ThreatQuotient

McAfee TIE Operation Guide

Version 1.0.1

August 09, 2021

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

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.

Versioning

- Current integration version `1.0.1`
- Supported on ThreatQ versions >= `4.30.0`

Introduction

The McAfee TIE operation provides **Get** and **Set** actions.

The **Get** action queries the configured TIE server for any threat information for the indicator in question.

The **Set** operation sets the Enterprise ThreatLevel of the indicator in question on the McAfee TIE server.

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 operation 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 operation and will require user confirmation before proceeding.
6. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* 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
EPO IP	The IP Address of the McAfee EPO server.
EPO Login	Your EPO login.
EPO Password	Your EPO password.
EPO Port	Optional - If left empty, the default port, **8443**, will be used.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUB-TYPE
Query Reputation	Query a McAfee TIE server for additional attributes relevant to certain indicators.	Indicator	MD-5, SHA-1, SHA-256
Set Reputation	Set the Enterprise reputation for an indicator. There are several versions on this action: • Set Reputation Might Be Malicious • Set Reputation Most Likely Malicious • Set Reputation Unknown • Set Reputation Known Malicious	Indicator	MD-5, SHA-1, SHA-256

Query Reputation

This action will create up to 12 attributes for an indicator depending upon how much information the McAfee ecosystem has about the selected indicator. The table below summarizes these 12 attributes. Each cell in the table represents the attribute name in ThreatQ.

MCAFEE SOURCE	REPUTATION	CREATED AT	COUNT	PREVALENCE
Global Threat Intelligence (GTI)	Global Threat Intelligence Trust Level	Global Threat Intelligence Created At	Global Threat Intelligence Count	Global Threat Intelligence Prevalence
Advanced Threat Defense (ATD)	Advanced Threat Defense Trust Level	Advanced Threat Defense Created At	Advanced Threat Defense Count	Advanced Threat Defense Prevalence
Enterprise	Enterprise Reputation	Enterprise Created At	Enterprise Count	Enterprise Prevalence

Attribute Values Mapping

The reputation attribute values are created from the mapping given in the table below.

MCAFEE REPUTATION SCORE	THREATQ TRUST LEVEL ATTRIBUTE VALUE
0	Not Set
1	Known Malicious
15	Most Likely Malicious
30	Might Be Malicious
50	Unknown
70	Might Be Trusted
85	Most Likely Trusted
100	Known Trusted

Set Reputation

This action allows you to set the Enterprise reputation 'trust level' in the McAfee TIE Database.

Attribute Values Mapping

The reputation attribute values are created from the mapping given in the table below.

MCAFEE REPUTATION SCORE	THREATQ TRUST LEVEL ATTRIBUTE VALUE
1	Known Malicious
15	Most Likely Malicious
30	Might Be Malicious
50	Unknown
100	Known Trusted

Change Log

- **Version 1.0.1**
  - Updated dependancies.
- **Version 1.0.0**
  - Initial Release