ThreatQuotient

VMRay Action

Version 1.0.1

December 17, 2024

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	1.0.1
Compatible with ThreatQ Versions	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The VMRay action for ThreatQ submits a data collection of URL objects to the VMRay provider to query and analyze.

The integration provides the following action:

- **VMRay - Submit IOCs** - export IOCs to the VMRay platform for analysis.

The integration is compatible and returns enriched URL type indicators.

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing URL type indicators.
- Your VMRay API key.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

> ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

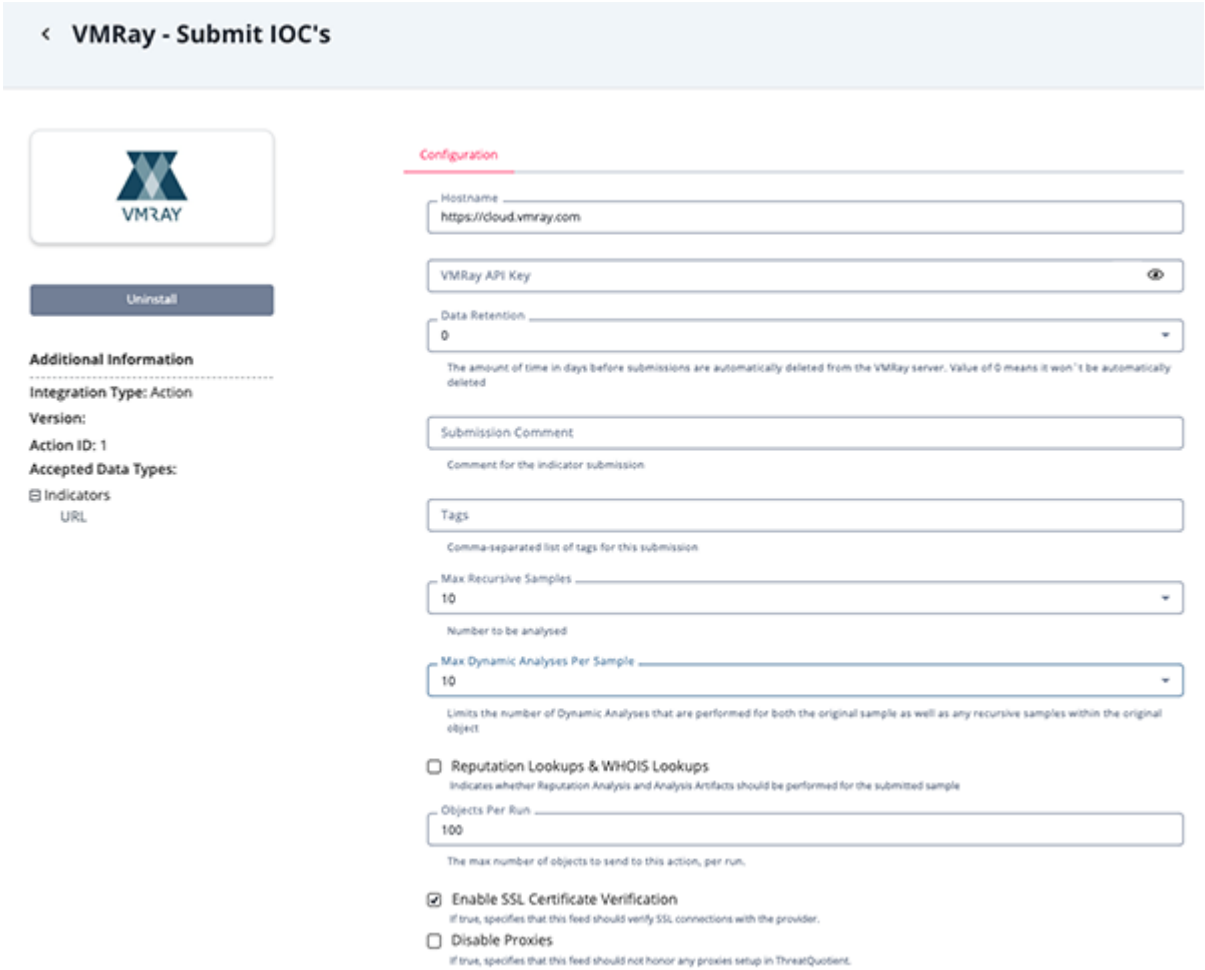
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Hostname	Enter your VMRay Hostname. The default value is https://cloud.vmray.com.
VMRay API Key	Enter your VMRay API Key.
Data Retention	Enter the amount of time in days before submissions are automatically deleted from the VMRay server.
Submission Comment	Enter a comment for the indicator submission.
Tags	Enter, in a comma-separated format, tags to attach to the submitted indicator.
Max Recursive Samples	Select the number of samples to be analyzed. Options include: ◦ 0 ◦ 1 ◦ 15 ◦ 20

PARAMETER	DESCRIPTION
	◦ 5 ◦ 10 ◦ 50
Max Dynamic Analyses Per Sample	Limits the number of Dynamic Analyses that are performed for both the original sample as well as any recursive samples within the original object. You can select from a range of 0 - 10.
Reputation Lookups & WHOIS Lookups	Enable this parameter if Reputation Analysis and Analysis Artifacts should be performed for the submitted sample.
Objects Per Run	The max number of objects to send to this action, per run.
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
VMRay - Submit IOCs	Export IOC's to VMRay platform to be analyzed.	Indicators	URL

VMRay - Submit IOCs

The VMRay - Submit IOCs action exports IOCs to VMRay platform to be analyzed

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

Sample Response:


```
{
    "data": {
        "errors": [],
        "jobs": [],
        "md_jobs": [],
        "reputation_jobs": [],
        "samples": [
            {
                "sample_child_sample_ids": [],
                "sample_container_type": null,
                "sample_created": "2016-06-01T14:21:53",
                "sample_display_url": "http://google.com",
                "sample_emailhash": null,
                "sample_filename": "sample.url",
                "sample_filesize": 17,
                "sample_id": 597114,
                "sample_imphash": null,
                "sample_is_multipart": false,
                "sample_md5hash": "c7b920f57e553df2bb68272f61570210",
                "sample_parent_sample_ids": [],
                "sample_password_protected": false,
                "sample_pe_signature": null,
                "sample_priority": 5,
                "sample_sha1hash": "234988566c9a0a9cf952cec82b143bf9c207ac16",
                "sample_sha256hash":
"aa2239c17609b21eba034c564af878f3eec8ce83ed0f2768597d2bc2fd4e4da5",
                "sample_ssdeephash": "3:N1KZK3uK:C03uK",
                "sample_type": "URL",
                "sample_url": "http://google.com",
                "sample_webif_url": "https://cloud.vmray.com/samples/597114",
                "submission_filename": "google.com"
            }
        ],
        "static_jobs": [],
        "submissions": [
            {
                "submission_analysis_cache_ids": [
                    13185823
                ],
                "submission_analyzer_mode_analysis_caching": "smart",
                "submission_analyzer_mode_analyzer_mode": "static_dynamic",
                "submission_analyzer_mode_archive_action": "sample",
```

```
                "submission_analyzer_mode_detonate_links_in_documents":
"smart",
                "submission_analyzer_mode_detonate_links_in_emails": "smart",
                "submission_analyzer_mode_disk_image_action":
"compound_sample",
                "submission_analyzer_mode_enable_reputation": false,
                "submission_analyzer_mode_enable_whois": false,
                "submission_analyzer_mode_id": 5238854,
                "submission_analyzer_mode_known_benign": false,
                "submission_analyzer_mode_known_malicious": false,
                "submission_analyzer_mode_max_dynamic_analyses_per_sample":
"1",
                "submission_analyzer_mode_max_recursive_samples": "1",
                "submission_analyzer_mode_ml_based_phishing_detection":
"normal",
                "submission_analyzer_mode_triage": "custom",
                "submission_analyzer_mode_triage_error_handling": null,
                "submission_api_key_id": 2162,
                "submission_billing_type": "analyzer",
                "submission_comment": null,
                "submission_created": "2024-03-14T11:36:24",
                "submission_deletion_date": "2024-05-13T11:36:24",
                "submission_dll_call_mode": null,
                "submission_dll_calls": null,
                "submission_document_password": null,
                "submission_enable_custom_av": false,
                "submission_enable_local_av": true,
                "submission_filename": "google.com",
                "submission_finish_time": "2024-03-14T11:36:24",
                "submission_finished": true,
                "submission_has_errors": false,
                "submission_has_recursive_errors": false,
                "submission_id": 14295353,
                "submission_interface_name": "VMRAY-Hamsters",
                "submission_ip_id": 3887692,
                "submission_ip_ip": "89.238.232.178",
                "submission_job_cache_ids": [],
                "submission_known_configuration": false,
                "submission_number_cached_analyses": 1,
                "submission_number_created_jobs": 0,
                "submission_original_filename": null,
                "submission_original_url": "google.com",
                "submission_parent_submission_id": null,
                "submission_prescript_force_admin": false,
                "submission_prescript_id": null,
                "submission_priority": 3,
                "submission_quota_type": "report",
                "submission_recursive": false,
                "submission_reputation_job_cache_id": null,
                "submission_reputation_lookup_cache_id": null,
```

```
                "submission_reputation_mode": "disabled",
                "submission_retention_period": 60,
                "submission_sample_id": 597114,
                "submission_sample_md5": "c7b920f57e553df2bb68272f61570210",
                "submission_sample_sha1":
"234988566c9a0a9cf952cec82b143bf9c207ac16",
                "submission_sample_sha256":
"aa2239c17609b21eba034c564af878f3eec8ce83ed0f2768597d2bc2fd4e4da5",
                "submission_sample_ssdeep": "3:N1KZK3uK:C03uK",
                "submission_score": 0,
                "submission_severity": "not_suspicious",
                "submission_shareable": false,
                "submission_status": "success",
                "submission_submission_metadata": "{}",
                "submission_submitter_email": null,
                "submission_system_time": null,
                "submission_tags": [],
                "submission_triage_error_handling": null,
                "submission_triage_stage": null,
                "submission_triaged": null,
                "submission_type": "api",
                "submission_used_cache": true,
                "submission_user_account_id": 1514,
                "submission_user_account_name": "ThreatQuotient",
                "submission_user_account_subscription_mode": null,
                "submission_user_account_type": "partner_demo",
                "submission_user_email": "ed.young@threatq.com",
                "submission_user_id": 6209,
                "submission_verdict": "clean",
                "submission_verdict_reason_code": null,
                "submission_verdict_reason_description": null,
                "submission_webif_url": "https://cloud.vmray.com/samples/
597114",
                "submission_whois_mode": "disabled"
            }
        ],
        "vt_jobs": [],
        "whois_jobs": []
    },
    "result": "ok"
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data.submissions[].submission_sample_id	Indicator.Attribute	VMRay Submission ID	N/A	597114	N/A

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	100
Indicator Attributes	100

Known Issues / Limitations

- It is recommended to use smaller collection sets (100 objects per run) when running this action.

Change Log

- **Version 1.0.1**
  - Users can now configure the hostname utilized by the integration.
  - Added the following new configuration parameters:
    - **Hostname** - allows you to enter the VMRay hostname for the integration to use.
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determine if the action should honor proxy settings set in the ThreatQ UI.
- **Version 1.0.0**
  - Initial release