ThreatQuotient

Trellix ATLAS CDF

Version 1.2.0

September 23, 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	1.2.0
Compatible with ThreatQ Versions	>= 4.46.0
Support Tier	ThreatQ Supported

Introduction

The Trellix ATLAS CDF ingests IP, FQDN, URL, Malware, Hashes, and Campaigns from the Trellix ATLAS data.

The integration provides the following feeds:

- Trellix ATLAS Campaigns - ingests IOCs, Campaigns, Attack Pattern, Malware, Adversaries, Cryptocurrencies, Signatures and Vulnerabilities from the Trellix ATLAS.
- Trellix ATLAS IPs - ingests IP Address from the Trellix ATLAS.
- Trellix ATLAS URLs - ingests URLs from the Trellix ATLAS.
- Trellix ATLAS Hashes - ingests Hashes from the Trellix ATLAS.

The integration ingests the following system object types:

- Adversaries
- Attack Pattern
- Campaigns
- Cryptocurrency
- Indicators
- Malware
- Signatures
- Vulnerabilities

Prerequisites

The following is required by the integration:

- Absolute JSON file path for each feed.
- Cryptocurrency custom object installed on your ThreatQ instance.

Cryptocurrency Custom Object

The integration requires the Cryptocurrency custom object.

Use the steps provided to install the custom object.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the following location:

   ```
   cd /var/lib/threatq/misc/
   ```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg

6. Run the following command:

   ```
   kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
   lib/threatq/misc/install.sh /var/lib/threatq/misc
   ```

> The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir trellix_cdf
   ```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the xxx_cdf directory.

   ```
   mkdir images
   ```

7. Upload the cryptocurrency.svg.
8. Navigate to the **/tmp/trellix_cdf**.

   The directory should resemble the following:

   - tmp
     - **trellix_cdf**
       - **cryptocurrency.json**
       - **install.sh**
       - **images**
         - **cryptocurrency.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf trellix_cdf
```

Installation

> The CDF requires the installation of Cryptocurrency custom object before installing the actual CDF. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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 zip file.
3. Extract the contents of the zip and install the required Cryptocurrency custom object.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine
7. Select the individual feeds to install, when prompted and click **Install**.

   > 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.

The feed(s) 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.

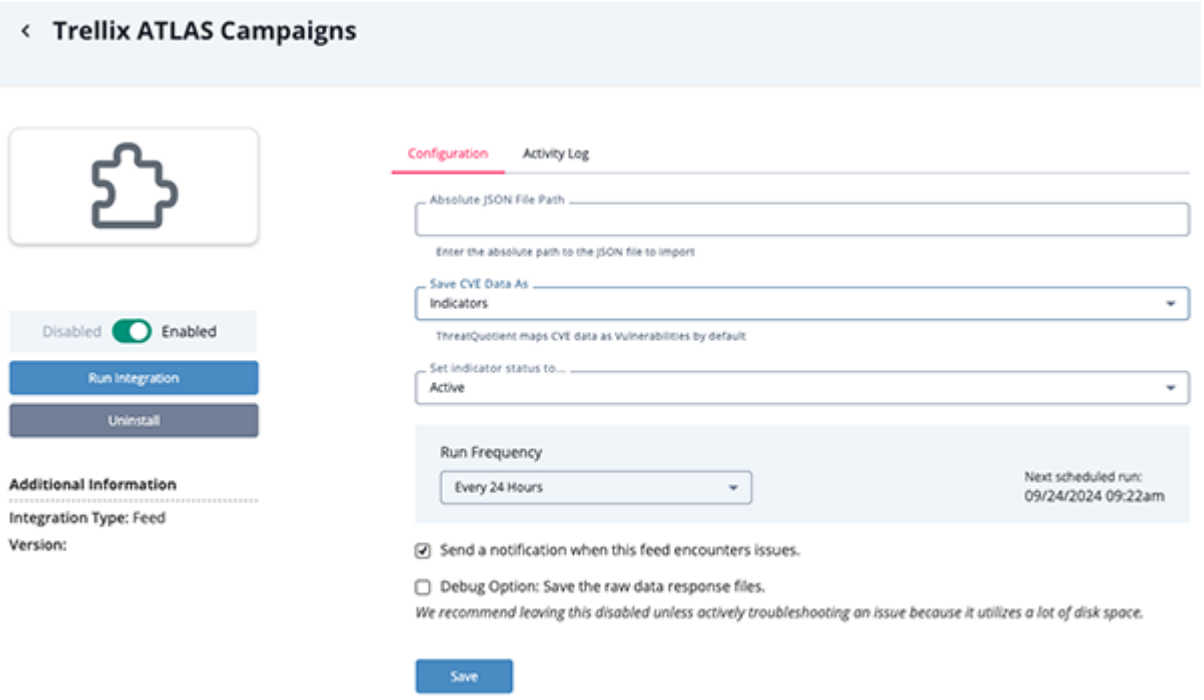
To configure the integration:

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

PARAMETER	DESCRIPTION
Absolute JSON File Path	Enter the absolute path to the JSON file to import.
Save CVE Data As *(ATLAS Campaigns only)*	Select how to ingests CVE data. Options include: ◦ Indicators ◦ Vulnerabilities (default)



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

Trellix ATLAS Campaigns

The Trellix ATLAS Campaigns feed ingests IOCs, Campaigns, Attack Pattern, Malware, Adversaries, Cryptocurrencies, Signatures and Vulnerabilities from the Trellix ATLAS.

`GET /path/to/file`

Sample Response:


```
[
  {
    "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": "0l8h4xuvxe - Binary was not available for analysis.",
    "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"
  }
]
```

Trellix ATLAS IPs

The Trellix ATLAS IPs feed ingests IP Address from the Trellix ATLAS.

`GET /path/to/file`

Sample Response:


```
[
  {
    "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"
  }
]
```

Trellix ATLAS URLs

The Trellix ATLAS URLs feed ingests URLs from the Trellix ATLAS.

`GET /path/to/file`

Sample Response:


```
[
  {
    "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/"
  }
]
```

Trellix ATLAS Hashes

The Trellix ATLAS Hashes feed ingests Hashes from the Trellix ATLAS.

`GET /path/to/file`

Sample Response:


```
[
  {
    "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"
  }
]
```

ThreatQuotient provides the following default mapping for all feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].category	Attribute	Category	External analysis	Only used by Trellix ATLAS Campaigns	
data[].event_threat_level	Attribute	Threat level	high	Only used by Trellix ATLAS Campaigns	
data[].comment	Attribute	Comment	0l8h4xuvxe - Binary was not available for analysis.	Only used by Trellix ATLAS Campaigns	
data[].value	Campaign.Value	Campaign Name	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Cryptocurrency.Value	N/A	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Adversary.Value	N/A	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Signature.Value	Custom	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Indicator.Value	MD5, SHA-1, SHA-256, SHA-512, IP Address, FQDN, CVE	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Vulnerability.Value	N/A	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Attribute	Description	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Attribute	Port	N/A	Only used by Trellix ATLAS Campaigns	
N/A	Attribute	Is Destination IP	YES	Only used by Trellix ATLAS Campaigns	
data[].value	Attribute	Command Line	N/A	Only used by Trellix	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				ATLAS Campaigns	
data[].value	Attribute	Annotation	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Attribute	Phishing	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Attribute	Geolocation	N/A	Only used by Trellix ATLAS Campaigns	
data[].value	Attribute	data[].category	N/A	Only used by Trellix ATLAS Campaigns	
data[].comment	Attribute	data[].category	N/A	Only used by Trellix ATLAS Campaigns	
N/A	Attribute	Sigma Rule	N/A	Only used by Trellix ATLAS Campaigns	
data[].reputation	Attribute	Reputation	high	N/A	
data[].trust	Attribute	Trust	1	N/A	
data[].customer_whois	Attribute	Customer WHOIS	N/A	N/A	
data[].client_country	Attribute	Client Country Code	US	N/A	
data[].sector	Attribute	Sector	Multi-sector	N/A	
data[].product_type	Attribute	Product Type	consumer	N/A	
data[].product	Attribute	Product	Trellix Personal Firewall	N/A	
data[].category_name	Attribute	Category	Malicious Sites	N/A	
data[].category_risk_group	Attribute	Risk Group	Security	N/A	
data[].category_functional_group	Attribute	Functional Group	Risk/Fraud/Crime	N/A	
data[].customer_sector	Attribute	Customer Sector	media & communications	N/A	
data[].is_destination	Attribute	Is Destination	1	N/A	
data[].is_enterprise	Attribute	Is Enterprise	true	N/A	
data[].is_inbound	Attribute	Is Inbound	N/A	N/A	
data[].event_id	Attribute	Event ID	12345	N/A	
data[].attack_id	Attribute	Attack ID	N/A	N/A	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].count_clients	Attribute	Count Clients	1	N/A	
data[].count_queries	Attribute	Count Queries	1	N/A	
data[].customer_id	Attribute	Customer ID	888345204999	N/A	
data[].protocol	Attribute	Protocol	tcp	N/A	
data[].port	Attribute	Port	443	N/A	
data[].ip_country	Attribute	IP Address Country	N/A	N/A	
data[].event_tags[]	Attribute	Targeted Country	"misp-galaxy:target-information="Vietnam""	N/A	
data[].event_tags[]	Attribute	Malware Classification	"atr:threat-category="Ransomware""	N/A	
data[].event_tags[]	Attribute	Incident Classification	"circl:incident-classification="phishing""	N/A	
data[].event_tags[]	Attribute	NCSC Label	"ncsc:label=""""	N/A	
data[].event_tags[]	Attribute	NCSC Action	"ncsc:action=""""	N/A	
data[].event_tags[]	Attribute	Targeted Platforms	"ms-caro-malware-full:malware-platform=""""	N/A	
data[].event_tags[]	Attribute	MISP Event Tag	N/A	N/A	
data[].event_tags[]	Attribute	Feed Source	"feed:source="BESICAT""	N/A	
data[].event_tags[]	Attribute	OSINT Source Type	"osint:source-type="block-or-filter-list""	N/A	
data[].event_tags[]	Attribute	Veris Country Code	"veris:country="USA""	N/A	
data[].event_tags[]	Attribute	Veris Asset Variety	"veris:asset:variety=""""	N/A	
data[].event_tags[]	Attribute	Sector	"misp-galaxy:sector="Academia - University""	N/A	
data[].event_tags[]	Attribute	Circl Incident Classification	"circl:incident-classification="malware""	N/A	
data[].event_tags[]	Attribute	Circl Topic	"csirt_case_classification:incident-category="finance""	N/A	
data[].event_tags[]	Attribute	CSIRT Incident Category	"csirt_case_classification:incident-category="DOS""	N/A	
data[].event_tags[]	Attribute	ENISA Nefarious Activity	"enisa:nefarious-activity-abuse="ransomware""	N/A	
data[].event_tags[]	Attribute	Malware Label	"malware:label="trojan""	N/A	
data[].event_tags[]	Attribute	Current Event	"current-event:"Hacking""	N/A	
data[].event_tags[]	Attribute	Kill Chain Phase	"kill-chain:Command and Control"	N/A	
data[].event_tags[]	Attribute	Targeted System	"cert-ist:threat_targeted_system="Windows""	N/A	
data[].event_tags[]	Attribute	IOC Accuracy	"cert-ist:ioc_accuracy="medium""	N/A	
data[].event_tags[]	Attribute	Threat Level	"cert-ist:threat_level="low""	N/A	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].event_tags[]	Attribute	Threat Type	"cert-ist:threat_type="malware_outbreak""	N/A	
data[].event_tags[]	Attribute	Threat Profile Type	"atr:threat-profile-type="tool""	N/A	
data[].event_tags[]	Attribute	Hunting Rule	"misp-galaxy:atr-hunting-rule="f666c899-863e-4256-9573-43b03541f321""	N/A	
data[].domain	Indicator	FQDN	denetsuk.com	N/A	
data[].host	Indicator	FQDN	denetsuk.com	N/A	
data[].url_path	Indicator	URL Path	/movie/249/4506/	N/A	
data[].ip	Indicator	IP Address	23.87.23.12	N/A	
data[].md5	Indicator	MD5	cf94eca668295888241fc07f54904517	N/A	
data[].sha256	Indicator	SHA-256	0181a9b8be4a3c28f38d442c03b53ea782cf1c90f0d8390292b6b06da58497ec	N/A	

Average Feed Run

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.

METRIC	RESULT
Run Time	3 hours
Adversaries	12,351
Adversary Attributes	1,453
Attack Pattern	732
Attack Pattern Attributes	2,353
Campaigns	546
Campaigns Attributes	1,453
Cryptocurrencies	86
Indicators	12,342
Indicator Attributes	354,123
Malware	174
Malware Attributes	154
Signatures	69

METRIC	RESULT
Signatures Attributes	56
Vulnerabilities	12,351
Vulnerabilities Attributes	1,453

Change Log

- **Version 1.2.0**
  - Updated the data parsed from the Trellix ATLAS Campaigns feed.
  - Added new custom object type requirement: Cryptocurrency.
  - Rebranded integration to Trellix ATLAS CDF (formerly McAfee ATLAS CDF).
- **Version 1.1.0**
  - Initial release