ThreatQuotient

A Securonix Company

MISP Import CDF

Version 2.5.0

May 18, 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	2.5.0
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

The MISP Import CDF enables ThreatQ to ingest threat intelligence data from a user-provided, self-hosted MISP (Malware Information Sharing Platform) instance. MISP is a widely adopted open-source threat sharing platform designed to facilitate the exchange of structured threat intelligence using the MISP data model.

This integration retrieves published MISP events through the MISP `events/restSearch` API endpoint and imports the associated intelligence into ThreatQ for analysis, correlation, and operational use. By leveraging data from MISP, organizations can centralize externally shared intelligence alongside internally curated threat data within the ThreatQ platform.

The integration supports the ingestion of a broad range of intelligence objects and related metadata, including events, indicators, adversaries, malware, attack patterns, tools, signatures, attachments, and associated attributes. This enables analysts to preserve the relationships and context provided by MISP while enhancing visibility and enrichment capabilities within ThreatQ.

The integration provides the following feed:

- **MISP Import** — Ingests published MISP events from a user-provided, self-hosted MISP server instance.

The integration ingests the following data types:

- Adversaries
  - Adversary Attributes
- Attachments
  - Attachment Attributes
- Attack Patterns
- Courses of Action
  - Event Attributes
- Events
  - Indicator Attributes
- Indicators
- Malware
- Signatures
- Tools

Prerequisites

- A self-hosted MISP server instance.
- If the user intends to ingest MISP events that are related to any MITRE MISP galaxies, make sure the following feeds (MITRE ATT&CK CDF) successfully run prior to running the MISP Import feed:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE ICS ATT&CK

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 feed 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 feed and will require user confirmation before proceeding.

You will still need to configure and then enable the feed.

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 **OSINT** option from the *Category* dropdown (optional).

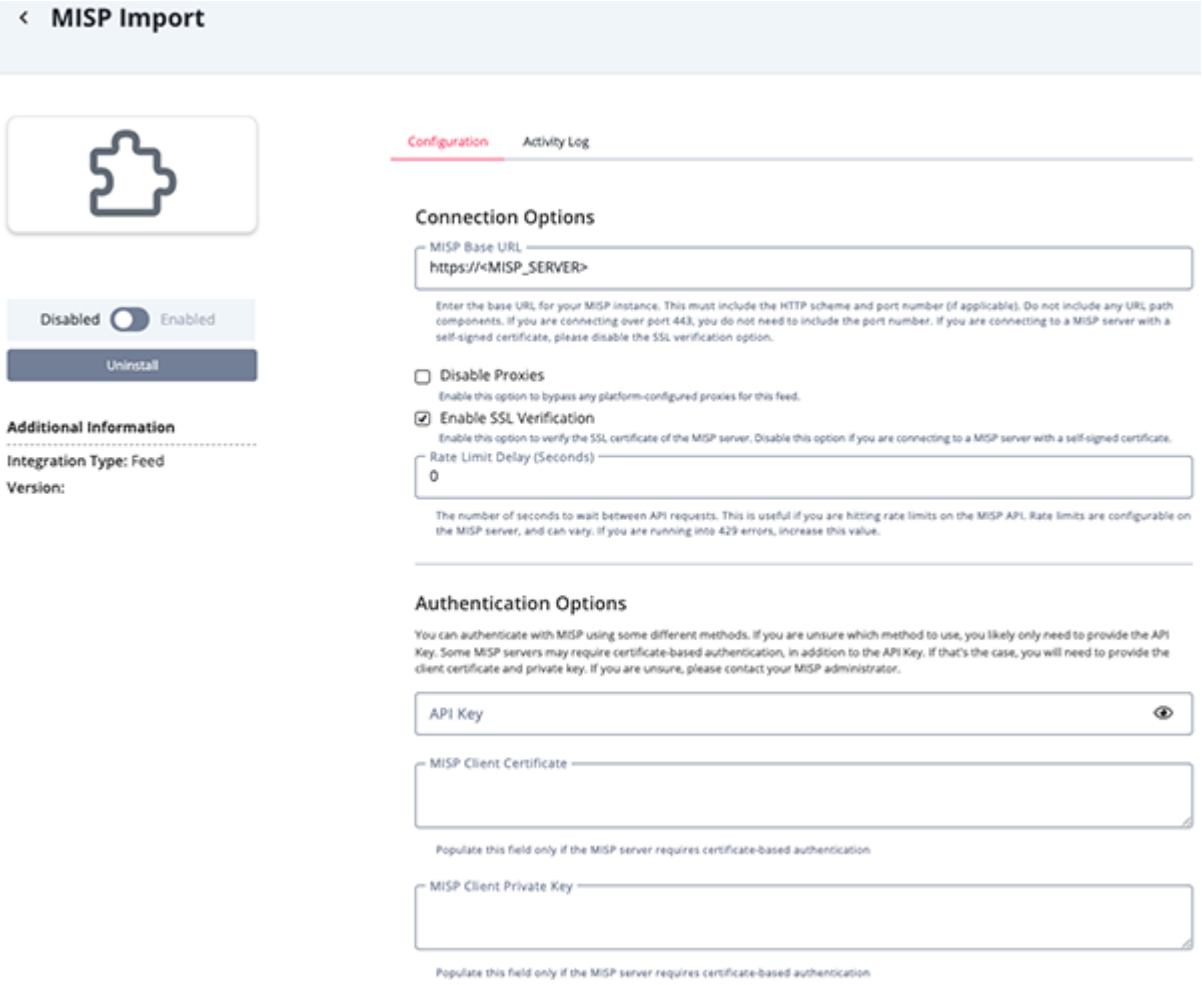
   If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

PARAMETER	DESCRIPTION
MISP Base URL	The MISP server instance domain name (or IP address) preceded by the protocol it uses, such as `https://my-misp-server.org`. The provided domain name or IP address must be reachable from the ThreatQ instance.
Disable Proxies	If enabled, specifies that this feed should not honor any proxies setup in ThreatQuotient. The default setting is **disabled**.
Enable SSL Verification	If enabled, specifies that this feed should verify SSL connections with the provider. The default setting is **enabled**.
Rate Limit Delay	The number of seconds to wait between API requests. This is useful if you are hitting rate limits on the MISP API. Rate limits are configurable on the MISP server, and can vary. Increase this value if you are running into 429 errors.

PARAMETER	DESCRIPTION
API Key	The MISP account API key.
MISP Client Certificate	Enter your MISP Client Certificate if the MISP server requires certificate-based authentication. Otherwise, leave this field blank.
MISP Client Private Key	Enter your MISP Client Private Key if the MISP server requires certificate-based authentication. Otherwise, leave this field blank.
Threat Level Filter	Select the Threat Levels to filter events. Option include: ◦ High (default) ◦ Medium (default) ◦ Low (default) ◦ Undefined (default)
Organization Filter	Optional - enter a line-separated list of organization names to filter events by. If left blank, all events will be imported. If populated, only events from the specified organizations will be imported. If both Organization and Community filters are populated, events that match **either** filter will be imported.
Community Filter	Optional - enter a line-separated list of community names to filter events by. If left blank, all events will be imported. If populated, only events from the specified communities will be imported. If both Organization and Community filters are populated, events that match **either** filter will be imported.
Only Import Published Events	Enable this option to only import events that are marked as published in MISP.
Inherited Context	Select the pieces of context to inherit from the event to the related IOCs. Options include: ◦ Related Malware

PARAMETER	DESCRIPTION
	◦ Related Adversaries ◦ Source Organization ◦ Member Organization ◦ ID ◦ MISP Threat Level ◦ Analysis ◦ Tags
Save Tags As	Select how to add Tags to the ThreatQ platform. Options include **Tags** and **Attributes**.



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.

ThreatQ Mapping

MISP Import

The MISP Import feed utilizes one of two event-search supplemental feeds — **MISP Import - Simple Auth - Event Search** or **MISP Import - SSL Auth - Event Search** — to retrieve MISP event metadata. Authentication behavior is determined by the **MISP Client Certificate** user field configuration. When a client certificate is provided, the integration authenticates with the MISP server using both the API key and the supplied client certificate. If the field is left empty, authentication is performed using the API key only.

This feed does not use a direct mapping configuration. Instead, it dynamically selects the appropriate supplemental feed based on the presence of the **MISP Client Certificate** user field, filters the returned event metadata, retrieves the associated event attributes and objects, and then parses the resulting MISP event data for ingestion into ThreatQ.

MISP Import - Simple Auth - Event Search, MISP Import - SSL Auth - Event Search (supplemental)

These feeds retrieve MISP event metadata. Only one of these feeds is used based on the authentication method.

```
POST {{user_fields.domain_name}}/events/restSearch
```

Sample Body:

```
{
  "returnFormat": "json",
  "metadata": 1,
  "timestamp": ["1739381040", "1778767884"],
  "tags": ["cobalt"],
  "limit": 100,
  "page": 1
}
```

> The `tags` field is included only when **Tag Filter** configuration parameter is populated. Each line in **Tag Filter** is sent as a separate tag value, and blank lines are ignored.

Sample Response:

```
{
  "response": [
    {
      "Event": {
        "id": "2068",
        "orgc_id": "1",
        "org_id": "1",
        "date": "2026-03-24",
        "threat_level_id": "1",
        "info": "Some Bad Indicators Alright",
        "published": false,
        "uuid": "70d28268-037d-42ec-977f-42e8bf4148ca",
        "attribute_count": "2",
        "analysis": "0",
        "timestamp": "1774383315",
        "distribution": "1",
        "proposal_email_lock": false,
        "locked": false,
        "publish_timestamp": "0",
        "sharing_group_id": "0",
        "disable_correlation": false,
        "extends_uuid": "",
        "protected": null,
        "event_creator_email": "admin@admin.test",
        "Org": {
          "id": "1",
          "name": "ThreatQuotient",
          "uuid": "8045797f-9dfd-4474-a3eb-9f153f5b860d",
          "local": true
        },
        "Orgc": {
          "id": "1",
          "name": "ThreatQuotient",
          "uuid": "8045797f-9dfd-4474-a3eb-9f153f5b860d",
          "local": true
        },
        "RelatedEvent": [],
        "Galaxy": [],
        "CryptographicKey": [],
        "Tag": [
          {
            "id": "2650",
            "name": "cobalt",
```

```
            "colour": "#ffffff",
            "exportable": true,
            "user_id": "0",
            "hide_tag": false,
            "numerical_value": null,
            "is_galaxy": false,
            "is_custom_galaxy": false,
            "local_only": false,
            "local": 1,
            "relationship_type": null
          }
        ]
      }
    }
  ]
}
```


There is no direct mapping for these feeds. The primary feed uses the returned metadata for threat level, publication status, organization, community, and tag filtering before fetching attributes and objects.

Attribute and Object Supplemental Feeds

After event metadata passes filtering, the primary feed retrieves the related attributes and objects with the following supplemental feeds:

MISP Import - Simple Auth - Get Attribute Count / MISP Import - SSL Auth - Get Attribute Count: `POST {{user_fields.domain_name}}/attributes/restSearch` with `returnFormat`: `count`, `eventid`, supported MISP attribute `type` values, and the current timestamp range.

MISP Import - Simple Auth - Get Attribute Data / MISP Import - SSL Auth - Get Attribute Data: `POST {{user_fields.domain_name}}/attributes/restSearch` with `returnFormat`: `json`, `eventid`, supported MISP attribute `type` values, page, limit, and the current timestamp range.

MISP Import - Simple Auth - Get Object by ID / MISP Import - SSL Auth - Get Object by ID: `{{user_fields.domain_name}}/objects/view/{{OBJECT_ID}}`. There is no direct mapping for these supplemental feeds.

There is no direct mapping for these supplemental feeds.

Composed Event Data Used for Mapping

Before reporting to ThreatQ, the primary feed composes the filtered event metadata with the fetched MISP attributes and objects. The mapping table below is based on this composed shape.

Sample Response (truncated):


```
{
  "response": [
    {
      "Event": {
        "id": "1",
        "orgc_id": "1",
        "org_id": "1",
        "date": "2018-12-14",
        "threat_level_id": "2",
        "info": "EVENT1",
        "published": false,
        "uuid": "5c142f52-5ad0-4c04-8069-03c8ac107221",
        "attribute_count": "4",
        "analysis": "1",
        "timestamp": "1545256410",
        "distribution": "1",
        "proposal_email_lock": false,
        "locked": false,
        "publish_timestamp": "1544827221",
        "sharing_group_id": "0",
        "disable_correlation": false,
        "extends_uuid": "",
        "event_creator_email": "admin@admin.test",
        "Org": {
          "id": "1",
          "name": "ORGNAME",
          "uuid": "5bd7a775-1d18-4fd7-b2f4-08b52dc69e54"
        },
        "Orgc": {
          "id": "1",
          "name": "ORGNAME",
          "uuid": "5bd7a775-1d18-4fd7-b2f4-08b52dc69e54"
        },
        "Attribute": [
          {
            "id": "1",
```

```
            "type": "link",
            "category": "Antivirus detection",
            "to_ids": false,
            "uuid": "5c17ccfe-3c1c-4f47-9a9f-38f6ac107221",
            "event_id": "1",
            "distribution": "3",
            "timestamp": "1545063678",
            "comment": "",
            "sharing_group_id": "0",
            "deleted": false,
            "disable_correlation": false,
            "object_id": "0",
            "object_relation": null,
            "value": "https://www.virustotal.com/#/file/
17a0d59255046ed2cff22cd5980fcc86c69e059839fe
            "Galaxy": [],
            "ShadowAttribute": []
          }
        ],
        "Object": [
          {
            "id": "1",
            "name": "file",
            "meta-category": "file",
            "description": "File object describing a file with meta-
information",
            "template_uuid": "688c46fb-5edb-40a3-8273-1af7923e2215",
            "template_version": "15",
            "event_id": "1",
            "uuid": "5c1abdda-4cb8-427c-97d5-71c9ac107221",
            "timestamp": "1545256410",
            "distribution": "5",
            "sharing_group_id": "0",
            "comment": "dnsrslvr.dll",
            "deleted": false,
            "ObjectReference": [],
            "Attribute": [
              {
                "id": "26131",
                "type": "md5",
                "category": "Payload delivery",
                "to_ids": true,
```

```
                "uuid": "5c1abdda-0960-4530-a4e4-71c9ac107221",
                "event_id": "1",
                "distribution": "5",
                "timestamp": "1545256410",
                "comment": "",
                "sharing_group_id": "0",
                "deleted": false,
                "disable_correlation": false,
                "object_id": "1",
                "object_relation": "md5",
                "value": "44d88612fea8a8f36de82e1278abb02f"
              }
            ]
          }
        ],
        "Galaxy": [
          {
            "id": "3",
            "uuid": "698774c7-8022-42c4-917f-8d6e4f06ada3",
            "name": "Threat Actor",
            "type": "threat-actor",
            "description": "Threat actors are characteristics of
malicious actors (or adversaries) r
            "version": "3",
            "icon": "user-secret",
            "namespace": "misp",
            "GalaxyCluster": [
              {
                "id": "5401",
                "collection_uuid": "7cdff317-
a673-4474-84ec-4f1754947823",
                "type": "threat-actor",
                "value": "Keyhole Panda",
                "tag_name": "misp-galaxy: threat-actor=\"Keyhole
Panda\"",
                "description": "no description",
                "galaxy_id": "3",
                "source": "MISP Project",
                "authors": [
                  "Alexandre Dulaunoy",
                  "Florian Roth",
                  "Thomas Schreck",
```

```
                "Timo Steffens",
                "Various"
              ],
              "version": "75",
              "uuid": "ad022538-b457-4839-8ebd-3fdcc807a820",
              "tag_id": "77",
              "meta": {
                "country": ["CN"],
                "synonyms": ["temp.bottle"]
              }
            }
          ]
        }
      ],
      "Tag": [
        {
          "id": "11",
          "name": "tlp:red",
          "colour": "#CC0033",
          "exportable": true,
          "user_id": "0",
          "hide_tag": false,
          "numerical_value": null
        }
      ]
    }
  }
]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response[].Event.info	Event.Title / Event.Description	MISP	.response[].Event.publish_timestamp	EVENT1	N/A
.response[].Event.date	Event.Happened At	N/A	N/A	2018-12-14T00:00:00	N/A
.response[].Event.Orgc.name	Event.Attribute / Related Indicator.Attribute	Source Organization	.response[].Event.publish_timestamp	ORGNAME	Attribute inherit by related indicators if Inherited Context includes Source Organization.
.response[].Event.Org.name	Event.Attribute / Related Indicator.Attribute	Member Organization	.response[].Event.publish_timestamp	ORGNAME	Attribute inherit by related indicators if Inherited Context includes Member Organization.
.response[].Event.id	Event.Attribute / Related Indicator.Attribute	ID	.response[].Event.publish_timestamp	1	Attribute inherit by related indicators if Inherited Context includes ID.
.response[].Event.uuid	Event.Attribute	UUID	.response[].Event.publish_timestamp	5c142f52-5ad0-4c04-8069-03c8ac107221	N/A
.response[].Event.threat_level_id	Event.Attribute / Related Indicator.Attribute	MISP Threat Level	.response[].Event.publish_timestamp	Medium	Maps an integer ID to a string based on the Threat Level Mapping below. If no match is found, this attribute is not ingested. Attribute inherit by related indicators if Inherited Context includes MISP Threat Level.
.response[].Event.analysis	Event.Attribute / Related Indicator.Attribute	Analysis	.response[].Event.publish_timestamp	Ongoing	Maps an integer ID to a string based on the Analysis Mapping below. If no match is found, this attribute is not ingested. Attribute inherit by related indicators if Inherited Context includes Analysis.
.response[].Event.distribution	Event.Attribute	Distribution	.response[].Event.publish_timestamp	This community only	Maps an integer ID to a string based on the Distribution Mapping below. If no match is found, this attribute is not ingested.
.response[].Event.sharing_group_id	Event.Attribute	Sharing Group	.response[].Event.publish_timestamp	0	N/A
.response[].Event.disable_correlation	Event.Attribute	Disable Correlation	.response[].Event.publish_timestamp	False	Title-cased

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response[].Event.id	Event.Attribute	External MISP	.response[].Event.publish_timestamp	{{user_fields.domain_name}}/events/view/1	Value created from the template: {{user_fields.domain_name}}/events/view/{{id}}
.response[].Event.Object[].Attribute[].value	Event.Attribute	YARA Rule Name	.response[].Event.publish_timestamp	My YARA Rule	Based on the jq expression: .response[].Event.Object[] | select(.name == "yara") | .Attribute[] | select(.type == "yara-rule-name") | .value
.response[].Event.Tag[].name	Event.Attribute / Related Indicator.Attribute	Tag	.response[].Event.publish_timestamp	tlp:red	If Attributes in Save Tags As
.response[].Event.Tag[].name	Event.TLP / Related Indicator.TLP	N/A	N/A	RED	TLP value is extracted from MISP tags whose name starts with either tlp: or iep:traffic-light-protocol=.
.response[].Event.Tag[].name	Event.Tag / Related Indicator.Tag	N/A	N/A	DDoS	Tags are extracted from MISP if name starts with: ms-caro-malware:, ecsirt:, veris:, circl:, europol-event:, malware_classification:, enisa:. If Inherited Context includes Tags and Tags in Save Tags As
.response[].Event.Attribute[].value	Event.Attribute	Category	.response[].Event.publish_timestamp	https://www.virustotal.com/#/file/17a0d59255046ed2cff22cd5980fcc86c69e059839fec07d705051ac2e178693/details	Based on the jq expression: .response[].Event.Attribute[] | select(.type == "link") | .value
.response[].Event.Attribute[].value	Event.Attribute	Comment	.response[].Event.publish_timestamp	sample comment	Based on the jq expression: .response[].Event.Attribute[] | select(.type == "comment") | .value
.response[].Event.Attribute[].value	Related Indicator.Value	The indicator's type is derived from .response[].Event.Attribute[].type (see MISP Attribute Type to ThreatQ Indicator Type Mapping below)	.response[].Event.Attribute[].timestamp	bunnyhop.exe	31f3720bef6bb3e2953d9ea2238e0580 (creates two indicators: the Filename bunnyhop.exe and the MD5 31f3720bef6bb3e2953d9ea2238e0580)
.response[].Event.Attribute[].category	Related Indicator.Attribute	Category	.response[].Event.Attribute[].timestamp	Payload installation	N/A
.response[].Event.Attribute[].to_ids	Related Indicator.Attribute	To IDS	.response[].Event.Attribute[].timestamp	False	Title-cased

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response[].Event.Attribute[].distribution	Related Indicator.Attribute	Distribution	.response[].Event.Attribute[].timestamp	All communities	Maps an integer ID to a string based on the Attribute Distribution Mapping below. If no match is found, this attribute is not ingested.
.response[].Event.Attribute[].timestamp	Related Indicator.Attribute	Timestamp	.response[].Event.Attribute[].timestamp	2019-04-08 09:27:58-00:00	N/A
.response[].Event.Attribute[].comment	Related Indicator.Attribute	Comment	.response[].Event.Attribute[].timestamp	sample comment	This attribute is created only if the comment does not contain the substring "Pertinence".
.response[].Event.Attribute[].comment	Related Indicator.Attribute	Pertinence	.response[].Event.Attribute[].timestamp	sample comment	This attribute is created only if "Pertinence" appears in the comment value. The attribute's value is the text after "Pertinence:".
.response[].Event.Attribute[].sharing_group_id	Related Indicator.Attribute	Sharing Group	.response[].Event.Attribute[].timestamp	0	N/A
.response[].Event.Attribute[].deleted	Related Indicator.Attribute	Deleted	.response[].Event.Attribute[].timestamp	False	Title-cased
.response[].Event.Attribute[].disable_correlation	Related Indicator.Attribute	Disable Correlation	.response[].Event.Attribute[].timestamp	False	Title-cased
.response[].Event.Attribute[].object_relation	Related Indicator.Attribute	Object Relation	.response[].Event.Attribute[].timestamp	N/A	Title-cased
.response[].Event.Attribute[].Tag[].name	Related Indicator.Attribute	Tag	.response[].Event.Attribute[].timestamp	N/A	N/A
.response[].Event.Attribute[].type	Related Indicator.Attribute	IP Type	.response[].Event.Attribute[].timestamp	ip-dst	The attribute value is "ip-dst" if "ip-dst" is in the type value. Else, the attribute value is "ip-src" if "ip-src" is in the type value. If neither of the aforementioned cases are true, this attribute is not created.
.response[].Event.Object[].Attribute[].value	Related Indicator.Value	The indicator's type is derived from .response[].Event.Object[].Attribute[].type (see MISP Attribute Type to ThreatQ	N/A	44d88612fea8a8f36de82e1278abb02f	All indicators created from a MISP Object's Attributes are inter-related. Only applicable if .response[].Event.Object[].Attribute[].type has a match in the MISP Attribute Type to

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
		Indicator Type Mapping below)			ThreatQ Indicator Type Mapping below.
.response[].Event.Object[].Attribute[].category	Related Indicator.Attribute	Category	N/A	Payload delivery	N/A
.response[].Event.Object[].Attribute[].to_ids	Related Indicator.Attribute	To IDS	N/A	False	Title-cased
.response[].Event.Object[].Attribute[].distribution	Related Indicator.Attribute	Distribution	N/A	All communities	Maps an integer ID to a string based on the Attribute Distribution Mapping below. If no match is found, this attribute is not ingested.
.response[].Event.Object[].Attribute[].sharing_group_id	Related Indicator.Attribute	Sharing Group	N/A	0	N/A
.response[].Event.Object[].Attribute[].comment	Related Indicator.Attribute	Comment	N/A	sample comment	N/A
.response[].Event.Object[].Attribute[].type	Related Indicator.Attribute	IP Type	N/A	ip-dst	The attribute value is "ip-dst" if "ip-dst" is in the type value. Else, the attribute value is "ip-src" if "ip-src" is in the type value. If neither of the aforementioned cases are true, this attribute is not created.
.response[].Event.Galaxy[].GalaxyCluster[].value / .response[].Event.Galaxy[].GalaxyCluster[].meta.synonyms[]	Related Indicator.Attribute	Related Adversary	N/A	Keyhole Panda	If Inherited Context includes Related Adversaries.
.response[].Event.Galaxy[].GalaxyCluster[].value	Related Indicator.Attribute	Malware Family	N/A	Pegasus	If Inherited Context includes Related Malware.
.response[].Event.Attribute[].value	Related Attachment.Name / Related Attachment.Title	MISP Attachment	.response[].Event.Attribute[].timestamp	sample.pdf	Based on the jq expression: .response[].Event.Attribute[] | select(.type == "attachment") | .value

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response[].Event.Attribute[].data	Related Attachment.Content	N/A	N/A	JVBERi0xLjMNCiXi48TDQoNCjEgMCBvYmo8DQovVHlwZS...	N/A
.response[].Event.Attribute[].id	Related Attachment.Attribute	ID	.response[].Event.Attribute[].timestamp	477506	N/A
.response[].Event.Attribute[].category	Related Attachment.Attribute	Category	.response[].Event.Attribute[].timestamp	Payload delivery	N/A
.response[].Event.Attribute[].to_ids	Related Attachment.Attribute	To IDS	.response[].Event.Attribute[].timestamp	True	Title-cased
.response[].Event.Attribute[].uuid	Related Attachment.Attribute	UUID	.response[].Event.Attribute[].timestamp	5dde5554-6320-4647-baa8-26d3ac107221	N/A
.response[].Event.Attribute[].distribution	Related Attachment.Attribute	Distribution	.response[].Event.Attribute[].timestamp	All communities	Maps an integer ID to a string based on the Attribute Distribution Mapping below. If no match is found, this attribute is not ingested.
.response[].Event.Attribute[].comment	Related Attachment.Attribute	Comment	.response[].Event.Attribute[].timestamp	sample comment	N/A
.response[].Event.Attribute[].sharing_group_id	Related Attachment.Attribute	Sharing Group	.response[].Event.Attribute[].timestamp	0	N/A
.response[].Event.Attribute[].deleted	Related Attachment.Attribute	Deleted	.response[].Event.Attribute[].timestamp	False	Title-cased
.response[].Event.Attribute[].disable_correlation	Related Attachment.Attribute	Disable Correlation	.response[].Event.Attribute[].timestamp	False	Title-cased
.response[].Event.Attribute[].value	Related Signature.Value	YARA	N/A	import "pe"\n\nrule OceanLotus_Steganography_Loader {\n\n\tmeta:...	Based on the jq expression: .response[].Event.Attribute[] | select(.type == "yara") | .value. Unicode characters "LEFT DOUBLE QUOTATION MARK" (\u201c) and "RIGHT DOUBLE QUOTATION MARK" (\u201d) are normalized to ASCII double quotations ("). Unicode character "HYPHEN" (\u2010) is normalized to the ASCII hyphen (-).

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response[].Event.Attribute[].value	Related Signature.Name	N/A	N/A	OceanLotus_Steganography_Loader	Rule name extracted from the YARA parser.
.response[].Event.Object[].Attribute[].value	Related Signature.Value	YARA	N/A	rule Contains_VBA_macro_code {\n\n\tmeta:...	Based on the jq expression: .response[].Event.Object[] | select(.name == "yara") | .Attribute[] | select(.type == "yara") | .value. Unicode characters "LEFT DOUBLE QUOTATION MARK" (\u201c) and "RIGHT DOUBLE QUOTATION MARK" (\u201d) are normalized to ASCII double quotations ("). Unicode character "HYPHEN" (\u2010) is normalized to the ASCII hyphen (-).
.response[].Event.Object[].Attribute[].value	Related Signature.Name	N/A	N/A	Contains_VBA_macro_code	Rule name extracted from the YARA parser.
.response[].Event.Attribute[].value	Related Signature.Value	Snort	N/A	alert tcp $HOME_NET any -> any 3306 (msg: \"mysql general_log write file\"; ...)	Based on the jq expression: .response[].Event.Attribute[] | select(.type == "snort") | .value. Unicode characters "LEFT DOUBLE QUOTATION MARK" (\u201c) and "RIGHT DOUBLE QUOTATION MARK" (\u201d) are normalized to ASCII double quotations ("). Unicode character "HYPHEN" (\u2010) is normalized to the ASCII hyphen (-).
.response[].Event.Attribute[].value	Related Signature.Name	N/A	N/A	mysql general_log write file	Name extracted from Snort msg option if available; else, defaults to "Snort Rule". Leading or trailing whitespace is trimmed.
.response[].Event.Object[].Attribute[].value	Related Signature.Value	Snort	N/A	alert tcp $HOME_NET any -> any 3306 (msg: \"mysql general_log write file\"; ...)	Based on the jq expression: .response[].Event.Object[] | select(.name == "suricata") | .Attribute[] | select(.type == "snort") | .value. Unicode characters "LEFT DOUBLE QUOTATION MARK" (\u201c) and "RIGHT DOUBLE QUOTATION MARK" (\u201d) are normalized to ASCII double quotations ("). Unicode character "HYPHEN" (\u2010) is normalized to the ASCII hyphen (-).

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response[].Event.Object[].Attribute[].value	Related Signature.Name	N/A	N/A	mysql general_log write file	Name extracted from Snort msg option if available; else, defaults to "Snort Rule". Leading or trailing whitespace is trimmed.
.response[].Event.Galaxy[].GalaxyCluster[].value / .response[].Event.Galaxy[].GalaxyCluster[].meta.synonyms[]	Related Adversary.Name	N/A	N/A	Keyhole Panda, temp.bottle	Based on the jq expression: .response[].Event.Galaxy[] | select(.type == "threat-actor") | (.GalaxyCluster[].value, .GalaxyCluster[].meta.synonyms[])
.response[].Event.Galaxy[].GalaxyCluster[].id	Related Adversary.Attribute	ID	N/A	5401	N/A
.response[].Event.Galaxy[].GalaxyCluster[].type	Related Adversary.Attribute	Type	N/A	threat-actor	N/A
.response[].Event.Galaxy[].GalaxyCluster[].description	Related Adversary.Attribute	Description	N/A	no description	N/A
.response[].Event.Galaxy[].GalaxyCluster[].galaxy_id	Related Adversary.Attribute	Galaxy ID	N/A	3	N/A
.response[].Event.Galaxy[].GalaxyCluster[].version	Related Adversary.Attribute	Version	N/A	75	N/A
.response[].Event.Galaxy[].GalaxyCluster[].tag_id	Related Adversary.Attribute	Tag ID	N/A	77	N/A
.response[].Event.Galaxy[].GalaxyCluster[].meta."cfr-suspected-state-sponsor"[]	Related Adversary.Attribute	Suspected State Sponsor	N/A	China	N/A
.response[].Event.Galaxy[].GalaxyCluster[].meta."cfr-	Related Adversary.Attribute	Suspected Victims	N/A	Japan	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
suspected-victims"[]					
.response[].Event.Galaxy[].GalaxyCluster[].meta."cfr-target-category"[]	Related Adversary.Attribute	Target Category	N/A	Private sector	N/A
.response[].Event.Galaxy[].GalaxyCluster[].meta."cfr-type-of-incident"[]	Related Adversary.Attribute	Type of Incident	N/A	Espionage	N/A
.response[].Event.Galaxy[].GalaxyCluster[].meta.country[]	Related Adversary.Attribute	Country	N/A	CN	N/A
.response[].Event.Galaxy[].GalaxyCluster[].meta.refs[]	Related Adversary.Attribute	References	N/A	http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf	N/A
.response[].Event.Galaxy[].GalaxyCluster[].value	Related Adversary.Name / Related Attack Pattern.Value / Related Course of Action.Value / Related Malware.Value / Related Tool.Value	N/A	N/A	N/A	Attempts to map .response[].Event.Galaxy[].GalaxyCluster[].type to a ThreatQ Object Type based on the MISP Galaxy Cluster Type to ThreatQ Object Type Mapping below.

Threat Level Mapping

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

Distribution Mapping

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

Attribute Distribution Mapping

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

Analysis Mapping

MISP ANALYSIS ID	THREATQ ATTRIBUTE VALUE
0	Initial
1	Ongoing
2	Completed

MISP Attribute Type to ThreatQ Indicator Type Mapping

MISP ATTRIBUTE TYPE	THREATQ INDICATOR TYPE
md5	MD5
sha1	SHA-1
sha256	SHA-256
sha384	SHA-384
sha512	SHA-512
filename	Filename
ip	IP Address
ip-src	IP Address
ip-dst	IP Address
hostname	FQDN
domain	FQDN
email-subject	Email Subject
email-attachment	Email Attachment
email-src	Email Address
email-x-mailer	X-Mailer

MISP ATTRIBUTE TYPE	THREATQ INDICATOR TYPE
ssdeep	Fuzzy Hash
regkey	Registry Key
user-agent	User-Agent
mutex	Mutex
url	URL
vulnerability	CVE
uri	URL Path

MISP Galaxy Cluster Type to ThreatQ Object Type Mapping

MISP GALAXY CLUSTER TYPE	THREATQ OBJECT TYPE
mitre-mobile-attack-malware	Malware
mitre-enterprise-attack-malware	Malware
mitre-malware	Malware
mitre-enterprise-attack-tool	Tool
mitre-mobile-attack-tool	Tool
mitre-tool	Tool
mitre-enterprise-attack-course-of-action	Course of Action
mitre-mobile-attack-course-of-action	Course of Action
mitre-course-of-action	Course of Action
mitre-pre-attack-intrusion-set	Adversary
mitre-intrusion-set	Adversary
mitre-enterprise-attack-intrusion-set	Adversary
mitre-mobile-attack-intrusion-set	Adversary
mitre-enterprise-attack-attack-pattern	Attack Pattern
mitre-attack-pattern	Attack Pattern

MISP GALAXY CLUSTER TYPE	THREATQ OBJECT TYPE
mitre-mobile-attack-attack-pattern	Attack Pattern
mitre-pre-attack-attack-pattern	Attack Pattern

Average Feed Run

MISP server instances vary widely in their setup and the data stored within them. Due to this, average feed run results cannot be confidently provided.

Known Issues / Limitations

- Authentication - users should not mix authentication methods when configuring the integration. The MISP Client Certificate and MISP Client Private Key configuration fields should only be used if required by the MISP server.
- MISP does not verify whether a Snort or YARA rule entered into it is valid. However, the Snort and YARA parsers used by this feed depend on the Snort or YARA rules being well-formed. Please refer to the following non-comprehensive list to aid in making sure that the Snort or YARA rules stored in your MISP server instance are valid so that they can be properly ingested by this feed.
- Snort:
  - Each rule option must be terminated with a semicolon (`;`).
  - Offending Snort rule: `alert tcp $HOME_NET any -> $EXTERNAL_NET [80,443,8080,7080,21,50000,995](msg:"BDS MALICIOUS Emotet Worming Traffic Likely";content:"d29ybSBzdGFydGVk";content:"POST";http_method;classtype:spreader;sid:7;rev:1)`
    - Correction needed: `rev:1` should be `rev:1;`
  - Rule option values must be valid. For instance, options like `rev`, `sid`, and `gid` must have base 10 integers as their value.
  - Offending Snort option: `sid:#########;`
    - Correction needed: Either remove `sid` if the value is not known or replace the value with a valid ID, like `sid:7;`.
  - The value of the `snort` MISP attribute must contain at least one entire Snort rule. Multiple Snort rules can be provided in a single value if separated by newlines. The value must not contain any excess text, such as a header like `Snort rule:`.
- YARA:
  - The value of the `yara` MISP attribute must contain at least one entire YARA rule. Multiple YARA rules can be provided in a single value if separated by newlines. The value must not contain any excess text, such as a header like `YARA rule:`.
  - Make sure that any text that is not valid YARA syntax is either removed or commented out.

Change Log

- **Version 2.5.0**
  - Added support for wildcard filtering in the **Organization** and **Community** configuration parameter filters.
  - Added support for tag-based filtering when searching for MISP events to ingest.
  - Removed the Query Filter Characteristics configuration parameter.
- **Version 2.4.1**
  - Resolved a `Threat Level` ingestion issue caused by a provider API update in which this data was returned as an integer opposed to a string.
- **Version 2.4.0**
  - Added new configuration parameters:
    - **Organization Filter** - filter out events based on the organization that published it.
    - **Community Filter** - filter out events based on the community that published it.
    - **Only Import Published Events** - filter out events based on whether or not they are published.
    - **Threat Level Filter** - filter out events based on their threat level.
  - Reorganized user field interface order to improve consistency.
- **Version 2.3.2**
  - Added the ability to select how Tags are ingested via a new configuration parameter: **Save Tags As**.
  - Added two new certificate configuration parameters:
    - **MISP Client Certificate**
    - **MISP Client Private Key**
  - Added events pagination improvements.
  - Added new **Known Issue / Limitation** entry in the user guide regarding authentication - users should only use the MISP Client Certificate and Private Key fields if required by the MISP server.
- **Version 2.3.1**

- Resolved an issue where uploading attachments with empty attributes would cause an error.
- Updated minimum ThreatQ version to 5.20.0

- **Version 2.3.0**
  - Added the ability to inherit meaningful event attributes and related indicators. See the **Inherited Context** parameter in the Configuration chapter for more details.
  - Fixed parsing of YARA and Snort rules that contain unicode special space separators.
  - Removed inter-relation of domains from the **domain-ip** object types.
  - Removed the **Save Intrusion Sets As** parameter.
  - Updated **MISP Galaxy Cluster Type to ThreatQ Object Type Mapping** table**.**
  - Updated minimum ThreatQ version to 5.19.0
- **Version 2.2.0**
  - Added new configuration option, **Inherited Context**, to inherit context from top-level events to related IOCs.
  - Added new configuration option, **Rate Limit Delay**, to set a delay to prevent rate limiting (429 errors).
- **Version 2.1.5**
  - Updated the python implementation of the MISP filter to improve feed efficiency.
  - Updated the minimum ThreatQ version to 4.50.0.
- **Version 2.1.4**
  - Removed the **Use the Event Data as Query Parameter** UI configuration parameter.
  - Added new UI configuration parameter: **Query Filter Characteristics**. Time constrained data fetching for both schedule and manual runs are now user configurable via this new field.
- **Version 2.1.3**
  - Added new configuration parameter - **Use Event Date as Query Parameter**.
  - Performed updates on time constrained data fetching for both scheduled and manual runs. **Scheduled Runs** retrieve MISP events and event attributes from events that have received a modification using the start date only. **Manual Runs** can retrieve MISP events and attributes using the start date only or the start and end dates depending on configuration options. See the

Use the Event Date as Query Parameter option in the Configuration chapter of this guide.

- **Version 2.1.2**
  - Updated the timing query parameters used for pulling data.
- **Version 2.1.1**
  - Added the ability to Normalize more Unicode quotations and hyphens
  - Add the ability to parse the YARA Rule Name ThreatQ Event Attribute from MISP Object Attributes that contain the key-value pair `object_relation: "yara-rule-name"` in addition to the parsing logic added in 2.1.0, in which the YARA Rule Name ThreatQ Attribute is parsed from MISP Object Attributes that contain the key-value pair `type: "yara-rule-name"`
- **Version 2.1.0**
  - Normalized Unicode double quotations to ASCII double quotations in YARA and Snort signature values
  - Normalized Unicode hyphens to ASCII hyphens in YARA and Snort signature values
  - Adjusted logic used to derive a YARA rule from MISP Object Attributes. Previously, the logic depended on a MISP YARA Object having both `yara` and `yara-rule-name` attributes, in which it derived a YARA rule based on the template `rule {{yara_rule_name}} {{yara}}` before passing the derived rule through the YARA parser. This was not often seen in the wild; the MISP `yara` attribute usually contains the entire YARA rule. Even the documentation for the MISP YARA Object suggests that these attributes be used in a mutually exclusive manner: use the `yara` attribute if the user has the entire YARA rule to provide to MISP; else, reference a YARA rule using the `yara-rule-name` attribute. As a result, the following changes are in this version of the CDF:
    - Ingest the `yara-rule-name` MISP Object Attribute as a ThreatQ Attribute of the MISP Event object
    - Ingest the `yara` MISP Object Attribute as a ThreatQ YARA Signature
  - Parse MISP Suricata Objects in order to ingest its Snort Object Attributes as ThreatQ Snort Signatures.
  - Although well-formed Snort rules should contain a `msg` option, which is used to derive the ThreatQ Snort Signature's Name, account for a Snort rule not containing a `msg` option by defaulting the ThreatQ Snort Signature's Name to "Snort Rule".
- **Version 2.0.0**

  - Add configuration parameter "Enable SSL Verification"
  - Change behavior of scheduled feed runs such that it only fetches data published within the last day
  - Add support for parsing MISP YARA Objects
  - Add support for parsing MISP Snort Attributes
  - Add additional key-value pairs to the MISP Galaxy Cluster Type to ThreatQ Object Type Mapping
  - Change the value of `happened_at` for ingested events by using `date` instead of `timestamp`

- **Version 1.0.4**
  - Ingest MISP Attachment Attributes as ThreatQ Attachments
- **Version 1.0.3**
  - Add configuration parameter "Disable Proxies"
- **Version 1.0.0**
  - Initial release