

ThreatQuotient



MISP Connector Implementation Guide

Version 1.0.1

Monday, October 14, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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 © 2019 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.

Last Updated: Monday, October 14, 2019

Contents

MISP Connector Implementation Guide	1
Warning and Disclaimer	2
Contents	4
Versioning	5
Introduction	5
MISP Trimmed Sample	5
Installation	13
ThreatQ Mapping	14
Change Log	31

Versioning

- Current integration version: 1.0.1
- Supported on ThreatQ versions: 4.21.0 or higher

Introduction

The MISP feed retrieves data from a user configurable MISP instance, using the following endpoint: `http://{{user_fields.domain_name}}/events/restSearch`.

- The API uses HTTP api key based authentication.
- Requests are made one page at a time (JSON responses).
- Time constrained events fetching is possible.



MITRE feeds need to run prior to running the MISP feed.

MISP Trimmed Sample

JSON

```
{
  "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.virus-
total.-
com/#/-
file/17a0d59255046ed2cfff22cd5980fc-
c86c69e059839fec07d705051ac2e178693/details",
        "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": "dnssrslvr.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":"44d88612fea8a8f36de82e1278ab-
b02f"
    }
]
}
],
"Galaxy":[
    {
        "id":"3",
        "uuid":"698774c7-8022-42c4-917f-
8d6e4f06ada3",
        "name":"Threat Actor",
        "type":"threat-actor",
        "description":"Threat actors are char-
acteristics of malicious actors (or adversaries) representing
a cyber attack threat including presumed intent and his-
torically observed behaviour.",
        "version":"3",
        "icon":"user-secret",
        "namespace":"misp",
        "GalaxyCluster":[
            {
                "id":"5401",
                "collection_uuid":"7cdf317-a673-4474-
84ec-4f1754947823",
```

```
        "type": "threat-actor",
        "value": "Keyhole Panda",
        "tag_name": "misp-galaxy:threat-act-
or=\"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-3fd-
cc807a820",
        "tag_id": "77",
        "meta": {
            "country": [
                "CN"
            ],
            "synonyms": [
                "temp.bottle"
            ]
        }
    }
]
```

```
{
  "id": "4",
  "uuid": "1fb6d5b4-1708-11e8-9836-8bbc8ce6866e",
  "name": "Pre Attack - Intrusion Set",
  "type": "mitre-pre-attack-intrusion-set",
  "description": "Name of ATT&CK Group",
  "version": "4",
  "icon": "user-secret",
  "namespace": "mitre-attack",
  "GalaxyCluster": [
    {
      "id": "5614",
      "collection_uuid": "1fdc8fa2-1708-11e8-99a3-67b4efc13c4f",
      "type": "mitre-pre-attack-intrusion-set",
      "value": "APT16 - G0023",
      "tag_name": "misp-galaxy:mitre-pre-attack-intrusion-set=\"APT16 - G0023\"",
      "description": "APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. (Citation: FireEye EPS Awakens Part 2)",
      "galaxy_id": "4",
      "source": "https://github.com/mitre/cti",
      "authors": [
        "MITRE"
      ]
    }
  ]
}
```

```
    ],
    "version": "6",
    "uuid": "d6e88e18-81e8-4709-82d8-
973095da1e70",
    "tag_id": "97",
    "meta": {
        "external_id": [
            "G0023"
        ],
        "refs": [
            "https://at-
tack.mitre.org/wiki/Group/G0023",
            "https://www.fireeye.com/blog/threat-
research/2015/12/the-eps-awakens-part-two.html"
        ],
        "synonyms": [
            "APT16"
        ]
    }
}
],
"Tag": [
    {
        "id": "11",
        "name": "tlp:red",
        "colour": "#CC0033",
```

```
        "exportable":true,  
        "user_id":"0",  
        "hide_tag":false,  
        "numerical_value":null  
      }  
    ]  
  }  
}  
]
```

Installation

Complete the following steps to install the connector:

1. Login to <https://download.threatq.com/integrations/>.
2. Download the **misp.yaml** file.
3. From the ThreatQ user interface, select the **Settings icon > Incoming Feeds**.
4. Click **Add New Feed**.
5. In the **Add New Feed** dialog box, complete one of the following actions:
 - Drag and drop the yaml file into the dialog box.
 - **Click to browse** to the yaml file and select it.

The connector installs as a feed on **OSINT** tab.

6. Under MISP, click **Feed Settings**.
7. For **MISP Domain Name**, enter the MISP instance domain.

8. For **Authorization**, enter the MISP account API key.
9. Click the toggle button next to MISP to enable the feed.
10. Click **Save Changes**.

ThreatQ Mapping

threat level map

```
'1': High  
'2': Medium  
'3': Low  
'4': Undefined
```

distribution map

```
'0': Your organization only  
'1': This community only  
'2': Connected communities  
'3': All communities  
'4': Sharing Group
```

attribute distribution map

```
'0': Your organization only  
'1': This community only  
'2': Connected communities  
'3': All communities  
'4': Sharing Group  
'5': Inherit event
```

analysis map

```
'0': Initial  
'1': Ongoing  
'2': Completed
```

indicator type map

```
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  
ssdeep: Fuzzy Hash  
regkey: Registry Key  
user-agent: User-Agent  
mutex: Mutex  
url: URL  
vulnerability: CVE  
uri: URL Path
```

taxonomy map

```
veris:action:malware:variety="Adware": Adware
malware_classification:malware-category="Adware": Adware
ms-caro-malware:malware-type="Adware": Adware
ecsirt:intrusion-attempts="brute-force": Brute Force
veris:action:malware:variety="Brute force": Brute Force
europol-event:brute-force-attempt: Brute Force
enisa:nefarious-activity-abuse="brute-force": Brute Force
ecsirt:availability="ddos": DDoS
europol-incident:availability="dos-ddos": DDoS
ms-caro-malware:malware-type="DDoS": DDoS
circl:incident-classification="denial-of-service": DDoS
enisa:nefarious-activity-abuse="denial-of-service": DDoS
veris:action:malware:variety="Downloader": Downloader
malware_classification:malware-category="Downloader": Down-
loader
Remote Access Tool: Downloader
enisa:nefarious-activity-abuse="remote-access-tool": Down-
loader
ms-caro-malware:malware-type="RemoteAccess": Downloader
circl:incident-classification="sql-injection": SQLi
veris:action:malware:variety="SQL injection": SQLi
veris:action:hacking:variety="SQLi": SQLi
enisa:nefarious-activity-abuse="web-application-attacks-injec-
tion-attacks-code-injection-SQL-XSS": SQLi
europol-event:sql-injection: SQLi
veris:action:malware:variety="Spyware/Keylogger": Spyware
malware_classification:malware-category="Spyware": Spyware
ms-caro-malware:malware-type="Spyware": Spyware
enisa:nefarious-activity-abuse="spyware-or-deceptive-adware":
```


Spyware

```
malware_classification:malware-category="Trojan": Trojan
ms-caro-malware:malware-type="Trojan": Trojan
ecsirt:malicious-code="trojan": Trojan
malware_classification:malware-category="Virus": Virus
ms-caro-malware:malware-type="Virus": Virus
ecsirt:malicious-code="virus": Virus
veris:action:malware:variety="Worm": Worm
malware_classification:malware-category="Worm": Worm
ms-caro-malware:malware-type="Worm": Worm
ecsirt:malicious-code="worm": Worm
ecsirt:intrusions="backdoor": Backdoor
veris:action:malware:variety="Backdoor": Backdoor
ms-caro-malware:malware-type="Backdoor": Backdoor
ecsirt:malicious-code="c&c": C&C
europol-incident:malware="c&c": C&C
europol-event:c&c-server-hosting: C&C
veris:action:malware:variety="C2": C&C
veris:action:malware:variety="Exploit vuln": Exploit
ecsirt:intrusion-attempts="exploit": Exploit
europol-event:exploit: Exploit
europol-incident:intrusion="exploitation-vulnerability":
Exploit
ms-caro-malware:malware-type="Exploit": Exploit
ecsirt:malicious-code="malware": Malware
circl:incident-classification="malware": Malware
circl:incident-classification="phishing": Phishing
ecsirt:fraud="phishing": Phishing
veris:action:social:variety="Phishing": Phishing
```

```
europol-incident:information-gathering="phishing": Phishing
enisa:nefarious-activity-abuse="phishing-attacks": Phishing
ecsirt:malicious-code="ransomware": Ransomware
enisa:nefarious-activity-abuse="ransomware": Ransomware
malware_classification:malware-category="Ransomware": Ransom-
ware
ms-caro-malware:malware-type="Ransom": Ransomware
veris:action:malware:variety="Ransomware": Ransomware
veris:action:malware:variety="Rootkit": Rootkit
enisa:nefarious-activity-abuse="rootkits": Rootkit
malware_classification:malware-category="Rootkit": Rootkit
circl:incident-classification="scan": Scan
ecsirt:information-gathering="scanner": Scan
europol-incident:information-gathering="scanning": Scan
veris:action:malware:variety="Scan network": Scan Network
europol-event:network-scanning: Scan Network
circl:incident-classification="spam": Spam
ecsirt:abusive-content="spam": Spam
enisa:nefarious-activity-abuse="spam": Spam
europol-event:spam: Spam
europol-incident:abusive-content="spam": Spam
veris:action:malware:variety="Spam": Spam
veris:action:social:variety="Spam": Spam
tlp:amber: TLP-Amber
iep:traffic-light-protocol="AMBER": TLP-Amber
tlp:green: TLP-Green
iep:traffic-light-protocol="GREEN": TLP-Green
tlp:red: TLP-Red
iep:traffic-light-protocol="RED": TLP-Red
```

```
tlp:white: TLP-White
iep:traffic-light-protocol="WHITE": TLP-White
circl:incident-classification="XSS": XSS
europol-event:xss: XSS
```

mitre_object_types_list

```
mitre-mobile-attack-malware: malware
mitre-enterprise-attack-malware: malware
mitre-enterprise-attack-tool: tool
mitre-mobile-attack-tool: tool
mitre-enterprise-attack-course-of-action: course
mitre-mobile-attack-course-of-action: course
mitre-pre-attack-intrusion-set: course
mitre-enterprise-attack-intrusion-set: intrusion
mitre-mobile-attack-intrusion-set: intrusion
mitre-enterprise-attack-attack-pattern: pattern
mitre-mobile-attack-attack-pattern: pattern
mitre-pre-attack-attack-pattern: pattern
```

ThreatQ provides the following default mapping for the connector:

Feed Data Path (response. Event)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.info	event. title	Title	.publish_ timestam- p	"info": "EVENT1"	

Feed Data Path (response. Event)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.Orgc.name	event.attribute	Source Organization	.publish_timestamp	"Orgc": { "name": "ORGNAM-E", ... }	
.Org.name	event.attribute	Member Organization	.publish_timestamp	"Org": { "name": "ORGNAM-E", ... }	
.id	event.attribute	ID	.publish_timestamp	"id": "1"	
.uuid	event.attribute	UUID	.publish_timestamp	"uuid": "5c142f52-5ad0-4c04-806903c8ac107221"	
.threat_level_id	event.attribute	MISP Threat Level	.publish_timestamp	"threat_level_id": "2"	threat level map

Feed Data Path (response. Event)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.info	event. attribute	Description	.publish_ timestam- p	"info": "EVENT1"	
.timestam- p	event. happene- d_ at	Event Timestamp	.publish_ timestam- p	"timestamp": "154525641- 0"	formatted
.publish_ timestamp	event. attribute	Published At	.publish_ timestam- p	"publish_ timestamp": "154482722- 1"	formatted
.analysis	event. attribute	Analysis	.publish_ timestam- p	"analysis": "1"	analysis map
.dis- tribution	event. attribute	Distribution	.publish_ timestam- p	"dis- tribution": "1"	dis- tribution map
.sharing_ group_id	event. attribute	Sharing Group	.publish_ timestam- p	"sharing_ group_ id": "0"	

Feed Data Path (response.Event)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.disable_correlation	event.attribute	Disable Correlation	.publish_timestamp	"disable_correlation": false	

Feed Data Path (response.Event.Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.type	indicator.type	Type	.timestamp	"type": "filename"	link
.value	indicator.value	Value	.timestamp	"value": "file.dll"	www.virus-total.com/ #/file..."
.category	indicator.attribute	Category	.timestamp	"category": "Antivirus detection"	
.to_ids	indicator.attribute	To IDS	.timestamp	"to_ids": false	

Feed Data Path (response.Event. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.dis- tribution	indic- ator. attribute	Dis- tribution	.timesta- mp	"dis- tribution": "3"	attribute distribution map
.timestam- p	indic- ator. attribute	Pub- lished At	.timesta- mp	"timestam- p": "15450636- 78"	formatted
.comment	indic- ator. attribute	Com- ment	.timesta- mp	"comment": "dummy comment"	*
.comment	indic- ator. attribute	Pertin- ence	.timesta- mp	"comment": "Pertin- ence: dummy pertinence"	**
.sharing_ group_id	indic- ator. attribute	Sharing Group	.timesta- mp	"sharing_ group_ id": "0"	

Feed Data Path (response.Event. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.deleted	indicator. attribute	Deleted	.timestamp	"deleted": false	
.disable_ cor- relation	indicator. attribute	Disable Cor- relation	.timestamp	"disable_ correlation": false	
.object_ relation	indicator. attribute	Object Relation	.timestamp	"object_ relation": null	

- *'Comment' attribute is created only if "Pertinence" does not appear in the .comment value
- ** 'Pertinence' attribute is created only if "Pertinence" appears in the .comment value and the value of the new attribute will be everything after 'Pertinence:'

Feed Data Path (response.Event. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.value	event. attribute	Category		"value": "http://link.com"	where . type == 'link'

Feed Data Path (response.Event. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.name	signature. name	Name		"HexExample"	Extracted from value key
.value	signature. name	Value		"value": "rule HexExample {\r\n\tstrings: \r\n\t\t..."	
.type	signature. name	Type		"YARA"	

Feed Data Path (response.Event. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.comment	indicator. attribute	Comment	.timestamp	"comment": "dnssrslvr.dll"	*

*Added to the response.Event.Object.Attribute indicators

Feed Data Path (response.Event. Object. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.type	indicator. type	Type	.timestam- p	"type": "md5"	indicator type map
.value	indic- ator. value	Value	.timestam- p	"value": "44d88612 fea8a8f36de 82e1278abb 02f"	
.category	indic- ator. attribute	Category	.timestam- p	"category": "Payload delivery"	
.to_ids	indic- ator. attribute	To IDS	.timestam- p	"to_ids": true	
.dis- tribution	indic- ator. attribute	Dis- tribution	.timestam- p	"dis- tribution": "5"	attribute dis- tribution

Feed Data Path (response.Event. Object. Attribute)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					map
.sharing_ group_ id	indic- ator. attribute	Sharing Group	.timestam- p	"sharing_ group_ id": "0"	

Feed Data Path (response.Event. Object.Galaxy. GalaxyCluster)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Pub- lished Date	Examples	Note- s
.value + . meta. synonyms	adversar- y. name	Name		"value": ["Keyhole Panda", "temp.bottle"]	
.id	adversar- y. attribute	ID		"id": "5401",	
.type	adversar- y. attribute	Type		"type": "threat-actor"	

Feed Data Path (response.Event. Object.Galaxy. GalaxyCluster)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Pub- lished Date	Examples	Note- s
.description	adversar- y. attribute	Descrip- tion		"description": "no description"	
.galaxy_id	adversar- y. attribute	Galaxy ID		"galaxy_id": "3"	
version	adversar- y. attribute	Version		"version": "75"	
tag_id	adversar- y. attribute	Tag ID		"tag_id": "77"	

Feed Data Path (response.Event. Object.Galaxy. GalaxyCluster)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Pub- lished Date	Examples	Note- s
.meta.cfr- suspected- state- sponsor	adversar- y. attribute	Suspected State Sponsor		meta["cfr- suspected- state- sponsor"]: ["dummy"]	
.meta.cfr- suspected- victims	adversar- y. attribute	Suspected Victims		meta["cfr- suspected- victims"]: ["dummy"]	
.meta.cfr- target- category	adversar- y. attribute	Target Category		meta["cfr- target- category"]: ["dummy"]	
..meta.cfr- type-of- incident	adversar- y. attribute	Type of Incident		meta["cfr- type-of-incident"]: ["dummy"]	

Feed Data Path (response.Event. Object.Galaxy. GalaxyCluster)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Pub- lished Date	Examples	Note- s
.meta.- country	adversar- y. attribute	Country		meta["country"]: ["CN"]	
.meta.ref	adversar- y. attribute	Refer- ences		meta["refs"]: ["www.- dummy.com"]	

** Where GalaxyCluster["type"] == "threat-actor"

Feed Data Path (response.Event. Object.Galaxy. GalaxyCluster**)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.value	STIX2 object***	Value****		"value": "APT16 - G0023"*****	mitre_ object_ types_list

** Where GalaxyCluster["namespace"] == "mitre-attack" *** STIX2 objects are created based on the '.type' mapped through mitre_object_types_list. **** The value suffers some changes in order to match the already created STIX2 objects ingested by the MITRE feeds.

Feed Data Path (response.Event.)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.name	event.attribute	Tag	.publish_timestamp	"malware_classification: malware category= "Downloader""	taxonomy map
.name	indicator & event.attributes	Tag		"malware_classification: malware category= "Downloader""	

TLPs assigned to each object if the response.Event.Tag array contains a dictionary item with the key 'name' and one of the two values: 'tlp:tlp_value' / 'iep:traffic-light-protocol="tlp_value"' (ex: "name": "tlp:red" / 'iep:traffic-light-protocol="RED"').

Change Log

Version 1.0.1:

In this version, we added:

- Yara signature support
- The ability to add "IP Type" indicator attributes

- The response.event.Tag[] as unmapped ingested indicator and event attributes
- Support for "Pertinence" indicator attributes

We removed MITRE Galaxy namespace filtering.

We also changed the following behaviors:

- Event.Object data is no longer added as indicators, but Event.Object.comments are now added as attributes to the Event.Object.Attribute indicators.

Event.Object.Attribute indicators are now related only per Event.Object.Attributes array and not to each other.