ThreatQuotient

VMRay Operation Guide

Version 1.2.0

January 30, 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 Indicator 10
Configuration Options 10
Submit File 11
Configuration Options 11
Get Report 12
Known Issues/Limitations 13
Change Log 14

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	1.2.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/vmray-operation

Introduction

The VMRay Operation is used to submit URLs, FQDNs and File Objects to VMRay for analysis and retrieve reports in PDF format.

The operation provides the following actions:

- **Submit Indicator** - submits an indicator to the VMRay platform.
- **Submit File** - Submits a file to the VMRay platform.
- **Get Report** - Retrieves the report for a submitted object.

The operation is compatible with Files and Indicator (FDQN, URL) object types.

> The VMRay Operation is required in order to use the VMRay CDF.

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
Hostname	Your VMRay instance hostname.
API Key	Your VMRay API Key.
Verify SSL	Enable or disable SSL verification.

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 VMRay operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Submit Indicator	Submits a supported indicator to the VMRay platform	Indicators	FQDN, URL
Submit File	Submits a file to the VMRay platform.	File	Attachment
Get Report	Retrieves the report for a submitted object.	Indicators	FQDN, URL

Notes

- By executing one of the submit actions, a `VMRay Sample ID` attribute is added to the object on which we ran the operation on.
- This `VMRay Sample ID` attribute will be used when executing the `get_report` action for fetching the submission report link.
- The attribute is automatically deleted when the report link is fetched for a completed analysis.

Submit Indicator

The Submit Indicator action submits an indicator for analysis.

```
POST https://cloud.vmray.com/rest/sample/submit
```

Configuration Options

The Submit Indicator action provides the following configuration options:

PARAMETER	TYPE	EXAMPLE	DEFAULT	NOTES
Data Retention	int	0	0	The amount of time in days, before submissions are automatically deleted from the VMRay server. Valid Options: 0, 60, 120, 180, 360. Value of 0 means it will not automatically delete.
Submission Comment	str	n/a	Some Comment	Comment for current indicator submission.
Tags	str	Some_Tag	n/a	Comma-separated list of tags for this submission.
Reputation Lookups & WHOIS Lookups	str	True	10	Indicates whether 'Reputation Analysis' and 'Analysis Artifacts' (applicable for file hashes and URLs) should be performed for the submitted sample.
Max Recursive Samples	int	1	10	Number of files to be analyzed. As example for a value of 10, by submitting a zip archive containing multiple files only the first 10 files would be analyzed.
Max Dynamic Analyses Per Sample	int	1	True	Protects the user by limiting the number of Dynamic Analyses that are performed for both the original sample as well as any recursive samples within the original object.

Submit File

The Submit File action submits a file for analysis.

`POST https://cloud.vmray.com/rest/sample/submit`

Configuration Options

The Submit File action provides the following configuration options:

PARAMETER	TYPE	EXAMPLE	DEFAULT	NOTES
tags	str	some_tag	n/a	Comma-separated list of tags for this submission.
Submission Comment	str	Some Comment	n/a	Comment for current indicator submission.

> When running the action `Submit File` on an Attachment with `Malware Safety Lock` enabled the file actually submitted to `VMRay` will be a zipped file, also the created `Filename` indicator will have a `.zip` extension. The Filename indicator will be the bridge relationship between the submitted file and the retrieved data from the CDF.

Get Report

The Get Report action can be executed for both Indicators and Attachments using the endpoint listed below. The action displays the submission status and the link for downloading the PDF report.

```
GET https://cloud.vmray.com/rest/sample/<sample_id>/vtis
```

Known Issues/Limitations

- By executing one of the submit actions, a `VMRay Sample ID` attribute is added to the object (the object which the action was executed on). This `VMRay Sample ID` attribute will be used when executing the `get_report` action for fetching the submission report link. The attribute is automatically deleted when the report link is fetched for a completed analysis.

Change Log

- **Version 1.2.0**
    - Updated the **Submit File** action to resolve a lost relationship issue that can occur between the submitted file and the retrieved indicators when running the VMRay CDF.
- **Version 1.1.1**
    - Added X-App-Name in the request header.
- **Version 1.1.0**
    - Added **Hostname** parameter to the operation's configuration page.
- **Version 1.0.0**
    - Initial release