

ThreatQuotient



McAfee MVISION EDR CDF Guide

Version 1.0.1

April 26, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

- Support 4
- Versioning..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- ThreatQ Mapping 10
 - McAfee MVISION EDR Threats..... 10
 - Get Detections (Supplemental) 12
- Average Feed Run..... 14
 - McAfee MVISION EDR Threats..... 14
- Change Log..... 15

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.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

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

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

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

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



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

Versioning

- Current integration version 1.0.1
- Compatible with ThreatQ versions \geq 4.45.0

Introduction

The McAfee MVISION EDR for ThreatQ enables analysts to automatically ingest Indicators, attributes, and detection tags (optional).

The McAfee MVISION EDR integration for ThreatQ provides the following feeds:

- **McAfee MVISION EDR Threats** - ingests indicators and their attributes.
- **Get Detections - Supplemental** - retrieves detection tags.

The integration ingests the following system objects:

- Indicators
 - Indicator Attributes
- Detection Tags (optional)

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

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

You will still need to [configure and then enable the feed](#).

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

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




If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Region	Your geographic regions such as US-West, US-East, Europe, Australia, Canada, or GOV.
Username	Username
Password	Password
Threat Severity	Allows you to select one or more threat severity levels to filter your results by.
Fetch Detections Tags	If checked, specifies the ingestion of detection tags.

McAfee MVISION EDR Threats



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.0

Configuration Activity Log

Region

Europe

Tenant Location

Username

Username

Password

Password

Threat Severity

Threat Severity Filter

☐ Level 0

☐ Level 1

☐ Level 2

☐ Level 3

☐ Level 4

☐ Level 5

☐ Fetch Detections Tags

If checked, specifies that detections tags are ingested.

How frequent should we pull information from this feed?

Every Day

Set indicator status to...

Active

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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.

McAfee MVISION EDR CDF
Version 1.0.1

9

ThreatQ Mapping

McAfee MVISION EDR Threats

The McAfee 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"
      }
    }
  ]
}
```

ThreatQ 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	
.threats[].type	indicator.attribute	Threat Type	.threats[].firstDetected	pe	
.threats[].severity	indicator.attribute	Severity	.threats[].firstDetected	s1	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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 McAfee 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"
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.detections[].tags[]	tag.name	n/a	n/a	@MSI._reg_ep0029_intranet	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.

McAfee MVISION EDR Threats

METRIC	RESULT
Run Time	1 minute
Indicators	6
Indicator Attributes	30

Change Log

- **Version 1.0.1**
 - Added expired token reauthorization.
- **Version 1.0.0**
 - Initial release