ThreatQuotient

Trellix MVISION EDR Threats CDF User Guide

Version 2.0.4

January 16, 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	2.0.4
Compatible with ThreatQ Versions	>= 4.45.0
Support Tier	ThreatQ Supported

Introduction

The Trellix MVISION EDR Threats for ThreatQ enables analysts to automatically ingest Assets, Attack Patterns, Indicators, Attributes, TTPs, and Tags.

The integration provides the following feed:

- **Trellix MVISION EDR Threats -** ingests indicators and their attributes.

The integration ingests the following system objects:

- Assets
- Attack Patterns
- Events
- Indicators
- TTPs

> ⚠ The Trellix MVISION EDR Threats CDF replaces the McAfee MVISION EDR CDF integration.

Prerequisites

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

- Access to Trellix MVISION EDR
- Trellix API Key, Client ID, and Client Secret Credentials with the following scope permissions: `soc.hts.c soc.hts.r soc.rts.c soc.rts.r soc.qry.pr`. See the Generating Credentials for Trellix MVISION EDR section for further details
- Asset Object

Generating Credentials for Trellix MVISION EDR

In order to use this integration, you will need to obtain an API Key, Client ID, and Client Secret from the Trellix Developer Portal. Previous versions of this integration (McAfee MVISION EDR CDF v1.0.1 and earlier), the integration utilized a now-deprecated authentication strategy. Since then, Trellix has placed the MVISION EDR APIs under their standardized IAM OAuth Authentication strategy.

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

1. Log into your Trellix MVISION EDR instance.
2. Navigate to Trellix's Developer Portal: https://www.mcafee.com/enterprise/en-us/solutions/mvision/developer-portal.html
3. Click on the **Documentation** tab and then the **Trellix API** link.
4. Click the **Self-Service** tab on the sidebar and then the **API Access Management** sub-tab.

   The API Access Management page will load. You can view your Trellix API Key and generate a Client ID and Secret.

5. Enter a client name and the following scopes when requesting for your client credentials: `soc.hts.c soc.hts.r soc.rts.c soc.rts.r soc.qry.pr`
6. Once submitted, Trellix will need to approve the credentials. After approval, the credentials can be used with this integration.

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 Asset 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
     - **trellix_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:

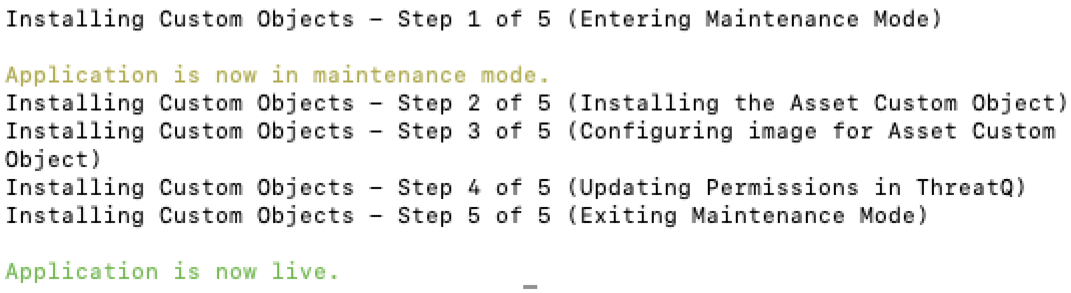
   ```
   chmod +x install.sh
   ```

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 a custom 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 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 file and, if you are on ThreatQ version 5.9 or earlier, install the required Asset custom object.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the yaml 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.

7. 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:

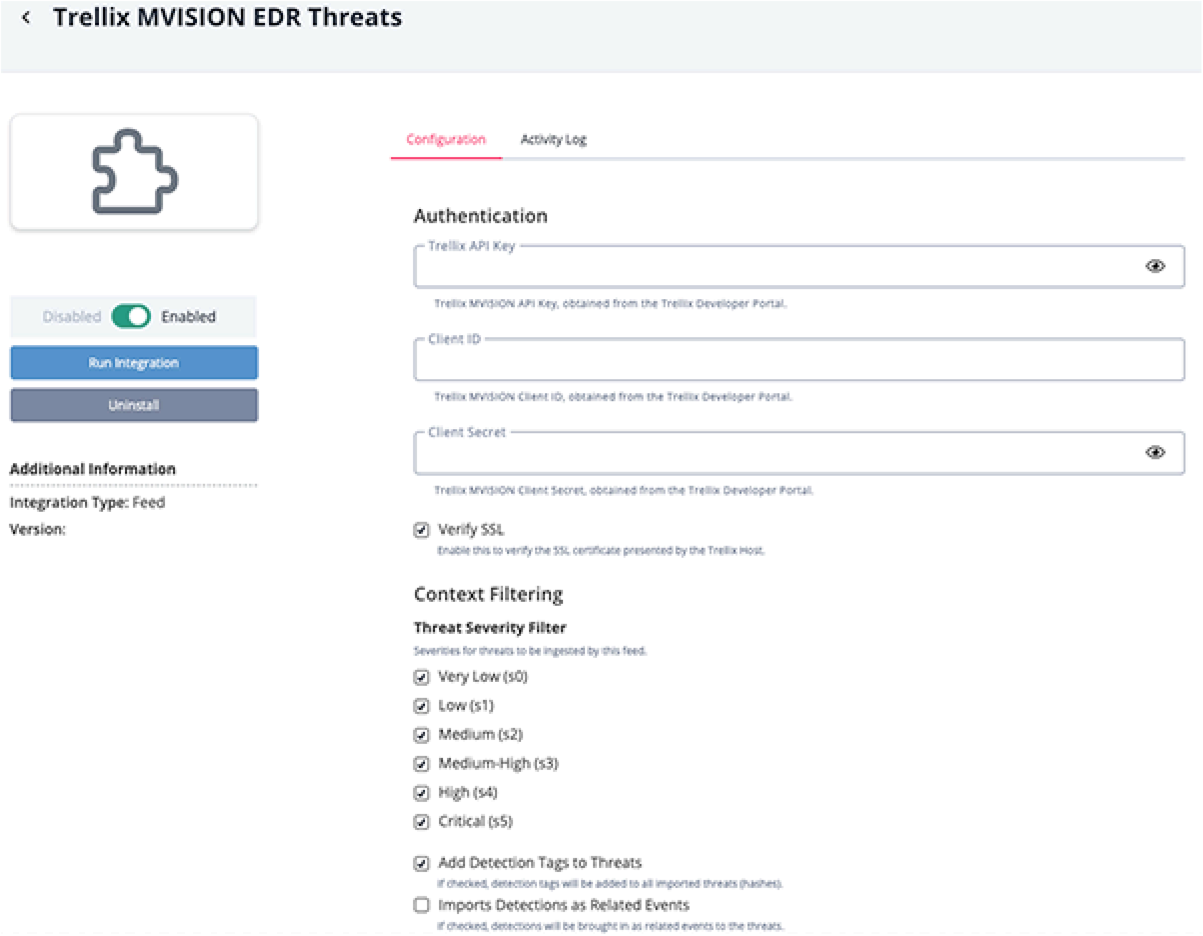
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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 MVISION API Key, obtained from the Trellix Developer Portal.
Client ID	Your Trellix MVISION Client ID, obtained from the Trellix Developer Portal.
Client Secret	Your Trellix MVISION Client Secret, obtained from the Trellix Developer Portal.
Verify SSL	Enable this paramater to verify the SSL certificate presented by the Trellix host.
Threat Severity	Allows you to select one or more threat severity levels to filter your results by. Options include: ◦ Very Low (s0) ◦ Low (s1) ◦ Medium (s2) - default ◦ Medium-High (s3) - default ◦ High (s4) - default ◦ Critical (s5) - default

PARAMETER	DESCRIPTION
Add Detection Tags to Threats	If enabled, detection tags will be bundled up and added to all imported threats (hashes).
Import Detections as Related Events	If enabled, detections will be brought in as related events to the threats.



Additional Information

Integration Type: Feed

Version:

Authentication

Trellix API Key

Trellix MVISION API Key, obtained from the Trellix Developer Portal.

Client ID

Trellix MVISION Client ID, obtained from the Trellix Developer Portal.

Client Secret

Trellix MVISION Client Secret, obtained from the Trellix Developer Portal.

☑ Verify SSL

Enable this to verify the SSL certificate presented by the Trellix Host.

Context Filtering

Threat Severity Filter

Severities for threats to be ingested by this feed.

☑ Very Low (s0)

☑ Low (s1)

☑ Medium (s2)

☑ Medium-High (s3)

☑ High (s4)

☑ Critical (s5)

☑ Add Detection Tags to Threats

If checked, detection tags will be added to all imported threats (hashes).

☐ Imports Detections as Related Events

If checked, detections will be brought in as related events to the threats.

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 MVISION EDR Threats

The Trellix MVISION EDR Threats feed ingests indicators and their attributes.

`GET https://api.<region>/ft/api/v2/ft/threats`

Sample Response:

```
{
    "total": 2,
    "skipped": 0,
    "items": 1,
    "threats": [
        {
            "id": "452825",
            "aggregationKey":
"P_5CC2C563D89257964C4B446F54AFE1E57BBEE49315A9FC001FF5A6BCB6650393",
            "severity": "s1",
            "rank": 88,
            "score": 38,
            "name": "rundll32.exe",
            "type": "pe",
            "status": "viewed",
            "firstDetected": "2022-02-11T21:16:56Z",
            "lastDetected": "2022-02-11T21:16:56Z",
            "hashes": {
                "sha256":
"5CC2C563D89257964C4B446F54AFE1E57BBEE49315A9FC001FF5A6BCB6650393",
                "sha1": "D4AC232D507769FFD004439C15302916A40D9831",
                "md5": "6C308D32AFA41D26CE2A0EA8F7B79565"
            }
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.threats[].hashes.sha256	indicator.value	SHA-256	.threats[].firstDetected	5CC2C563D89257964C4B446F54AFE1E57BBEE49315A9FC001FF5A6BCB6650393	
.threats[].hashes.sh1	indicator.value	SHA-1	.threats[].firstDetected	D4AC232D507769FFD004439C15302916A40D9831	
.threats[].hashes.md5	indicator.value	MD5	.threats[].firstDetected	6C308D32AFA41D26CE2A0EA8F7B79565	
.threats[].name	indicator.attribute	Threat Name	.threats[].firstDetected	rundll32.exe	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.threats[].type	indicator.attribute	Threat Type	.threats[].firstDetected	pe	
.threats[].severity	indicator.attribute	Severity	.threats[].firstDetected	s1	
.threats[].rank	indicator.attribute	Rank	.threats[].firstDetected	88	
.threats[].score	indicator.attribute	Score	.threats[].firstDetected	38	

Get Detections (Supplemental)

The Get Detections (Supplemental) feed retrieves detection tags. The feed is called once per each `.threats[].id` returned by the `Trellix MVISION EDR Threats` feed.

`GET https://api.<region>/ft/api/v2/ft/threats/<threat_id>/detections`

Sample Response:

```
{
    "total": 1,
    "skipped": 0,
    "items": 1,
    "detections": [
        {
            "id": "45154556",
            "traceId": "de298c04-296d-4ae7-8fdc-6d7bcda30733",
            "firstDetected": "2022-02-11T21:16:56Z",
            "severity": "s1",
            "rank": 88,
            "tags": [
                "@MSI._reg_ep0029_intranet",
                "@MSI._reg_ep0037_iepages",
                "@ATE.T1112",
                "@ATA.DefenseEvasion"
            ],
            "host": {
                "maGuid": "32EDA829-0106-451D-9273-E099D04D81AE",
                "hostname": "tis-epo-testser",
                "os": {
                    "major": 6,
                    "minor": 3,
                    "build": 9600,
                    "sp": "",
                    "desc": "Windows 2012 R2"
                },
                "netInterfaces": [
                    {
                        "name": "Ethernet",
                        "macAddress": "fa:16:3e:08:89:58",
                        "ip": "172.16.114.30",
                        "type": 6
                    }
                ],
                "traceExtendedVisibility": 0
            },
            "sha256":
"5CC2C563D89257964C4B446F54AFE1E57BBEE49315A9FC001FF5A6BCB6650393"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.detections[].host.hostname	Event.Title	N/A	.detections[].firstDetected	EDR Detection - Host: tis-epo-testser - Threat Type: pe - Severity: High - ID: 45154556	Title is made with hostname + threat type + severity and the ID
.detections[].severity	Event.Attribute	Severity	.detections[].firstDetected	Low	Value updated accordingly the Severity map
.detections[].rank	Event.Attribute	Rank	.detections[].firstDetected	88	N/A
.detections[].tags[]	Event.Attribute	Tactic	.detections[].firstDetected	Defense Evasion	Only ingest this attribute if starts with '@ATA.'
.detections[].tags[]	Tag.name	N/A	n/a	@MSI._reg_ep0029_intranet	N/A
.detections[].host.hostname[]	Related Asset.Value	N/A	n/a	tis-epo-testser	N/A
.detections[].host.os.desc	Related Asset.Attribute	Operating System	.detections[].firstDetected	Windows 2012 R2	N/A
.detections[].host.hostname	Related Asset.Attribute	Hostname	.detections[].firstDetected	tis-epo-testser	N/A
.detections[].host.netInterfaces[0].ip	Related Asset.Attribute	IP Address	.detections[].firstDetected	172.16.114.30	N/A
.detections[].tags[]	Related TTP.Value	N/A	n/a	reg ep0037 iepages	Only ingest this object if starts with '@MSI.'
.detections[].tags[]	Related Attack Pattern.Value	N/A	n/a	T1112	

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 MVISION EDR Threats

METRIC	RESULT
Run Time	1 minute
Assets	1
Asset Attributes	2
Events	2
Event Attributes	21
TTPs	2
Attack Patterns	8
Indicators	6
Indicator Attributes	30

Known Issues / Limitations

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns extracted from detection event tags to be related to the event. MITRE ATT&CK attack patterns are ingested from the following feeds:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE PRE-ATT&CK

Change Log

- **Version 2.0.4**
    - Removed the **Region** configuration parameter and updated the Trellix base URL.
    - Resolved a related events and indicator tags ingestion issue.
    - Updated the filtering based on a response schema change.
    - Removed the `MVISION link` attribute due to a lack of information the feed provided.
    - Added a new known Issue / limitation entry regarding MITRE ATT&CK Patterns. MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns extracted from detection event tags to be related to the event.
- **Version 2.0.3**
    - Fixed an ingestion issue regarding Assets and Events.
- **Version 2.0.2**
    - Resolved a filter mapping error for tags.
    - Updated the method for retrieving attack patterns from the ThreatQ API.
- **Version 2.0.1**
    - Added validation for non-existent detection list.
- **Version 2.0.0 rev-a (Guide Update)**
    - Updated the Prerequisites chapter regarding the Asset object. ThreatQ version 5.10.0 introduced the Asset object as a seeded default system object. Users on ThreatQ 5.10.0 or later do not have to install the Asset custom object prior to installing the integration.
- **Version 2.0.0**
    - Integration has been rebranded from **McAfee MVISION EDR** to **Trellix MVISION EDR Threats**.
    - Switched authentication method to new IAM authentication using API Key, Client ID, and Client Secret.
    - Updated the **Fetch Detection Tags** configuration field to **Add Detection Tag to Threats**.
    - Added new configuration option: **Import Detections as Related Events**.
    - Updated the **Threat Severity Filter** configuration options scale from Level X to Very Low, Low, Medium, Medium-High, High, and Critical.
    - The Detection (event) tags will now be parsed to create Attack Pattern, TTP, and Tactic relationships.
- **Version 1.0.1**
    - Added expired token reauthorization.
- **Version 1.0.0**
    - Initial release