ThreatQuotient

Trellix TIE Operation

Version 1.3.0

April 01, 2025

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	1.3.0
Compatible with ThreatQ Versions	>= 6.7.3
Support Tier	ThreatQ Supported

Introduction

The Trellix TIE operation provides **Get** and **Set** actions against a TIE-configured server.

- The **Get** action queries the configured TIE server for any threat information for the indicator in question.
- The **Set** action sets the Enterprise Threat Level of the indicator in question on the Trellix TIE server.

The operation provides the following actions:

- **Query Reputation** - queries a Trellix TIE server for additional attributes relevant to certain indicators.
- **Set Reputation** - sets the Enterprise reputation for an indicator.

The operation is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256

Prerequisites

The integration requires the following:

- ePO hostname or IP Address, ePO username and ePO Password.
- The OpenDXL Python client used by this integration must have permission to send messages to the `/mcafee/service/tie/file/reputation/set` topic which is part of the `TIE Server Set Enterprise Reputation` authorization group. Run the `Query Reputation` action to generate the ePO managed certificates. Then log into Trellix ePO console to authorize the generated credentials.

  The following page provides an example of authorizing a Python client to send messages to an `authorization group`. While the example is based on McAfee Active Response (MAR), the instructions are the same with the exception of swapping the `TIE Server Set Enterprise Reputation` `authorization group` in place of `Active Response Server API`:

  https://opendxl.github.io/opendxl-client-python/pydoc/marsendauth.html

  Additionally, all prerequisites from the following link should be fulfilled:

  https://opendxl.github.io/opendxl-tie-client-python/pydoc/basicsetreputationexample.html#prerequisites

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 .whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the .whl file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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
PO IP	The IP Address of the Trellix 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. 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 Reputation	Query a Trellix TIE server for additional attributes relevant to certain indicators.	Indicator	MD-5, SHA-1, SHA-256
Set Reputation Might Be Malicious	Set the Enterprise reputation for an indicator.	Indicator	MD5, SHA-1, SHA-256
Set Reputation Most Likely Malicious	Set the Enterprise reputation for an indicator.	Indicator	MD5, SHA-1, SHA-256
Set Reputation Unknown	Set the Enterprise reputation for an indicator.	Indicator	MD5, SHA-1, SHA-256
Set Reputation Known Malicious	Set the Enterprise reputation for an indicator.	Indicator	MD5, SHA-1, SHA-256
Set Reputation Known Trusted	Set the Enterprise reputation for an indicator.	Indicator	MD5, SHA-1, SHA-256
Set Reputation Known Trusted Installer	Set the Enterprise reputation for an indicator.	Indicator	MD5, SHA-1, SHA-256

Query Reputation

The Query Reputation action will create several attributes for an indicator depending upon how much information the Trellix ecosystem has about this indicator.

The action uses the function `get_file_reputation` from `dxltieclient` library. See the following for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/basicgetreputationexample.html.

Sample Response:

```
{
  "1": {
    "trustLevel": 1,
    "createDate": 1742561512,
    "attributes": {
      "2120340": "2134902792"
    },
    "providerId": 1
  },
  "3": {
    "trustLevel": 50,
    "createDate": 1742561512,
    "attributes": {
      "2101652": "0",
      "2114965": "0",
      "2098277": "0",
      "2139285": "289919230306943286",
      "2111893": "1",
      "2123156": "0",
      "2102165": "1742561512"
    },
    "providerId": 3
  }
}
```

ThreatQuotient provides the following mapping for the action based on items within the provider information (`.1` and `.3`).

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.trustLevel`	Indicator.Attribute	`{PROVIDER_NAME} Trust Level`	N/A	`Unknown`	Converted to string according to `Trust Level Mapping`
`.createDate`	Indicator.Attribute	`{PROVIDER_NAME} Created At`	N/A	`Fri Mar 21 12:51:52 2025`	Converted to human readable timestamp
`.attributes[PREVALENCE_ID]`	Indicator.Attribute	`{PROVIDER_NAME} Prevalence`	N/A	`0`	`PREVALENCE_ID` taken from `File Enterprise Attributes Mapping`
`.attributes[DETECTION_COUNT_ID]`	Indicator.Attribute	`{PROVIDER_NAME} Count`	N/A	N/A	`DETECTION_COUNT_ID` taken from `File Enterprise Attributes Mapping`

File Provider Mapping

The following is the File provider mapping for the action. See the following for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.constants.html#dxltieclient.constants.FileProvider.

TRELLIX PROVIDER ID	TRELLIX PROVIDER NAME	THREATQ PROVIDER NAME
1	GTI	GTI
3	ENTERPRISE	Enterprise
5	ATD	ATD

Trust Level Mapping

The reputation attribute values are created from the mapping given in the table below. See the following for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.constants.html#dxltieclient.constants.TrustLevel.

TRELLIX 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
99	Known Trusted
100	Known Trusted Installer

File Enterprise Attributes Mapping

The following is the File Enterprise Attributes mapping for the action. See the following for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.constants.html#dxltieclient.constants.FileEnterpriseAttrib.

TRELLIX FILE ENTERPRISE ATTRIBUTE ID	TRELLIX FILE ENTERPRISE ATTRIBUTE NAME	THREATQ FILE ENTERPRISE ATTRIBUTE NAME
2113685	DETECTION_COUNT	Count
2101652	PREVALENCE	Prevalence

Set Reputation Might Be Malicious

The Set Reputation Might Be Malicious action allows the user to set the Enterprise reputation `trust level` for a hash in the Trellix TIE Database to `Might Be Malicious`

The action uses the function `set_file_reputation` from `dxltieclient` library. See the following link for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.client.html?highlight=set_file_reputation#dxltieclient.client.TieClient.set_file_reputation.

Set Reputation Most Likely Malicious

The Set Reputation Most Likely Malicious action allows the user to set the Enterprise reputation `trust level` for a hash in the Trellix TIE Database to `Most Likely Malicious`

The action uses the function `set_file_reputation` from `dxltieclient` library. See the following link for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.client.html?highlight=set_file_reputation#dxltieclient.client.TieClient.set_file_reputation.

Set Reputation Unknown

The Set Reputation Unknown action allows the user to set the Enterprise reputation `trust level` for a hash in the Trellix TIE Database to `Unknown`

The action uses the function `set_file_reputation` from `dxltieclient` library. See the following link for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.client.html?highlight=set_file_reputation#dxltieclient.client.TieClient.set_file_reputation.

Set Reputation Known Malicious

The Set Reputation Known Malicious action allows the user to set the Enterprise reputation `trust level` for a hash in the Trellix TIE Database to `Known Malicious`

The action uses the function `set_file_reputation` from `dxltieclient` library. See the following link for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.client.html?highlight=set_file_reputation#dxltieclient.client.TieClient.set_file_reputation.

Set Reputation Known Trusted

This operation allows the user to set the Enterprise reputation `trust level` for a hash in the Trellix TIE Database to `Known Trusted`

This operation uses the function `set_file_reputation` from `dxltieclient` library. See the following link for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.client.html?highlight=set_file_reputation#dxltieclient.client.TieClient.set_file_reputation.

Set Reputation Known Trusted Installer

The Set Reputation Known Trusted Installer action allows the user to set the Enterprise reputation `trust level` for a hash in the Trellix TIE Database to `Known Trusted Installer`

The action uses the function `set_file_reputation` from `dxltieclient` library. See the following link for more information: https://opendxl.github.io/opendxl-tie-client-python/pydoc/dxltieclient.client.html?highlight=set_file_reputation#dxltieclient.client.TieClient.set_file_reputation.

Change Log

- **Version 1.3.0**
  - Updated integration name from McAfee TIE Operation to Trellix TIE Operation.
  - Updated the minimum ThreatQ version to 6.7.3.
- **Version 1.2.0**
  - Automatic certificate regeneration will now only be performed if credentials are changed.
- **Version 1.1.0**
  - Fixed a Reputation bug.
  - Added `Set Reputation Known Trusted Installer` action.
  - Attribute names synced with McAfee TIE Reputation Change integration.
- **Version 1.0.1**
  - Updated dependancies.
- **Version 1.0.0**
  - Initial Release