ThreatQuotient

McAfee ATLAS CDF Guide

Version 1.1.0

December 14, 2021

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

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.

Versioning

- Current integration version: `1.1.0`
- Compatible with ThreatQ versions >= `4.46.0`

Introduction

Threat intelligence feed that ingests IP, FQDN, URL, Malware, Hashes, and Campaigns from the McAfee ATLAS data. The data is exported in JSON files, transferred to ThreatQ and imported by the feed.

The integration downloads JSON files from the following feeds:

- McAfee ATLAS Campaigns
- McAfee ATLAS IPs
- McAfee ATLAS URLs
- McAfee ATLAS Hashes

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.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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.

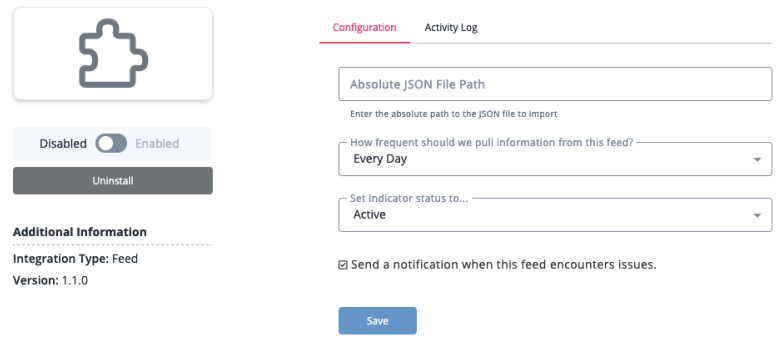
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** 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 to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Absolute JSON File Path	Enter the absolute path to the JSON file to import.



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

McAfee ATLAS Campaigns

The McAfee ATLAS Campaigns feed downloads a JSON file into the ThreatQ platform.

```
GET /path/to/file
```

> The pathway is defined in the Configuration section.

JSON response sample:


```
[
  {
    "parsed_tags.threat-profile-type": [
      "tool"
    ],
    "event_threat_level": "high",
    "event_timestamp": "1534567873",
    "type": "link",
    "event_tags": [
      "ATR Blog - McAfee",
      "misp-galaxy:mitre-attack-pattern=\"Data Encrypted for Impact - T1486\"",
      "ATR:Event Created:2020:Q1",
      "misp-galaxy:sector=\"Multi-sector\"",
      "misp-galaxy:mitre-attack-pattern=\"Spearphishing Attachment - T1193\"",
      "misp-galaxy:mitre-attack-pattern=\"PowerShell - T1086\"",
      "misp-galaxy:mitre-attack-pattern=\"Commonly Used Port - T1043\"",
      "misp-galaxy:mitre-attack-pattern=\"Remote System Discovery - T1018\"",
      "misp-galaxy:mitre-attack-pattern=\"Windows Remote Management - T1028\"",
      "misp-galaxy:mitre-attack-pattern=\"Account Discovery - T1087\"",
      "misp-galaxy:mitre-attack-pattern=\"Credentials in Registry - T1214\"",
      "misp-galaxy:mitre-attack-pattern=\"Permission Groups Discovery - T1069\"",
      "ATR-Tracked-Threat",
      "misp-galaxy:mitre-attack-pattern=\"System Network Configuration Discovery - T1016\"",
      "misp-galaxy:mitre-attack-pattern=\"Masquerading - T1036\"",
      "misp-galaxy:mitre-attack-pattern=\"Process Injection - T1055\"",
      "misp-galaxy:mitre-attack-pattern=\"Process Discovery - T1057\"",
      "misp-galaxy:mitre-attack-pattern=\"File and Directory Discovery - T1083\"",
      "misp-galaxy:mitre-attack-pattern=\"Access Token Manipulation - T1134\"",
      "misp-galaxy:mitre-attack-pattern=\"Service Stop - T1489\"",
      "misp-galaxy:mitre-attack-pattern=\"Inhibit System Recovery - T1490\"",
      "misp-galaxy:mitre-attack-pattern=\"Registry Run Keys / Startup Folder - T1060\"",
      "misp-galaxy:mitre-attack-pattern=\"Disabling Security Tools - T1089\"",
      "misp-galaxy:mitre-attack-pattern=\"Software Packing - T1027.002\"",
      "misp-galaxy:mitre-attack-pattern=\"Obfuscated Files or Information - T1027\"",
      "TLP: white",
      "misp-galaxy:mcafee-tool=\"Ryuk Ransomware\"",
      "atr:threat-profile-type=\"tool\"",
      "atr:threat-category=\"Ransomware\"",
      "misp-galaxy:mitre-attack-pattern=\"Ingress Tool Transfer - T1105\"",
```

```
    "misp-galaxy:mitre-attack-pattern=\"OS Credential Dumping - T1003\"",
    "misp-galaxy:mitre-attack-pattern=\"PowerShell - T1059.001\"",
    "misp-galaxy:mitre-attack-pattern=\"Windows Command Shell - T1059.003\"",
    "misp-galaxy:mitre-attack-pattern=\"Native API - T1106\"",
    "MISP_General",
    "misp-galaxy:mcafee-tool=\"Bazar Loader\"",
    "misp-galaxy:mcafee-tool=\"Cobalt Strike\"",
    "misp-galaxy:mcafee-tool=\"TrickBot\"",
    "misp-galaxy:mcafee-tool=\"certutil\"",
    "misp-galaxy:sector=\"Accounting\"",
    "misp-galaxy:sector=\"Automotive\"",
    "misp-galaxy:sector=\"Electronic\"",
    "misp-galaxy:sector=\"Health\"",
    "misp-galaxy:mcafee-tool=\"Ryuk Stealer\"",
    "misp-galaxy:mcafee-tool=\"AdFind\"",
    "misp-galaxy:mcafee-tool=\"Mimikatz\"",
    "misp-galaxy:mcafee-tool=\"BloodHound\"",
    "misp-galaxy:mcafee-tool=\"BITSAdmin\"",
    "misp-galaxy:mcafee-tool=\"KERBRUTE\"",
    "misp-galaxy:mcafee-tool=\"Net.exe\"",
    "misp-galaxy:mcafee-tool=\"Nltest\"",
    "misp-galaxy:mcafee-tool=\"Taskkill\"",
    "misp-galaxy:mitre-attack-pattern=\"Active Scanning - T1595\"",
    "misp-galaxy:mitre-attack-pattern=\"Network Service Scanning - T1046\"",
    "misp-galaxy:mcafee-threat-actor=\"FIN12\"",
    "misp-galaxy:mcafee-threat-actor=\"TrickBot  Group\"",
    "misp-galaxy:atr-hunting-rule=\"123456-789-1bcs-8590-034545kfrf\""
  ],
  "parsed_tags.mcafee-threat-actor": [
    "FIN12",
    "TrickBot  Group"
  ],
  "event_id": "123456",
  "event_info": "Threat Profile: Ryuk Ransomware",
  "parsed_tags.threat-category": [
    "Ransomware"
  ],
  "event_date": "2019-01-09",
  "parsed_tags.mitre-attack-pattern": [
    "Data Encrypted for Impact",
    "Spearphishing Attachment",
    "PowerShell",
    "Commonly Used Port",
    "Remote System Discovery",
    "Windows Remote Management",
    "Account Discovery"
  ],
  "event_publish_timestamp": "1638194423",
  "parsed_tags.mcafee-tool": [
    "Ryuk Ransomware",
    "Bazar Loader",
    "Cobalt Strike",
    "TrickBot",
    "certutil",
    "Ryuk Stealer",
    "AdFind",
    "Mimikatz",
    "BloodHound",
    "BITSAdmin",
    "KERBRUTE",
    "Net.exe",
```

```
      "Nltest",
      "Taskkill"
    ],
    "comment": "",
    "id": "9876543",
    "category": "External analysis",
    "value": "https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-
the-point/",
    "timestamp": "1599771717"
  }
]
```

McAfee ATLAS IPs

The McAfee ATLAS IPs feed downloads a JSON file into the ThreatQ platform.

```
GET /path/to/file
```

> The pathway is defined in the Configuration section.

JSON response sample:


```
[
  {
    "trust": 15,
    "product": "NSP",
    "first_seen": 1638135306000,
    "last_seen": 1638135306000,
    "is_enterprise": true,
    "ip": "2.3.4.183",
    "connected_port": 25,
    "reputation": "high",
    "source": "repper",
    "is_ipv4": true,
    "protocol": "tcp",
    "count_queries": 1,
    "product_type": "corporate",
    "event_type": "ip",
    "port": 1216,
    "customer_sector": "Banking/Financial/Wealth Management",
    "client_country": "BG",
    "count_clients": 1,
    "customer_id": "11267",
    "is_destination": false
  },
  {
    "trust": 15,
    "product": "EG",
    "first_seen": 1638089963000,
    "last_seen": 1638089963000,
    "is_enterprise": true,
    "ip": "54.34.23.23",
    "reputation": "high",
    "source": "repper",
    "is_ipv4": true,
    "count_queries": 1,
    "product_type": "corporate",
    "event_type": "ip",
    "port": 25,
    "client_country": "BG",
    "count_clients": 1,
    "sector": "media & communications"
  }
]
```

McAfee ATLAS URLs

The McAfee ATLAS URLs feed downloads a JSON file into the ThreatQ platform.

```
GET /path/to/file
```

> The pathway is defined in the Configuration section.

JSON response sample:


```
[
  {
    "trust": 1,
    "product": "McAfee WebAdvisor",
    "first_seen": 1638073965000,
    "category_name": [
      "Games",
      "Malicious Sites"
    ],
    "last_seen": 1638073965000,
    "category_risk_group": [
      "Productivity",
      "Security"
    ],
    "reputation": "high",
    "category_functional_group": [
      "Games/Gambling",
      "Risk/Fraud/Crime"
    ],
    "source": "rest",
    "count_queries": 2,
    "product_type": "consumer",
    "event_type": "domain",
    "domain": "olsdfn.com",
    "host": "sd.olsdfn.com",
    "client_country": "US",
    "count_clients": 1,
    "category": [
      "116",
      "130"
    ],
    "url_path": "/sdfsdf-ke/"
  }
]
```

McAfee ATLAS Hashes

The McAfee ATLAS Hashes feed downloads a JSON file into the ThreatQ platform.

```
GET /path/to/file
```

> The pathway is defined in the Configuration section.

JSON response sample:


```
[
  {
    "trust": 2,
    "product": "TIE Server",
    "first_seen": 1638093800000,
    "last_seen": 1638140548000,
    "is_enterprise": true,
    "reputation": "trojan",
    "source": "rest",
    "count_queries": 2,
    "event_type": "file",
    "product_type": "corporate",
    "client_country": "US",
    "count_clients": 1,
    "md5": "cf94eca567345123241fc07f54904517"
  },
  {
    "trust": 4,
    "product": "TIE Server",
    "first_seen": 1638097155000,
    "last_seen": 1638143993000,
    "is_enterprise": true,
    "reputation": "pup",
    "source": "rest",
    "count_queries": 2,
    "event_type": "file",
    "product_type": "corporate",
    "client_country": "US",
    "count_clients": 1,
    "md5": "3j4jsorj544561b9b0a8205e5a54fb7"
  }
]
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
data[].category	Attribute	Category		Only used by McAfee ATLAS Campaigns
data[].event_threat_level	Attribute	Threat level		Only used by McAfee ATLAS Campaigns
data[].comment	Attribute	Comment		Only used by McAfee ATLAS Campaigns
data[].value	Campaign	Campaign Name		Only used by McAfee ATLAS Campaigns
data[].reputation	Attribute	Reputation	high	
data[].trust	Attribute	Trust	1	
data[].customer_whois	Attribute	Customer WHOIS		
data[].client_country	Attribute	Client Country Code	US	
data[].sector	Attribute	Sector	Multi-sector	
data[].product_type	Attribute	Product Type	consumer	
data[].product	Attribute	Product	McAfee Personal Firewall	
data[].category_name	Attribute	Category	Malicious Sites	
data[].category_risk_group	Attribute	Risk Group	Security	
data[].category_functional_group	Attribute	Functional Group	Risk/Fraud/Crime	
data[].customer_sector	Attribute	Customer Sector	media & communications	
data[].is_destination	Attribute	Is Destination	1	
data[].is_enterprise	Attribute	Is Enterprise	true	
data[].is_inbound	Attribute	Is Inbound		
data[].event_id	Attribute	Event ID	12345	
data[].attack_id	Attribute	Attack ID		
data[].count_clients	Attribute	Count Clients	1	
data[].count_queries	Attribute	Count Queries	1	
data[].customer_id	Attribute	Customer ID	888345204999	
data[].protocol	Attribute	Protocol	tcp	
data[].port	Attribute	Port	443	
data[].ip_country	Attribute	IP Address Country		
data[].event_tags[]	Attribute	Targeted Country	"misp-galaxy:target-information="Vietnam""	
data[].event_tags[]	Attribute	Malware Classification	"atr:threat-category="Ransomware""	
data[].event_tags[]	Attribute	Incident Classification	"circl:incident-classification="phishing""	
data[].event_tags[]	Attribute	NCSC Label	"ncsc:label=""	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
data[].event_tags[]	Attribute	NCSC Action	"ncsc:action="""	
data[].event_tags[]	Attribute	Targeted Platforms	"ms-caro-malware-full:malware-platform="""	
data[].event_tags[]	Attribute	MISP Event Tag		
data[].event_tags[]	Attribute	Feed Source	"feed:source="BESICAT""	
data[].event_tags[]	Attribute	OSINT Source Type	"osint:source-type="block-or-filter-list""	
data[].event_tags[]	Attribute	Veris Country Code	"veris:country="USA""	
data[].event_tags[]	Attribute	Veris Asset Variety	"veris:asset:variety="""	
data[].event_tags[]	Attribute	Sector	"misp-galaxy:sector="Academia - University""	
data[].event_tags[]	Attribute	Circl Incident Classification	"circl:incident-classification="malware""	
data[].event_tags[]	Attribute	Circl Topic	"csirt_case_classification:incident-category="finance""	
data[].event_tags[]	Attribute	CSIRT Incident Category	"csirt_case_classification:incident-category="DOS""	
data[].event_tags[]	Attribute	ENISA Nefarious Activity	"enisa:nefarious-activity-abuse="ransomware""	
data[].event_tags[]	Attribute	Malware Label	"malware:label="trojan""	
data[].event_tags[]	Attribute	Current Event	"current-event:"Hacking""	
data[].event_tags[]	Attribute	Kill Chain Phase	"kill-chain:Command and Control"	
data[].event_tags[]	Attribute	Targeted System	"cert-ist:threat_targeted_system="Windows""	
data[].event_tags[]	Attribute	IOC Accuracy	"cert-ist:ioc_accuracy="medium""	
data[].event_tags[]	Attribute	Threat Level	"cert-ist:threat_level="low""	
data[].event_tags[]	Attribute	Threat Type	"cert-ist:threat_type="malware_outbreak""	
data[].event_tags[]	Attribute	Threat Profile Type	"atr:threat-profile-type="tool""	
data[].event_tags[]	Attribute	Hunting Rule	"misp-galaxy:atr-hunting-rule="f666c899-863e-4256-9573-43b03541f321""	
data[].domain	Indicator	FQDN	denetsuk.com	
data[].host	Indicator	FQDN	denetsuk.com	
data[].url_path	Indicator	URL Path	/movie/249/4506/	
data[].ip	Indicator	IP Address	23.87.23.12	
data[].md5	Indicator	MD5	cf94eca668295888241fc07f54904517	
data[].sha256	Indicator	SHA-256	0181a9b8be4a3c28f38d442c03b53ea782cf1c90f0d8390292b6b06da58497ec	

Average Feed Run

This integration contains four separate feeds that exports system data in the form JSON files. The ThreatQ platform then imports the JSON files. System objects will differ based on what has been exported.

FEED	RUN TIME
McAfee ATLAS Campaigns	3.5 hours
McAfee ATLAS URLs	1.5 hours
McAfee ATLAS IPs	1 hours
McAfee ATLAS Hashes	2 hours

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

Change Log

- **Version 1.1.0**
  - Updated and improved the list of items parsed from the feeds.
- **Version 1.0.0**
  - Initial release