ThreatQuotient

Trellix ePO Events CDF Guide

Version 1.0.0

May 09, 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
ThreatQ Marketplace	https://marketplace.threatq.com/details/trellix-epo-events-cdf

Introduction

The Trellix ePO Events CDF brings in assets (hosts/devices) with threat events from Trellix ePO Saas.

The integration provides the following feed:

- **Trellix ePO Events** - This feed brings in assets (hosts/devices) with threat events from Trellix ePO Saas.

The integration ingests the following system objects:

- Indicators
- Assets
- Events

Prerequisites

The following is required in order to install and run the integration:

- Access to Trellix ePO Saas
- API Key, Client ID, and Client Secret Credentials with the following scope permissions:
  `epo.device.r epo.device.w epo.tags.r epo.tags.w epo.evt.r`

  > See the Generating Credentials for Trellix ePO Saas section for more details.

- The 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 ePO Saas

In order to use this integration, 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 ePO Saas instance
2. Navigate to Trellix's Developer Portal: https://developer.manage.trellix.com/
3. Click on the **Documentation** tab and then click on the **Trellix API** link.
4. On the sidebar, click the **Self-Service** tab, and then the **API Access Management** sub-tab.
5. From 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 and the following scopes when requesting for your client credentials:
   `epo.device.r epo.device.w epo.tags.r epo.tags.w epo.evt.r`
7. Once submitted, Trellix will need to approve the credentials. Once that is completed, they can be used with this integration.
8. Once you can access your account, get Api Key from: 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 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 trellix_cdf directory.

   ```
   <> mkdir images
   ```

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

   The directory should resemble the following:

   - tmp
     - treliix_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_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 Prerequisites chapter for more details. The Asset object must be installed prior to installing the CDF. Attempting to install the CDF without the Asset 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.

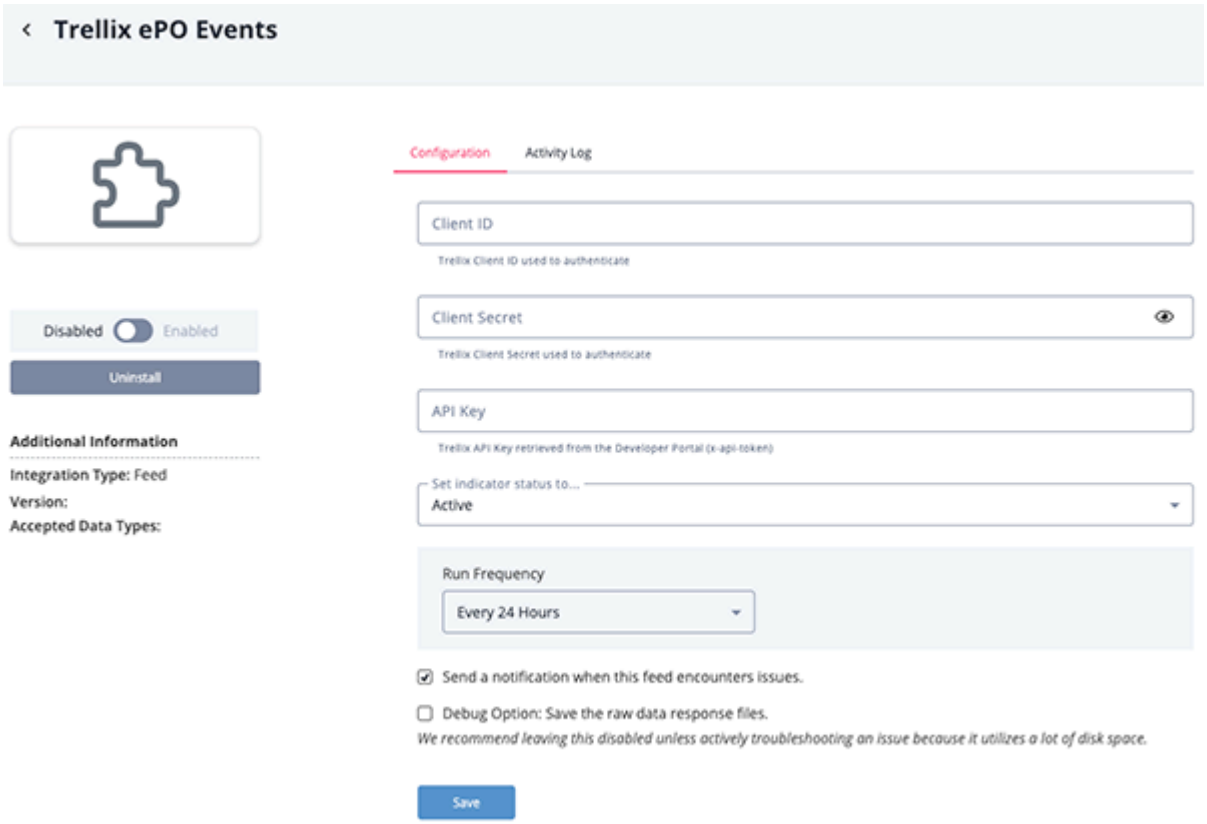
To configure the integration:

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
Client ID	Your Trellix Client ID used to authenticate.
Client Secret	Your rellix Client Secret used to authenticate.
API Key	Your Trellix API Key retrieved from the Developer Portal (x-api-token). See the Generating Credentials for Trellix ePO Saas section for more details.



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 ePO Events

The Rellix ePO Events bring in assets (hosts/devices) with threat events from Trellix ePO.

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

Sample Response:


```
{
  "data": [
    {
      "id": "093d6883-d4aa-485a-92bc-e1e91c351b13",
      "type": "MVEvents",
      "links": {
        "self": "/epo/v2/events/093d6883-d4aa-485a-92bc-e1e91c351b13"
      },
      "attributes": {
        "timestamp": "2023-05-04T08:11:40.345Z",
        "autoguid": "ba5d6605-0d85-407b-9bac-962f299605a8",
        "detectedutc": "1683187699000",
        "receivedutc": "1683187900345",
        "agentguid": "674cef00-21b7-4905-87a9-3d10606e5edd",
        "analyzer": "ENDP_AM_1070",
        "analyzername": "Trellix Endpoint Security",
        "analyzerversion": "10.7.0.5200",
        "analyzerhostname": "windows-new",
        "analyzeripv4": "172.16.114.109",
        "analyzeripv6": "/0:0:0:0:0:ffff:ac10:726d",
        "analyzermac": "fa163e6f6827",
        "analyzerdatversion": "5151.0",
        "analyzerengineversion": "6600.9927",
        "analyzerdetectionmethod": "On-Access Scan",
        "sourcehostname": null,
        "sourceipv4": "172.16.114.109",
        "sourceipv6": "/0:0:0:0:0:ffff:ac10:726d",
        "sourcemac": null,
        "sourceusername": null,
        "sourceprocessname": "C:\\Windows\\explorer.exe",
        "sourceurl": null,
        "targethostname": null,
        "targetipv4": "172.16.114.109",
        "targetipv6": "/0:0:0:0:0:ffff:ac10:726d",
        "targetmac": null,
        "targetusername": "WINDOWS-NEW\\Admin",
        "targetport": null,
        "targetprotocol": null,
        "targetprocessname": null,
        "targetfilename": "C:\\Users\\Admin\\AppData\\Local\\Temp\\2\\Temp1_eicar_com.zip\\eicar.com",
        "threatcategory": "av.detect",
        "threateventid": 1278,
        "threatseverity": "2",
```

```
      "threatname": "EICAR test file",
      "threattype": "test",
      "threatactiontaken": "IDS_ALERT_ACT_TAK_DEL",
      "threathandled": true,
      "nodepath": "1\\4655257\\12172011",
      "targethash": "44d88612fea8a8f36de82e1278abb02f",
      "sourceprocesshash": null,
      "sourceprocesssigned": null,
      "sourceprocesssigner": null,
      "sourcefilepath": null
    }
  }
 ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.[analyzername, threatname, threatseverity, analyzeripv4]	Event.Title	Sighting	.data[].attributes.detectedutc	Trellix Endpoint Security detected a threat - EICAR test file (Severity: Critical) - 172.16.114.109	N/A
.data[].attributes.agentguid	Event.Attribute	Agent GUID	.data[].attributes.timestamp	674cef00-21b7-4905-87a9-3d10606e5edd	N/A
.data[].attributes.analyzername	Event.Attribute	Analyzer	.data[].attributes.timestamp	Trellix Endpoint Security	N/A
.data[].attributes.analyzerdetectionmethod	Event.Attribute	Analyzed Detection Method	.data[].attributes.timestamp	On-Access Scan	N/A
.data[].attributes.threatactiontaken	Event.Attribute	Action Taken	.data[].attributes.timestamp	IDS_ALERT_ACT_TAK_DEL	N/A
.data[].attributes.targetusername	Event.Attribute	Target Username	.data[].attributes.timestamp	WINDOWS-NEW\Admin	N/A
.data[].attributes.targetport	Event.Attribute	Target Port	.data[].attributes.timestamp	N/A	N/A
.data[].attributes.targetfilename	Indicator.Value	File Path	.data[].attributes.timestamp	C:\Users\Admin\AppData\Local\Temp\2\Temp1_eicar_com.zip\eicar.com	N/A
.data[].attributes.targethash	Indicator.Value	MD5	.data[].attributes.timestamp	44d88612fea8a8f36de82e1278abb02f	N/A
.data[].attributes.sourceipv4	Indicator.Value	IP Address	.data[].attributes.timestamp	172.16.114.109	As long as it's not the same as the device IP
.data[].attributes.targetipv4	Indicator.Value	IP Address	.data[].attributes.timestamp	172.16.114.109	As long as it's not the same as the device IP

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.targetprocessname	Indicator.Value	Filename	.data[].attributes.timestamp	N/A	N/A
.data[].attributes.threatname	Event.Attribute, Indicator.Attribute	Threat Name	.data[].attributes.timestamp	EICAR test file	N/A
.data[].attributes.threatcategory	Event.Attribute, Indicator.Attribute	Threat Category	.data[].attributes.timestamp	av.detect	N/A
.data[].attributes.threattype	Event.Attribute, Indicator.Attribute	Threat Type	.data[].attributes.timestamp	test	N/A
.data[].attributes.threatseverity	Event.Attribute, Indicator.Attribute	Severity	.data[].attributes.timestamp	2	Mapped by using the Threat Severity mapping table below

Trellix to ThreatQ Severity Mapping

ThreatQuotient provides the following Severity Mapping:

TRELLIX THREAT SEVERITY	THREATQ ATTRIBUTE VALUE
1	Alert
2	Critical
3	Warning
4	Unknown
5	Notice
6	Info

The Threat Severity can be found in `.data[].attributes.threatseverity`.

Trellix ePO Device by Agent ID (Supplemental)

The Trellix ePO Device by Agent ID supplemental feed fetches a single device by its ID from the 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
    }
}
```


ThreatQuotient 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 ePO Events

METRIC	RESULT
Run Time	1 min
Asset	1
Asset Attributes	12
Events	2
Event Attributes	18
Indicators	2
Indicator Attributes	8

Change Log

- **Version 1.0.0**
  - Initial release