 1.1.0**
 - Added new action: **Send Investigation** - export an Investigation from ThreatQ to MISP, along with related content such as indicators, attachments, tasks, and events.
- **Version 1.0.2**
 - Added functionality to upload attachments from ThreatQ to MISP.
- **Version 1.0.1**
 - Optimized integration code to improve overall performance and upgraded support tier from Not Supported to ThreatQ Supported.
- **Version 1.0.0**
 - Initial Release