ThreatQuotient

McAfee Active Response (AR) Operation User Guide

Version 2.0.3

November 01, 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	2.0.3
Compatible with ThreatQ Versions	>= 4.31.0
Support Tier	ThreatQ Supported

Introduction

The McAfee Active Response (AR) Operation enables users to enrich indicators from McAfee AR.

The operation provides the following actions:

- **Query Hash** - queries McAfee Active Response for sightings of hashes on deployed agents.
- **Query Netflow -** queries McAfee Active Response for traffic related to an IP Address, either as a source or destination.

The operation is compatible with the following indicator types:

- IP Address
- MD5
- SHA-1
- SHA-256

Prerequisites

The following items are required to run the McAfee AR Operation.

- A route between ThreatQ and McAfee ePO.
- The following McAfee products:
    - ePO with an installed Active Response extension.
    - Active Response server connected to ePO.
- McAfee DXL and Active Response SDKs installed in ThreatQ. This is performed after installing the operation and before configuring it in the ThreatQ UI.

Installing McAfee DXL and Active Response SDKs

Follow the steps below for the configuration.

1. SSH into ThreatQ.
2. Activate Python 3.5:

```
source /opt/threatq/python/bin/activate
```

3. Install the McAfee DXL and AR SDKs:

```
pip install dxlclient dxlmarclient
```

4. Generate certificates for authenticating the connection between ThreatQ and McAfee ePO.

   Before executing the commands, confirm that you have the hostname/IP address, username and password for ePO available.

```
source /opt/threatq/python/bin/activate

cd /var/tmp

python -m dxlclient provisionconfig /var/tmp/dxl_certs/ <McAfee
ePO Hostname or IP Address> threatq-certs
```

5. Change the owner of the generated files to `apache`. This is the system user that ThreatQ uses to execute the operations in the UI.

```
sudo chown -R apache:apache dxl_certs/
```

6. Add the generated certificates to the trusted store in McAfee ePO:
    a. Log into ePO as an admin via the UI.
    b. Navigate to **Server Settings -> DXL Topic Authorization**.
    c. Click on the **Edit** button in the lower right corner and select the topics:
        - `TIE Server Set Enterprise Reputation`
        - `TIE Server External Reputation Provider Event`
        - `Active Response Server API`

   d. With the topics selected, click on **Actions**, located in the lower-left corner, and select **Send Certificates**.
   e. Select the entry in the certificate list called `threatq-certs` and click **OK**.
   f. Click **Save** when you return to the previous page.
   g. Log out of ePO.

7. Log into the ThreatQ UI to configure and then enable the operation.

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 operation 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.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

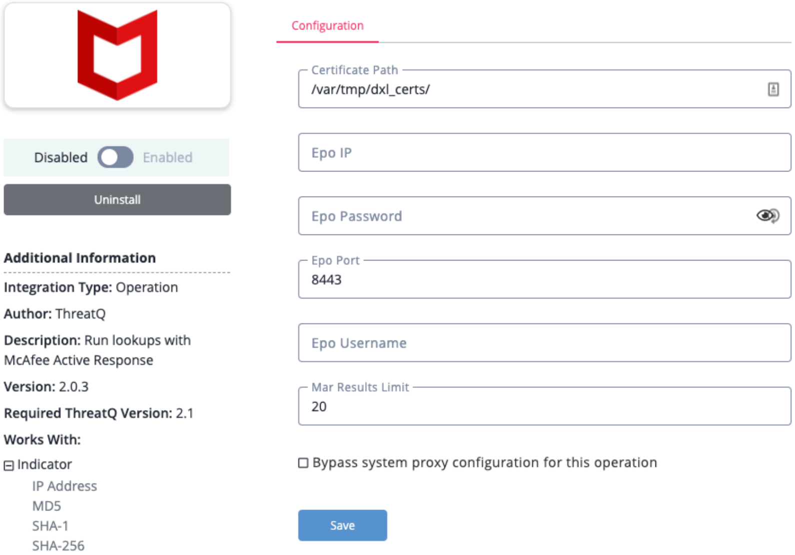
Configuration

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

PARAMETER	DESCRIPTION
Certificate Path	Enter the path to the certificate for McAfee MAR. The default is `/var/tmp/dxl_certs/`.
ePO IP	Enter the host or IP address for ePO.
ePO Port	Enter the ePO communication port. The default is 8443, which can be changed if needed.
ePO Username	Enter the username for ePO.
ePO Password	Enter the password for ePO.
MAR Result Limit	The maximum number of items to return from MAR. The default value is 20.



Configuration

Certificate Path: /var/tmp/dxl_certs/

Epo IP

Epo Password

Epo Port: 8443

Epo Username

Mar Results Limit: 20

□ Bypass system proxy configuration for this operation

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Run lookups with McAfee Active Response

Version: 2.0.3

Required ThreatQ Version: 2.1

Works With:

⊟ Indicator
- IP Address
- MD5
- SHA-1
- SHA-256

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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query Hash	Queries McAfee Active Response for sightings of hashes on deployed agents	Indicator	MD5, SHA-1, SHA-256
Query Netflow	Queries McAfee Active Response for traffic related to an IP Address, either as a source or destination	Indicator	IP Address

Query Hash

The Query Hash action queries McAfee Active Response for sightings of hashes on deployed agents. The operation uses the McAfee SDK to execute the search actions on ePO.

Query Netflow

The Query Netflow action queries McAfee Active Response for traffic related to an IP Address, either as a source or destination. The operation uses the McAfee SDK to execute the search actions on ePO.

This action has the following configutation options:

OPTION	DESCRIPTION
Destination IP	Search for the IP Address as a destination IP.
Source IP	Search for the IP Address as a source IP.

Change Log

- **Version 2.0.3**
  - Updated ThreatQ UI configurations for the operation
- **Version 1.0.0**
  - Initial release