ThreatQuotient

Trellix Insights CDF Guide

Version 1.0.0

May 15, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported

Introduction

The Trellix Insights CDF for ThreatQ enables analysts to automatically ingest campaigns provided by Trellix.

The integration provides the following feeds:

- **Trellix Insights Campaigns** - brings in campaigns & related context from the Trellix Insights App.
- **Trellix Insights Events** - ingests assets (hosts/devices) with threat events relating to a campaign within the Trellix Insights App.
- **Trellix Insights IOC Data (Supplemental)** - fetches related IOCs to a given Campaign.
- **Trellix Insights Galaxies Data (Supplemental)** - fetches related Galaxy Data to a given Campaign.
- **Trellix Insights Campaign by ID (Supplemental)** - fetches a single campaign by its ID, from Trellix via the Insights endpoint.
- **Trellix ePO Device by Agent ID (Supplemental)** - fetches a single device by its ID from Trellix ePO Saas.

The integration ingests the following system objects:

- Adversaries
- Assets
  - Asset Attributes
- Attack Patterns
- Campaign
  - Campaign Attributes
- Indicators
  - Indicator Attributes
- Malware

Prerequisites

The integration requires the following:

- Trellix API Key, Client ID, and Client Secret. See the Generating Credentials for Trellix Insights section for additional details.
- Asset object type. The Asset object was seeded with ThreatQ v5.10.0. If you are running a ThreatQ instance 5.9.0 or earlier, you will need to install the Asset object prior to installing the integration.

Generating Credentials for Trellix Insights

You will need to obtain an API Key, Client ID, and Client Secret from the Trellix Developer Portal.

Below are instructions on how you can obtain these credentials to use with the integration:

1. Log into your Trellix Insights instance.
2. Navigate to the Trellix's Developer Portal: https://developer.manage.trellix.com/.
3. Click on the **Documentation** tab and select the **Trellix API** link.
4. Click the **Self-Service** tab on the sidebar and then the **API Access Management** sub-tab.
5. On the **API Access Management** page, you'll be able to view your **Trellix API Key** and generate a **Client ID** and **Secret**.
6. Enter a **Client Name**.
7. Enter the following scopes when requesting for your client credentials:
   - ins.user
   - ins.suser
   - ins.ms.r
   - epo.device.r

   > Once submitted, Trellix will need to approve the credentials. Once that has been completed, the credentials can be used with this integration.
8. Once you can access your account, retrieve your Api Key from the following link: https://developer.manage.trellix.com/mvision/selfservice/access_manag

Asset Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

> ⚠ You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system 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.

1. Download the custom object 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_insights_cdf
   ```

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

   ```
   <> mkdir images
   ```

7. Upload the asset.svg.
8. Navigate to the **/tmp/trellix_insights_cdf**.

   The directory should resemble the following:

   - tmp
     - **trellix_insights_cdf**
       - **asset.json**
       - **install.sh**
       - **images**

- asset.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.

```
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)

Application is now in maintenance mode.
Installing Custom Objects - Step 2 of 5 (Installing the Asset Custom Object)
Installing Custom Objects - Step 3 of 5 (Configuring image for Asset Custom
Object)
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode)

Application is now live.
```

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

```
<> rm -rf trellix_insights_cdf
```

Installation

> The CDF requires the installation of the Asset object before installing the actual CDF if your are on ThreatQ version 5.9.0 or earlier. See the Asset section of this guide 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 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.

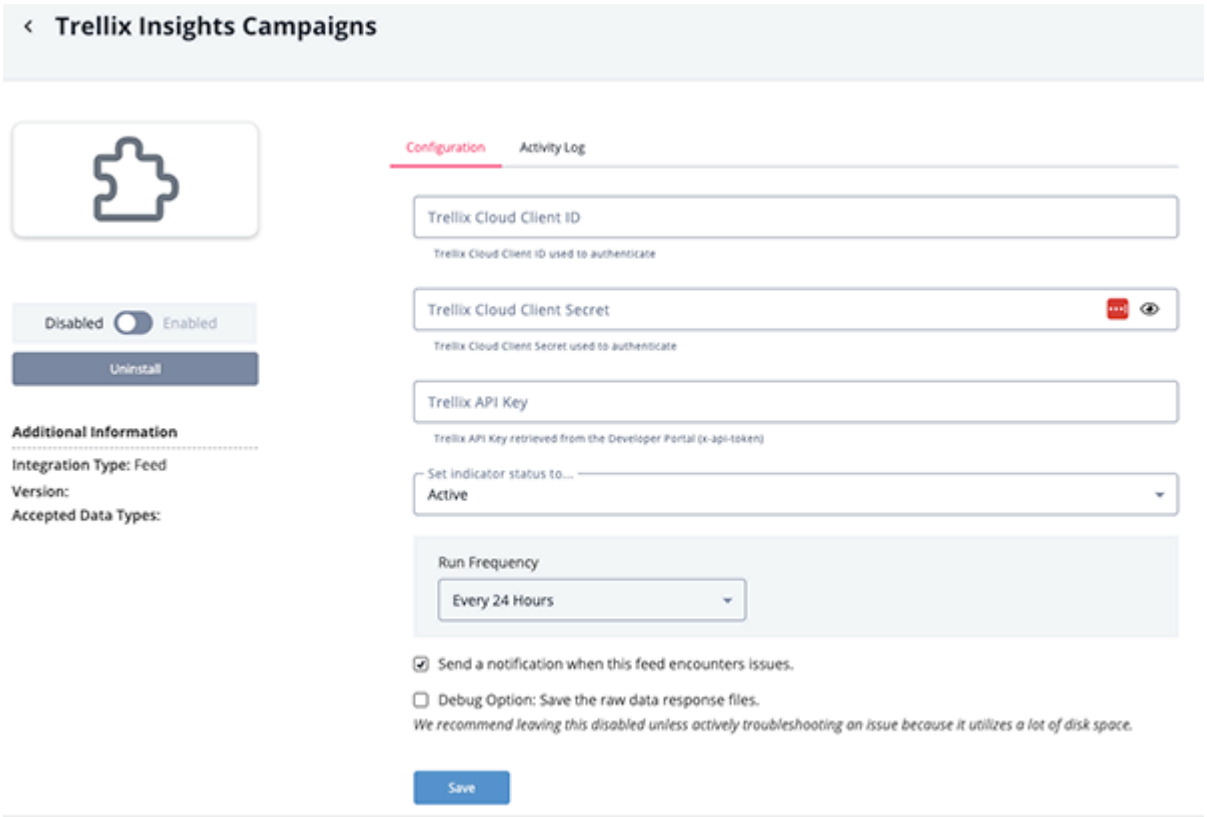
To configure the integration:

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

PARAMETER	DESCRIPTION
Trellix API Key	Your Trellix API Key retrieved from the Developer Portal (x-api-token).
Trellix Cloud Client ID	Your Trellix Cloud Client ID used to authenticate.
Trellix Cloud Client Secret	Your Trellix Cloud Client Secret used to authenticate.



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 Insights Campaigns

The Trellix Insights Campaigns feed brings in campaigns & related context from the Trellix Insights App.

```
GET https://api.manage.trellix.com/insights/v2/campaigns
```

Sample Response:


```
{
    "links": {
        "self": "https://api.manage.trellix.com/insights/v2/campaigns?include=prevalence",
        "first": "https://api.manage.trellix.com/insights/v2/campaigns?
include=prevalence&page[limit]=500&page[offset]=0",
        "last": "https://api.manage.trellix.com/insights/v2/campaigns?
include=prevalence&page[limit]=500&page[offset]=2500",
        "prev": null,
        "next": "https://api.manage.trellix.com/insights/v2/campaigns?
include=prevalence&page[limit]=500&page[offset]=500"
    },
    "data": [
        {
            "type": "campaigns",
            "id": "0026519b-ad7b-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "name": "The Stealthy Email Stealer in the TA505 Arsenal",
                "description": "The TA505 threat group targeted the banking sector with spear-phishing emails that
contained a malicious attachment and installed the FlawedAmmyy remote access trojan. The RAT was used to drop an
email stealer to harvest credentials from multiple software applications.",
                "threat-level-id": 2,
                "kb-article-link": null,
                "coverage": {
                    "dat_version": {
                        "min": 4388
                    },
                    "linux_dat_version": {
                        "min": 4708
                    }
                },
                "updated-on": "2023-04-11T15:07:40.000Z",
                "external-analysis": {
                    "links": [
                        "https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/"
                    ]
                },
                "is-coat": 1,
                "created-on": "2020-06-13T13:37:18.000Z",
                "prevalence": {
```

```
                    "countries": [
                        {
                            "iso_code": "IT",
                            "affected": 69.91,
                            "events": 138.04,
                            "total": 1000000
                        }
                    ],
                    "events": 4.74,
                    "nodes": 2.53,
                    "sectors": [
                        {
                            "sector": "Unknown",
                            "affected": 16.48,
                            "events": 30.91,
                            "total": 1000000
                        }
                    ],
                    "countriesTotalDevices": 1000000
                }
            },
            "relationships": {
                "iocs": {
                    "links": {
                        "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/iocs",
                        "related": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/iocs"
                    }
                },
                "galaxies": {
                    "links": {
                        "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/galaxies",
                        "related": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/galaxies"
                    }
                }
            }
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Campaign.Value	N/A	.data[].attributes.created-on	The Stealthy Email Stealer in the TA505 Arsenal	N/A
.data[].attributes.description	Campaign.Description	N/A	N/A	The TA505 threat group targeted the banking sector ..	Gets the first 64000 characters of the description and adds .data[].attributes.kb-article-link
.data[].attributes.updated-on	Campaign.Ended_at	N/A	N/A	2023-04-11T15:07:40	Timestamp value

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.kb-article-link	Campaign.Attribute	Knowledgebase Article Link	.data[].attributes.created-on	N/A	N/A
.data[].attributes.threat-level-id	Campaign.Attribute	Threat Level	.data[].attributes.created-on	2	Mapped by using the `Threat Level` mapping table below
.data[].attributes.prevalence.countries[].iso_code	Campaign.Attribute	Affected Country Code	.data[].attributes.created-on	IT	N/A
.data[].attributes.external-analysis.links[]	Campaign.Attribute	External Analysis	.data[].attributes.created-on	N/A	N/A
.data[].attributes.is-coat	Campaign.Attribute	Analysed by Coat Team	.data[].attributes.created-on	1	Mapped to bool (1 => True, 0 => False)

Trellix Threat Level Mapping

The Threat Level (as found in `.data[].attributes.threat.severity`) to ThreatQ Type mapping is as follows:

TRELLIX THREAT LEVEL	THREATQ THREAT LEVEL ATTRIBUTE
1	Unverified
2	Low
3	Medium
4	High
5	Very High

The feed calls the `Trellix Insights IOC Data` and `Trellix Insights Galaxies Data` supplemental feeds using `.data[].id` as `campaign_id` parameter.

Trellix Insights IOC Data (Supplemental)

The Trellix Insights IOC Data feed fetches related IOCs to a given Campaign.

`GET https://api.manage.trellix.com/insights/v2/campaigns/{{campaign_id}}/iocs`

Sample Response:


```
{
    "links": {
        "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/iocs",
        "first": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/iocs?
page[limit]=500&page[offset]=0",
        "last": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/iocs?
page[limit]=500&page[offset]=0",
        "prev": null,
        "next": null
    },
    "data": [
        {
            "type": "iocs",
            "id": "00936f77-ad7b-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.manage.trellix.com/insights/v2/iocs/00936f77-ad7b-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "type": "ip",
                "value": "178.48.154.38",
                "coverage": null,
                "uid": "32aa0246-385d-4aae-b4f7-3bf68c1620a9",
                "is-coat": 0,
                "is-sdb-dirty": 1,
                "category": "Network activity",
                "comment": null,
                "lethality": null,
                "determinism": null,
                "created-on": "2020-06-13T13:37:19.000Z"
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "self": "https://api.manage.trellix.com/insights/v2/iocs/00936f77-
ad7b-11ea-9477-02d538d9640e/relationships/campaigns",
                        "related": "https://api.manage.trellix.com/insights/v2/iocs/00936f77-
ad7b-11ea-9477-02d538d9640e/campaigns"
                    }
                }
            }
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.value	Indicator.Value	N/A	.data[].attributes.created-on	178.48.154.38	N/A
.data[].attributes.type	Indicator.Type	N/A	N/A	ip	Mapped by using the `IOC Type` mapping table below
.data[].attributes.is-sdb-dirty	Indicator.Attribute	Potentially Malicious	.data[].attributes.created-on	1	Mapped to bool (1 => True, 0 => False)
.data[].attributes.lethality	Indicator.Attribute	Lethality	.data[].attributes.created-on	N/A	N/A
.data[].attributes.comment	Indicator.Attribute	Comment	.data[].attributes.created-on	N/A	N/A
.data[].attributes.category	Indicator.Attribute	Category	.data[].attributes.created-on	Network activity	N/A
.data[].attributes.is-coat	Indicator.Attribute	Analysed by Coat Team	.data[].attributes.created-on	0	Mapped to bool (1 => True, 0 => False)
.data[].attributes.threat.name	Indicator.Attribute	Threat Name	.data[].attributes.created-on	N/A	N/A
.data[].attributes.threat.classification	Indicator.Attribute	Classification	.data[].attributes.created-on	N/A	N/A
.data[].attributes.threat.severity	Indicator.Attribute	Severity	.data[].attributes.created-on	N/A	Mapped by using the `Threat Severity` mapping table below

Trellix IOC Type Mapping

The IOC Type (as found in `.data[].attributes.type`) to ThreatQ Type mapping is as follows:

TRELLIX INDICATOR TYPE	THREATQ INDICATOR TYPE
sha1	SHA-1
sha256	SHA-256
sha384	SHA-384
sha512	SHA-512

TRELLIX INDICATOR TYPE	THREATQ INDICATOR TYPE
ip	IP Address
md5	MD5
fqdn	FQDN
url	URL

Trellix Threat Severity Mapping

The Threat Severity (as found in `.data[].attributes.threat.severity`) to ThreatQ Type mapping is as follows:

TRELLIX THREAT SEVERITY	THREATQ SEVERITY ATTRIBUTE
1	Unverified
2	Low
3	Medium
4	High
5	Very High

Trellix Insights Galaxies Data (Supplemental)

The Trellix Insights Galaxies Data feed fetches related Galaxy Data to a given Campaign.

`GET https://api.manage.trellix.com/insights/v2/campaigns/{campaign_id}/galaxies`

Sample Response:


```
{
    "links": {
        "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/galaxies",
        "first": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/galaxies?
page[limit]=500&page[offset]=0",
        "last": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/galaxies?
page[limit]=500&page[offset]=0",
        "prev": null,
        "next": null
    },
    "data": [
        {
            "type": "galaxies",
            "id": "978bac8b-67e5-11eb-9477-02d538d9640e",
            "links": {
                "self": "https://api.manage.trellix.com/insights/v2/galaxies/978bac8b-67e5-11eb-9477-02d538d9640e"
            },
            "attributes": {
                "category": "trellix-threat-actor",
                "name": "TA505 Group",
                "description": "TA505 is a financially motivated threat group. The variety of malware delivered by
the group also demonstrates its deep connections to the underground malware scene. TA505 is responsible for the large
malicious spam campaigns distributing instances of the Dridex banking Trojan, Locky ransomware, Jaff ransomware, and
Clop Ransomware.\r\n\r\nTA505 is a sophisticated and innovative threat actor, with plenty of cyber-crime experience,
that engages in targeted attacks across multiple sectors and geographies for financial gain. Over time, TA505 evolved
from a lesser partner to a mature, self-subsisting and versatile crime operation with a broad spectrum of targets.
Throughout the years the group heavily relied on third party services and tooling to support its fraudulent
activities, however, the group now mostly operates independently from initial infection until monetization.
\r\n\r\nThroughout 2019, TA505 changed tactics and adopted a proven simple, although effective, attack strategy:
encrypt a corporate network with ransomware, more specifically the Clop ransomware strain, and demand a ransom in
Bitcoin to obtain the decryption key. Targets are selected in an opportunistic fashion and TA505 currently operates a
broad attack arsenal of both in-house developed and publicly available tooling to exploit its victims. In the
Netherlands, TA505 is notorious for its involvement in the Maastricht University incident in December 2019.
\r\n\r\nTo obtain a foothold within targeted networks, TA505 heavily relies on two pieces of malware: Get2/GetandGo
and SDBbot. Get2/GetandGo functions as a simple loader responsible for gathering system information, C&C beaconing
and command execution. SDBbot is the main remote access tool, written in C++ and downloaded by Get2/GetandGo,
composed of three components: an installer, a loader and the RAT.\r\n(source: [FOX-IT](https://research.nccgroup.com/
2020/11/18/ta505-a-brief-history-of-their-time/)",
                "created-on": "2021-02-05T19:08:55.000Z"
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "self": "https://api.manage.trellix.com/insights/v2/galaxies/
978bac8b-67e5-11eb-9477-02d538d9640e/relationships/campaigns",
                        "related": "https://api.manage.trellix.com/insights/v2/galaxies/
978bac8b-67e5-11eb-9477-02d538d9640e/campaigns"
                    }
```

```
                }
            }
        },
    {
            "type": "galaxies",
            "id": "aac75757-ad7a-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.manage.trellix.com/insights/v2/galaxies/aac75757-ad7a-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "category": "rat",
                "name": "FlawedAmmyy",
                "description": "FlawedAmmyy, has been used since the beginning of 2016 in both highly targeted email attacks as well as massive, multi-million message campaigns. The RAT is based on leaked source code for Version 3 of the Ammyy Admin remote desktop software. As such FlawedAmmyy contains the functionality of the leaked version, including: Remote Desktop control, File system manager, Proxy support, Audio Chat.",
                "created-on": "2020-06-13T13:34:55.000Z"
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "self": "https://api.manage.trellix.com/insights/v2/galaxies/aac75757-ad7a-11ea-9477-02d538d9640e/relationships/campaigns",
                        "related": "https://api.manage.trellix.com/insights/v2/galaxies/aac75757-ad7a-11ea-9477-02d538d9640e/campaigns"
                    }
                }
            }
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Adversary.Name	N/A	N/A	TA505 Group	Ingested if `.data[].attributes.category` contains `threat-actor`
.data[].attributes.description	Adversary.Description	N/A	N/A	TA505 is a financially motivated threat group..	Ingested if `.data[].attributes.category` contains `threat-actor`
.data[].attributes.name	Malware.Value	N/A	N/A	FlawedAmmyy	Ingested if `.data[].attributes.category` ends with `malware` or is one of: `rat`, `tool`, `malpedia`
.data[].attributes.description	Malware.Description	N/A	N/A	FlawedAmmyy, has been used since the beginning of 2016..	Ingested if `.data[].attributes.category` ends with `malware` or is one of: `rat`, `tool`, `malpedia`
.data[].attributes.name	Campaign.Attribute	Affected Sector	N/A	N/A	Ingested if

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`.data[].attributes.category` is `sector`
.data[].attributes.name	Value	Attack Pattern	N/A	N/A	Ingested if `.data[].attributes.category` end in `attack-pattern`

Trellix Insights Events

The Trellix Insights Events feed ingests assets (hosts/devices) with threat events relating to a campaign within the Trellix Insights App.

```
GET https://api.manage.trellix.com/insights/v2/events
```

Sample Response:


```
{
    "events": [
        {
            "id": 7767559,
            "exec_uid": "7889542aef0511edb548063f59524e99",
            "timestamp": "2023-05-10T07:35:06.000Z",
            "customer_details": {
                "ma_id": "674cef0021b7490587a93d10606e5edd",
                "epo_server_id": "cf528de0ceef4bb583f969c6336c31cd",
                "epo_tenant_id": "35e68ed5b09c464296be54bd724f1e04",
                "bps_tenant_id": null
            },
            "md5": "217b06dfa9102b1a96a9d043dd3efd4a",
            "campaign_id": "d5a2a7e9-caf5-11ea-9477-02d538d9640e",
            "iocs": [
                {
                    "type": "md5",
                    "value": "217b06dfa9102b1a96a9d043dd3efd4a"
                },
                {
                    "type": "sha1",
                    "value": "ca1c6481399aa9039329882a717e7944e6889f65"
                },
                {
                    "type": "sha256",
                    "value": "51c906a0de98fbeda712bc622a5b28aab7908251b2f1f25c824d5b1b9e1dfdc8"
                }
            ],
            "resolution": "unknown",
            "product": {
                "name": "ENS",
                "version": "10.7.0"
            }
        }
    ],
    "metadata": {
        "totalRecords": 1,
        "nextOffset": "end"
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.events[].iocs[].value	Indicator.Value	MD5	.events[].timestamp	217b06dfa9102b1a96a9d043dd3efd4a	If .events[].iocs[].type is `md5`
.events[].iocs[].value	Indicator.Value	SHA-1	.events[].timestamp	ca1c6481399aa9039329882a717e7944e6889f65	If .events[].iocs[].type is `sha1`
.events[].iocs[].value	Indicator.Value	SHA-256	.events[].timestamp	51c906a0de98fbeda712bc622a5b28aab7908251b2f1f25c824d5b1b9e1dfdc8	If .events[].iocs[].type is `sha256`

The feed calls the `Trellix ePO Device by Agent ID` and `Trellix Insights Campaign by ID` supplemental feed using `.data[].attributes['campaign-id']` as `campaign_id` parameter.

Trellix Insights Campaign by ID (Supplemental)

The Trellix Insights Campaign by ID feed fetches a single campaign by its ID, from Trellix via the Insights endpoint.

`GET https://api.manage.trellix.com/insights/v2/campaigns/{campaign_id}`

Sample Response:


```
{
    "links": {
        "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e"
    },
    "data": {
        "type": "campaigns",
        "id": "0026519b-ad7b-11ea-9477-02d538d9640e",
        "links": {
            "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e"
        },
        "attributes": {
            "name": "The Stealthy Email Stealer in the TA505 Arsenal",
            "description": "The TA505 threat group targeted the banking sector with spear-phishing emails that
contained a malicious attachment and installed the FlawedAmmyy remote access trojan. The RAT was used to drop an
email stealer to harvest credentials from multiple software applications.",
            "threat-level-id": 2,
            "kb-article-link": null,
            "coverage": {
                "dat_version": {
                    "min": 4388
                },
                "linux_dat_version": {
                    "min": 4708
                }
            },
            "updated-on": "2023-04-11T15:07:40.000Z",
            "external-analysis": {
                "links": [
                    "https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/"
                ]
            },
            "is-coat": 1,
            "created-on": "2020-06-13T13:37:18.000Z"
        },
        "relationships": {
            "iocs": {
                "links": {
                    "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/iocs",
                    "related": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/iocs"
                }
            },
            "galaxies": {
                "links": {
                    "self": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/galaxies",
```

```
                    "related": "https://api.manage.trellix.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/galaxies"
                }
            }
        }
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Campaign.Value	N/A	.data.attributes.created-on	The Stealthy Email Stealer in the TA505 Arsenal	N/A
.data[].attributes.description	Campaign.Description	N/A	N/A	The TA505 threat group targeted the banking sector with spear-phishing emails ..	N/A
.data[].attributes.kb-article-link	Campaign.Attribute	Knowledgebase Article Link	.data.attributes.created-on	N/A	N/A
.data[].attributes.threat-level-id	Campaign.Attribute	Threat Level	.data.attributes.created-on	2	Mapped by using the `Threat Level` mapping table below
.data[].attributes.external-analysis.links[]	Campaign.Attribute	External Analysis	.data.attributes.created-on	https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/	N/A
.data[].attributes.is-coat	Campaign.Attribute	Analyzed by Coat Team	.data.attributes.created-on	1	N/A
.data[].attributes.created-on	Campaign.Started_at	N/A	N/A	2020-06-13T13:37:18.000Z	Timestamp value

Trellix Threat Level Mapping

The Threat Level (as found in `.data[].attributes.threat-level-id`) to ThreatQ Type mapping is as follows:

TRELLIX THREAT LEVEL	THREATQ THREAT LEVEL ATTRIBUTE
1	Unverified
2	Low
3	Medium
4	High
5	Very High

Trellix ePO Device by Agent ID (supplemental)

The Trellix ePO Device by Agent ID feed fetches a single device by its ID from Trellix ePO Saas.

`GET https://api.manage.trellix.com/epo/v2/devices`

Sample Response:


```
{
    "data": [
        {
            "id": "2496624",
            "type": "devices",
            "links": {
                "self": "https://api.manage.trellix.com/epo/v2/devices/2496624"
            },
            "attributes": {
                "name": "TIS-EPO-TESTSER",
                "parentId": 5387625,
                "agentGuid": "32EDA829-0106-451D-9273-E099D04D81AE",
                "lastUpdate": "2023-05-04T09:41:26.067+00:00",
                "agentState": 0,
                "nodePath": null,
                "agentPlatform": "Windows Server 2012 R2:6:3:0",
                "agentVersion": "5.7.9.139",
                "nodeCreatedDate": "2022-02-11T15:49:02.637+00:00",
                "managed": "1",
                "tenantId": 32713,
                "tags": "Server, Test",
                "excludedTags": "",
                "managedState": 1,
                "computerName": "TIS-EPO-TESTSER",
                "domainName": "WORKGROUP",
                "ipAddress": "172.16.114.30",
                "osType": "Windows Server 2012 R2",
                "osVersion": "6.3",
                "osBuildNumber": 9600,
                "cpuType": "Intel Xeon E312xx (Sandy Bridge, IBRS update)",
                "cpuSpeed": 2600,
                "numOfCpu": 2,
                "totalPhysicalMemory": 4294414336,
                "macAddress": "FA163E088958",
                "userName": "N/A",
                "osPlatform": "Server",
                "ipHostName": "tis-epo-testser.threatq.com",
                "subnetAddress": "",
                "isPortable": "non-portable",
                "systemSerialNumber": "393d2d36-46f1-4682-b6c8-957c49a4a589",
                "systemRebootPending": 0,
                "systemModel": "OpenStack Compute",
                "systemManufacturer": "RDO",
                "systemBootTime": "2023-02-21T15:15:50.000+00:00"
            },
            "relationships": {
                "assignedTags": {
                    "links": {
```

```
                        "self": "https://api.manage.trellix.com/epo/v2/devices/2496624/relationships/assignedTags",
                        "related": "https://api.manage.trellix.com/epo/v2/devices/2496624/assignedTags"
                    }
                },
                "installedProducts": {
                    "links": {
                        "self": "https://api.manage.trellix.com/epo/v2/devices/2496624/relationships/
installedProducts",
                        "related": "https://api.manage.trellix.com/epo/v2/devices/2496624/installedProducts"
                    }
                }
            }
        }
    ],
    "links": {
        "first": "https://api.manage.trellix.com/epo/v2/devices?page[limit]=20",
        "last": "https://api.manage.trellix.com/epo/v2/devices?page[limit]=20"
    },
    "meta": {
        "totalResourceCount": 3
    }
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.domainName + '/' + .data[].attributes.name]	Asset.Value	N/A	.data[].attributes.nodeCreatedAt	WORKGROUP/TIS-EPO-TESTSER	Keys concatenated together
.data[].attributes.tags	Asset.Tag	N/A	N/A	Server, Test	N/A
.data[].attributes.agentGuid	Asset.Attribute	Agent GUID	.data[].attributes.nodeCreatedAt	32EDA829-0106-451D-9273-E099D04D81AE	N/A
.data[].attributes.agentPlatform	Asset.Attribute	Agent Platform	.data[].attributes.nodeCreatedAt	Windows Server 2012 R2:6:3:0	N/A
.data[].attributes.agentState	Asset.Attribute	Agent State	.data[].attributes.nodeCreatedAt	0	`Online` if .data[].attributes.agentState = 1, else is `Offline`
.data[].attributes.computerName	Asset.Attribute	Computer Name	.data[].attributes.nodeCreatedAt	TIS-EPO-TESTSER	N/A
.data[].attributes.cpuType	Asset.Attribute	CPU Type	.data[].attributes.nodeCreatedAt	Intel Xeon E312xx (Sandy Bridge, IBRS update)	N/A
.data[].attributes.domainName	Asset.Attribute	Domain Name	.data[].attributes.nodeCreatedAt	WORKGROUP	N/A
.data[].attributes.ipAddress	Asset.Attribute	IP Address	.data[].attributes.nodeCreatedAt	172.16.114.30	N/A
.data[].attributes.numOfCpu	Asset.Attribute	Number of CPUs	.data[].attributes.nodeCreatedAt	2	N/A
.data[].attributes.osPlatform	Asset.Attribute	OS Platform	.data[].attributes.nodeCreatedAt	Server	N/A
.data[].attributes.osType	Asset.Attribute	Operating System	.data[].attributes.nodeCreatedAt	Windows Server 2012 R2	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.userName	Asset.Attribute	Username	.data[].attributes.nodeCreatedAt	N/A	N/A
.data[].attributes.managedState	Asset.Attribute	Is Managed	.data[].attributes.nodeCreatedAt	1	bool -> string

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.

Trellix Insights Campaigns

METRIC	RESULT
Run Time	9 minutes
Campaigns	6
Campaign Attributes	116
Adversaries	2
Indicators	7211
Indicator Attributes	42476
Malware	4
Tools	19

Trellix Insights Events

METRIC	RESULT
Run Time	1 minute
Asset	1
Asset Attributes	12
Campaigns	2
Campaign Attributes	2
Indicators	3

Change Log

- **Version 1.0.0**
  - Initial release