ThreatQuotient

A Securonix Company

MISP Operation

Version 2.0.0

August 10, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	2.0.0
Compatible with ThreatQ Versions	>= 6.10.0
Support Tier	ThreatQ Supported

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:

- **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 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. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
MISP Host	Your MISP Hostname or IP.
MISP API Key	Your MISP API Key.
MISP Client Certificate	Enter the client certificate used to authenticate with the MISP server. Configure this parameter only if your MISP deployment requires client certificate-based authentication.
MISP Client Private Key	Enter the private key associated with the client certificate used to authenticate with the MISP server. Configure this parameter only if your MISP deployment requires client certificate-based authentication.
Verify SSL Certificate	Enable this parameter if the operation should validate the host-provided SSL certificate. Leave this parameter disabled if you are using a self-signed certificate.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The MISP operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE
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.

Run Configuration Parameters

The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this operation 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)

PARAMETER	DESCRIPTION
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: • 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: • 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.

Run Configuration Parameters

The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available for this operation action:

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

Change Log

- **Version 2.0.0**
  - Migrated the operation to the Python 3.11 runtime to align with the latest platform standards and improve compatibility.
  - Removed the external PyMISP dependency. The operation now communicates directly with the MISP REST API using the ThreatQ framework's built-in HTTP client.
  - Added **MISP Client Certificate** and **MISP Client Private Key** configuration parameters to support MISP deployments that require client certificate-based authentication.
  - Updated the minimum supported ThreatQ version for this operation to **6.10.0**.
- **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