ThreatQuotient

MISP Exporter Action User Guide

Version 1.0.0

March 12, 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	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The MISP Exported Action enables userS to create or update MISP Events from ThreatQ individual objects or collection of objects.

The integration provides the following action:

- **MISP Exporter** - creates or updates MISP Events based on ThreatQ objects.

The action is compatible with the following system object types:

- Campaign
- Event
- Incident
- Indicator

The action does not return enriched system objects.

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

Prerequisites

The action requires the following:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A MISP API Key.

  > The API Key must be associated with a sync user in order to set the Creator Organization.

- A data collection containing at least one of the following object types:
  - Campaign
  - Event
  - Incident
  - Indicator

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:

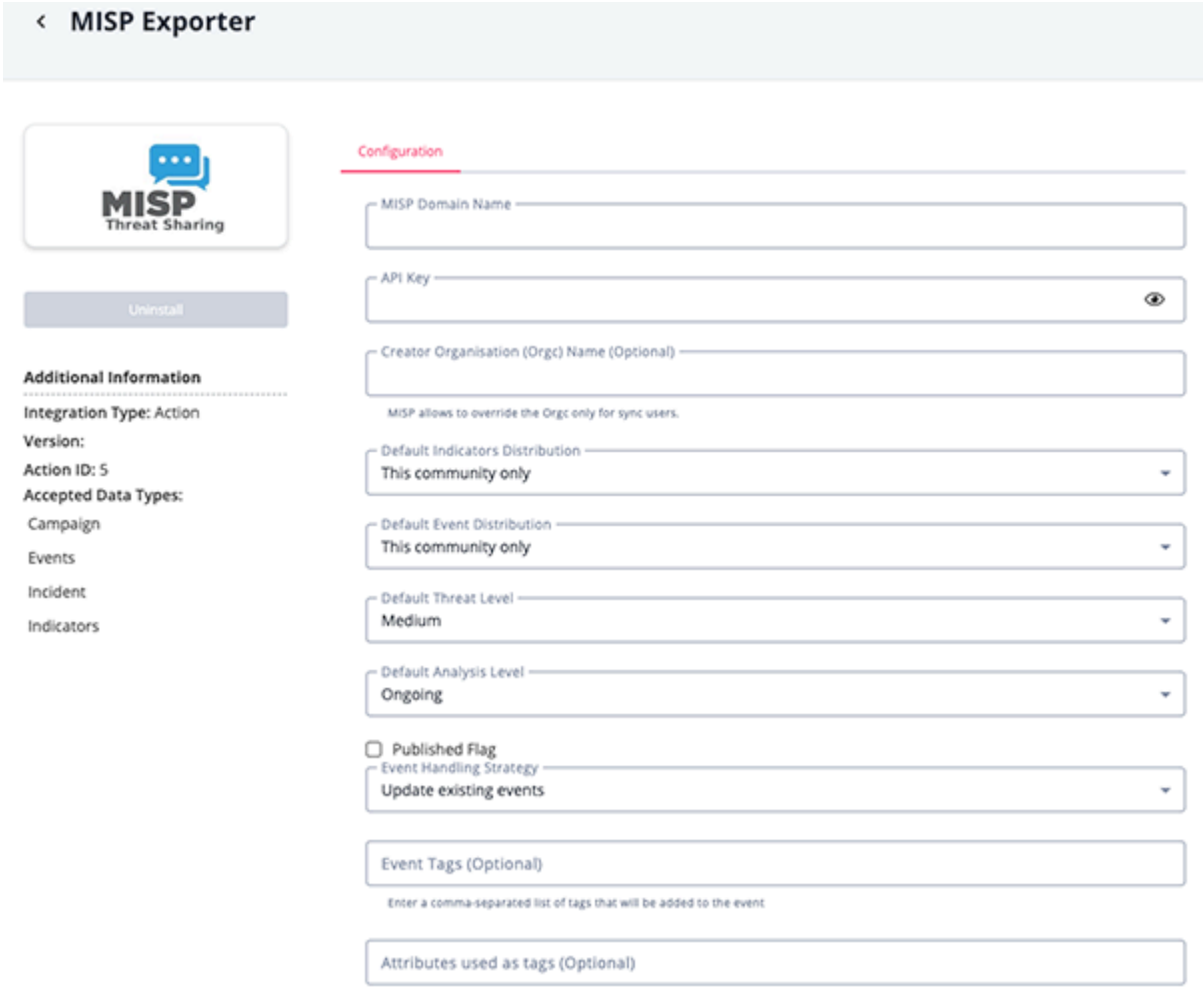
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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
MISP Domain Name	URL to MISP instance.
API Key	MISP API Key.
Creator Organization (Orgc) Name (Optional)	MISP allows to override the Orgc only for sync users.
Default Indicators Distribution	The distribution value set for each indicator, if the attribute `Distribution` is missing. Options include: ◦ Your Organization Only ◦ This Community Only ◦ Connected Communities ◦ All Communities ◦ Inherit Event
Default Event Distribution	The distribution value set for each TQ event/incident/campaign, if the attribute `Distribution` is missing. Options include: ◦ Your Organization Only ◦ This Community Only

PARAMETER	DESCRIPTION
	◦ Connected Communities ◦ All Communities
Default Threat Level	The threat level value set for each TQ event/incident/campaign, if the attribute `MISP Threat Level` is missing. Options include: ◦ High ◦ Medium ◦ Low ◦ Undefined
Default Analysis Level	The threat level value set for each TQ event/incident/campaign, if the attribute `Analysis` is missing. Options include: ◦ Initial ◦ Ongoing ◦ Complete
Published Flag	Specify if the created event is ready to be synchronized.
Event handling strategy	Selecting the option `Create new events` always creates new events from TQ Objects. The option `Update existing events` searches to see if an event with ID equal to attribute `ID` exists, or there is an event with the same name. If such an event exists it will be updated, otherwise a new event is created.
Event Tags (Optional)	Enter a comma-separated list of tags that will be added to the MISP event.
Attributes used as tags (Optional)	Enter a comma-separated list of ThreatQ object attributes that will be added as tags to the event.
Campaign objects handling strategy	Select what to do with objects of type Campaign from the input collection. Options include: ◦ Ignore objects of type Campaign ◦ Create an event for each Campaign object
Related Adversaries handling strategy	Select what to do with the related Adversaries of TQ event/ incident/campaign. Options include: ◦ Ignore related Adversaries ◦ Add related Adversaries as event tags

PARAMETER	DESCRIPTION
Related Campaigns handling strategy	Select what to do with the related Campaigns of TQ event/ incident/campaign. Options include: ◦ Ignore related Campaign ◦ Add related Campaigns as event tags
Related Attack Patterns handling strategy	Select what to do with the related Attack Patterns of TQ event/ incident/campaign. Options include: ◦ Ignore related Attack Patterns ◦ Add related Attack Patterns as comments ◦ Add related Attack Patterns as tags
Related Malware handling strategy	Select what to do with the related Malware of TQ event/incident/ campaign. Options include: ◦ Ignore related Malware ◦ Add related Malware as tags
Related Tools handling strategy	Select what to do with the related Tools of TQ event/incident/ campaign. Options include: ◦ Ignore related Tools ◦ Add related Tools as tags
Related Courses of Action handling strategy	Select what to do with the related Courses of Action of TQ event/ incident/campaign. Options include: ◦ Ignore related Courses of Action ◦ Add related Courses of Action as tags
Add related Signatures as attributes	Specify if related signatures of type Snort or YARA should be added as MISP event attributes. This parameter is disabled by defaults.
Add Indicator's attributes as a comment	Specify if the attributes of an indicator should be exported as a comment. This parameter is enabled by default.
Enable SSL Verification	If True, specifies that this feed should verify SSL connections with the provider. This parameter is enabled by default.
Objects per run	Maximum number of objects to send to MISP Exporter per-run.



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
MISP Exporter	Creates/Update MISP Events based on TQ Objects	Campaign, Incident, Indicator, Event	Indicators - All

MISP Exporter

If the user field `Event handling strategy` is set to `Create new event`, then this function creates an event for each ThreatQ object of type: Campaign, Incident or Event. If the input is a collection of type Indicators, it creates a single MISP event for the entire collection, the name of the event will be the collection name.

If the user field `Event handling strategy` is set to `Update existing events`, then this function searches MISP for events having the ID equal to the ThreatQ object attribute `ID`, or having the name equal to ThreatQ Object name. If such an event exists it will be updated, otherwise a new event is created.

Depending on the user configuration for each ThreatQ object of type Campaign, Incident or Event the related Adversaries, Campaigns, Attack Patterns, Malware, Tools, Courses of Action, Signatures can be set as Attributes or Tags for the MISP Event.

Search Existing Event

`POST {{MISP_URL}}/events/restSearch?limit=1`

Sample Request Body:

```
{
  "eventid": "{{TQ_OBJECT_ATTRIBUTE_ID}}",
  "eventinfo": "{{TQ_OBJECT_NAME}}"
}
```

Sample Response:

```
{
  "response": [
    {
      "Event": {
        "id": "1724",
        "orgc_id": "1",
        "org_id": "1",
        "date": "2024-03-01",
        "threat_level_id": "2",
        "info": "Phishing fish",
        "published": false,
        "uuid": "c15f1cbc-a9a8-4a9c-b116-99e6e6a0b0ce",
        "attribute_count": "0",
        "analysis": "0",
        "timestamp": "1709629500",
        "distribution": "1",
        "proposal_email_lock": false,
        "locked": false,
        "publish_timestamp": "0",
        "sharing_group_id": "0",
        "disable_correlation": false,
```

```
        "extends_uuid": "",
        "event_creator_email": "admin@admin.test",
        "Org": {
          "id": "1",
          "name": "ORGNAME",
          "uuid": "b6c633c5-e4d8-4cea-9cf1-0a71a0cf67ac",
          "local": true
        },
        "Orgc": {
          "id": "1",
          "name": "ORGNAME",
          "uuid": "b6c633c5-e4d8-4cea-9cf1-0a71a0cf67ac",
          "local": true
        },
        "Attribute": [],
        "ShadowAttribute": [],
        "RelatedEvent": [],
        "Galaxy": [],
        "Object": [],
        "EventReport": [],
        "Tag": [
          {
            "id": "1826",
            "name": "workflow",
            "colour": "#ffffff",
            "exportable": true,
            "user_id": "0",
            "hide_tag": false,
            "numerical_value": null,
            "is_galaxy": false,
            "is_custom_galaxy": false,
            "local_only": false,
            "local": 0
          }
        ]
      }
    }
  ]
}
```

Create/Update MISP Event

This request is made only if the user field `Event handling strategy` is set to `Update existing events`.
There is no mapping table for this API request. If the request returns a result, then the MISP Event having the id `.response[0].Event.id` will be updated by this action.

`POST {{MISP_URL}}/events/add` `PUT {{MISP_URL}}/events/edit/{{ID}}`

Request Body:

```
{
  "distribution": "0",
  "threat_level_id": "2",
  "analysis": "1",
  "info": "Usa Iocs Event Data",
  "date": "2024-03-05",
  "published": false,
  "Tag": [
    {
      "colour": "#ffffff",
      "exportable": true,
      "hide_tag": false,
      "name": "type:\"OSINT\""
    }
  ],
  "Attribute": [
    {
      "category": "Network activity",
      "disable_correlation": false,
      "distribution": "0",
      "to_ids": false,
      "type": "ip-src",
      "value": "148.72.164.186"
    }
  ]
}
```

Attribute Distribution Mapping

MISP ATTRIBUTE DISTRIBUTION ID	THREATQ ATTRIBUTE VALUE
0	Your organization only
1	This community only
2	Connected communities
3	All communities
5	Inherit event

Event Distribution Mapping

MISP DISTRIBUTION ID	THREATQ ATTRIBUTE VALUE
0	Your organization only
1	This community only
2	Connected communities
3	All communities

Analysis Mapping

MISP ANALYSIS ID	THREATQ ATTRIBUTE VALUE
0	Initial
1	Ongoing

MISP ANALYSIS ID	THREATQ ATTRIBUTE VALUE
2	Completed

Threat Level Mapping

MISP THREAT LEVEL ID	THREATQ ATTRIBUTE VALUE
1	High
2	Medium
3	Low
4	Undefined

MISP Attribute Type to ThreatQ Indicator Type Mapping

MISP ATTRIBUTE TYPE	THREATQ INDICATOR TYPE
AS	ASN
md5	MD5
sha1	SHA-1
sha256	SHA-256
sha384	SHA-384
sha512	SHA-512
ssdeep	Fuzzy Hash

MISP ATTRIBUTE TYPE	THREATQ INDICATOR TYPE
filename	Filename
ip-src	IPv6 Address
ip-src	IP Address
mac-address	MAC Address
domain	FQDN
email-subject	Email Subject
email-attachment	Email Attachment
email-src	Email Address
email-x-mailer	X-Mailer
regkey	Registry Key
user-agent	User-Agent
mutex	Mutex
url	URL
vulnerability	CVE
uri	URL Path

All indicator types not present into this table are mapped to `Other`.

MISP Attribute Category to ThreatQ Indicator Type Mapping

MISP CATEGORY	THREATQ INDICATOR TYPE
Network activity	ASN
Payload delivery	MD5
Payload delivery	SHA-1
Payload delivery	SHA-256
Payload delivery	SHA-384
Payload delivery	SHA-512
Payload delivery	Fuzzy Hash
Payload delivery	Filename
Network activity	IPv6 Address
Network activity	IP Address
Network activity	MAC Address
Network activity	FQDN
Payload delivery	Email Subject
Payload delivery	Email Attachment
Payload delivery	Email Address
Payload delivery	X-Mailer

MISP CATEGORY	THREATQ INDICATOR TYPE
Persistence mechanism	Registry Key
Network activity	User-Agent
Artifacts dropped	Mutex
Network activity	URL
External analysis	CVE
Network activity	URL Path

Signatures Category Mapping

MISP CATEGORY	THREATQ TYPE
Network activity	Snort
Payload installation	YARA

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	2 minute
Indicators	50
Events	2

Change Log

- **Version 1.0.0**
  - Initial release