

ThreatQuotient



Trellix AX Operation Guide

Version 1.1.0

February 22, 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

- Integration Details..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- Actions 9
 - Submit..... 10
 - Configuration Options..... 10
 - Get Reports 12
 - Add YARA Rule..... 13
 - Configuration Options..... 13
 - Remove YARA Rule..... 14
 - Configuration Options..... 14
 - Query Alerts 15
 - Configuration Options..... 15
- Change Log..... 17

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 © 2023 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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
-----------------------------	-------

Compatible with ThreatQ Versions	>= 4.10.0
----------------------------------	-----------

Support Tier	ThreatQ Supported
--------------	-------------------

ThreatQ Marketplace	https:// marketplace.threatq.com/ details/trellix-ax-operation
---------------------	---

Introduction

The Trellix AX Operation provides you with the ability to submit a File, URL, or FQDN for sandboxing, add or remove YARA rules, and query alerts.

You can also query your Trellix AX appliance using indicators from ThreatQ to find any alerts related to those indicators. The operation also allows you to seamlessly add and remove YARA rules from your Trellix AX appliance.

The operation provides the following actions:

- **Submit** - submits a file or URL/FQDN to Trellix AX.
- **Get Reports** - retrieves all reports for the sample from Trellix AX.
- **Add YARA Rule** - adds a YARA rule to ThreatQ from Trellix AX.
- **Remove YARA Rule** - removes YARA rules from ThreatQ.
- **Query Alerts** - queries alerts in Trellix AX.

The operation can be run on the following object types:

- Files
- Indicators (Email Address, FQDN, IP Address, MD5, URL)
- Signatures (YARA Rule)



The Trellix AX operation replaces the FireEye AX operation as of version 1.1.0.

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
Trellix AX Host	Your Host or IP of your Trellix AX instance.
Trellix Username	Your Trellix AX username for the API.
Trellix Password	Your Trellix AX password for the API.
Trellix Profiles	The sandboxing profiles to use to sandbox the samples.

Example: `win-7sp1m` - see the Trellix AX UI for more options.

You can specify multiple profiles using a comma-separated format.



This parameter can be overridden using action-specific parameters.

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 Trellix AX operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Submit	Submits a file or URL/FQDN to Trellix AX.	File, Indicator	Indicator - URL, FQDN
Get Reports	Retrieves all reports for the sample from Trellix AX.	File, Indicator	Indicator - URL, FQDN
Add YARA Rule	Adds a YARA rule to ThreatQ from Trellix AX.	Signature	YARA
Remove YARA Rule	Removes YARA rules from ThreatQ.	Signature	YARA
Query Alerts	Queries alerts in Trellix AX.	Indicator, File	Indicator - FQDN, Filename, Email, IP Address

Submit

The Submit action will submit a file (attachment) or a URL/FQDN to Trellix AX for sandboxing.

POST `https://{host_url}/wsapis/v2.0.0/submissions/url`

Sample Response:

```
{
  "rawType": "com.fireeye.v200.rest.model.SubmitUrlResponse",
  "type": "com.fireeye.v200.rest.model.RestModelBase",
  "entity": {
    "response": [
      {
        "id": "L31",
        "link": {
          "rel": "status",
          "href": "/submissions/status/L31"
        },
        "submission_details": "[{\\"vnc_port\\":[],\\"job_ids\\":[],\\"id\\":501,\\"uuid\\":\\"5b8d6f3a-3093-47df-9a41-c57e6c5319d3\\"}]"
      }
    ]
  }
}
```

Configuration Options

The action provides the following configuration options:

PARAMETER	DESCRIPTION
Run Using Custom Application	Allows you to run the sample with a specific application within the sandbox profile. This value is a number that corresponds to the custom application. The default setting is 0 - this tells Trellix to determine the application to use.
Timeout	Determines how long the sandbox will take to "timeout" after inactivity. The default setting is 500.
Priority	Sets a priority for the task. Options include:

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none">• Normal (default)• Urgent
Profiles List (overrides config)	This parameter is a list of profiles to use to sandbox the sample. The action will use the profiles set in the UI configuration if this is left blank. Otherwise, this will override the profiles listed in the UI configuration
Force	This parameter will force resubmit a sample. If this is set to False, it will mark the sample as a duplicate and will not resubmit it.
Analysis Type	Set the Analysis Type. The default setting is Sandbox.
Prefetch	<p>Determine the file target based on an internal determination rather than browsing to the target location.</p> <p>The Analysis Type must be set to 1 if you are using the Sandbox.</p>

Get Reports

The Get Reports action will get all the reports for the sample, with the only condition being that the sample (in ThreatQ) has an attribute with the name "Trellix AX Submission ID" and the value will be the submission ID.

For each of these attributes, it will fetch a report correlating to the submission ID. If submission results are found, results will be shown and the full JSON report will be uploaded and related to the sample in ThreatQ.

GET `https://{host_url}/wsapis/v2.0.0/submissions/results/{submissionID}`

Sample Response:

```
{
  "alert": [
    {
      "explanation": {
        "malwareDetected": {
          "malware": [
            {
              "md5Sum": "be5d431e32bea4c4bbfc331e233f5a7b",
              "sha256":
"437d73cfff51cd3571b306430484bb781af93c45011c96cfc45eb2d6caa48a68"
            }
          ]
        },
        "osChanges": []
      },
      "src": {},
      "alertUrl": "https://10.20.0.133/malware_analysis/analyses?maid=500",
      "action": "notified",
      "attackTime": "2023-02-13 12:56:01 +0000",
      "dst": {},
      "applianceId": "AC1F6B720474",
      "id": 500,
      "name": "MALWARE_OBJECT",
      "severity": "MINR",
      "uuid": "4456d46b-d0e9-4b66-9ecc-0dfde7a67f07",
      "ack": "no",
      "product": "MAS",
      "vlan": 0,
      "malicious": "no"
    }
  ],
  "appliance": "MAS",
  "version": "MAS (MAS) 9.1.1.956704",
  "msg": "concise",
  "alertsCount": 1
}
```

Add YARA Rule

The Add YARA Rule action allows you to add YARA rules from ThreatQ to Trellix AX.

POST `https://{host_url}/wsapis/v2.0.0/customioc/yara/add/{file_type}`

Sample Response:

```
sample
```

Configuration Options

The action provides the following parameters:

PARAMETER	DESCRIPTION
Content Type	Specify which content type the new YARA rule should be applied to. Options include: <ul style="list-style-type: none">• Active content: Extracts the macros from files and executes special YARA rules on them.• Base (default): If file contains a macro, don't extract and analyze macros; only analyze the base file.• All: Does both
File Type	The file type of the YARA rules file being submitted, such as exe, pdf, or ppt. The default setting is Common .

Remove YARA Rule

The Remove YARA Rule action allows you to remove YARA rules from ThreatQ.

POST `https://{host_url}/wsapis/v2.0.0/customioc/yara/remove/{file_type}/{yara_rule}`

Sample Response:

```
sample
```

Configuration Options

The action provides the following parameters:

PARAMETER	DESCRIPTION
Content Type	Specify which content type the new YARA rule should be applied to. Options include: <ul style="list-style-type: none">• Active content: Extracts the macros from files and executes special YARA rules on them.• Base (default): If file contains a macro, don't extract and analyze macros; only analyze the base file.• All: Does both
File Type	The file type of the YARA rules file being submitted, such as exe, pdf, or ppt. The default setting is Common .

Query Alerts

The Query Alerts action allows you to query alerts in Trellix AX.



This action only applies to FQDNs, Filenames, Emails, and IP Addresses.

```
GET https://{host_url}/wsapis/v2.0.0/alerts
```



Sample Response:

```
{
  "alert": [],
  "appliance": "MAS",
  "version": "MAS (MAS) 9.1.1.956704",
  "msg": "extended",
  "alertsCount": 0
}
```

Configuration Options

The action provides the following parameters:

PARAMETER	DESCRIPTION
Start Time	<p>Set the start time to search for alerts. This is used in conjunction with the Duration parameter. You cannot use this at the same time as using the End Time parameter</p> <ul style="list-style-type: none">• Format: YYYY-MM-DDTHH:mm:ss.sss-OH:om• Example: 2019-02-21T16:30:00.000-07:00
End Time	<p>Set the end time to search for alerts. This is used in conjunction with the Duration parameter. You cannot use this at the same time as using the Start Time parameter.</p> <ul style="list-style-type: none">• Format : YYYY-MM-DDTHH:mm:ss.sss-OH:om• Example: 2019-02-21T16:30:00.000-07:00

PARAMETER	DESCRIPTION
	 If no end time or start time is provided, the end time will be set to the current date/time
Duration	Set the amount of time you want to either look after a start time or before an end time. The default setting is 12 hours.
Info Level	<p>Set the detail level of the alerts. Options include:</p> <ul style="list-style-type: none">• Concise (default)• Normal• Extended  Normal and Extended options will provide a very large alert and may take longer to download.

Change Log

- **Version 1.1.0**
 - Rebranded the operation from FireEye to Trellix to match vendor branding.
- **Version 1.0.2**
 - Fixed an issue where users were unable to add attributes for certain tables.
- **Version 1.0.1**
 - Fixed an issue with mapping popup windows.
 - Added failsafe to mapper to improve stability.
- **Version 1.0.0**
 - Initial Release