ThreatQuotient

A Securonix Company

ReversingLabs Operation

Version 1.4.0

August 05, 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	1.4.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The ReversingLabs Operation enriches ThreatQ objects with context obtained from the ReversingLabs API. Once a submission has happened, users can decide to add these attributes to ThreatQ as well as download the original ReversingLabs Summary Report.

The operation provides the following actions:

- **Submit URL** - submits a URL to the appliance for analysis.
- **Submit File** - submits a File to the appliance for analysis.
- **URL Submission Status** - checks the processing status of a submitted URL.
- **Create PDF Report** - initiates the creation of a PDF analysis.
- **Get PDF Report** - retrieves a PDF analysis report.
- **Get Report Summary** - retrieves a summary of the analysis report.
- **Get Classification** - retrieves classified information.
- **Reanalyze Sample** - tries to send previously uploaded files to be analyzed again

The operation is compatible with the following object types:

- Files
- Indicators
    - FQDN
    - MD5
    - SHA-1
    - SHA-256
    - SHA-512
    - URL

Prerequisites

The following is required to run the integration:

- A ReversingLabs instance.
- A ReversingLabs API Token - see https://docs.reversinglabs.com/SpectraAnalyze/9.5.0/API%20Documentation/tokens/ for more information.

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 ReversingLabs hostname.
API Token	Enter your API Token used to authenticate with the ReversingLabs API.
Enable SSL Certificate Verification	Enable this parameter if the operation should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the operation should not honor proxies set in the ThreatQ UI.

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
Submit URL	Submit a URL to the appliance for analysis.	Indicators (URL)	URL
Submit File	Submit a File to the appliance for analysis.	Files	N/A
URL Submission Status	Check the processing status of a submitted URL.	Indicators	MD5, SHA-1, SHA-256 and SHA-512
Create PDF Report	Initiate the creation of a PDF analysis.	Indicators	MD5, SHA-1, SHA-256 and SHA-512
Get PDF Report	Retrieve a PDF analysis report.	Indicators	MD5, SHA-1, SHA-256 and SHA-512
Get Report Summary	Retrieve a summary of the analysis report.	Indicators	MD5, SHA-1, SHA-256 and SHA-512
Get Classification	Retrieve classified information.	Indicators	MD5, SHA-1, SHA-256 and SHA-512
Reanalyze Sample	Attempts to send previously uploaded files to be analyzed again.	Indicator	MD5, SHA-1, SHA-256, SHA-512

Submit URL

The Submit URL action is used to submit a URL to the appliance for analysis.

`POST https://a1000.reversinglabs.com/api/submit/url`

Sample Body:

```
{
  "url": "http://ilavorianmosy.eastus.cloudapp.azure.com/",
  "crawler": "local"
}
```

Sample Response:

```
{
    "code": 201,
    "message": "Done.",
    "detail": {
        "id": 18384734,
        "user": 889,
        "created": "2021-05-13T11:35:59.958687Z",
        "filename": "http://ilavorianmosy.eastus.cloudapp.azure.com/"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.detail.id	Indicator.Attribute	ReversingLabs Submission ID	18384734	Automatically added

Submit URL Run Parameters

The following run parameters are available for the Submit URL action:

PARAMETER	DESCRIPTION
Crawler	Specify crawler behavior. Options include • Private (local) • Spectra Intelligence (cloud)
URL Scheme Behaviour	Specify how FQDNs and URL indicators without a scheme should be handled as ReversingLabs requires a scheme defined for indicators. Options include: • Add "https" • Add "http"

Submit File

The Submit File action is used to submit a File to the appliance for analysis.

`POST https://a1000.reversinglabs.com/api/submit/file/`

Sample Body:

```
{
  "file": "{{BINARY FILE CONTENT}}",
  "tags": "threatq",
  "comment": "Submitted by ThreatQ"
}
```

Sample Response:

```
{
    "code": 201,
    "message": "Done.",
    "detail": {
        "id": 18384735,
        "sha1": "86bb5ed57999602fc4540ace6086a891c996e3f3",
        "user": 889,
        "created": "2021-05-13T11:37:50.768559Z",
        "filename": "0.exe.zip",
        "href": "/?q=86bb5ed57999602fc4540ace6086a891c996e3f3"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
detail.sha1	Indicator.Value	SHA-1	86bb5ed57999602fc4540ace6086a891c996e3f3	Automatically added

Submit File Run Parameters

The following run parameters are available for the Submit File action:

PARAMETER	DESCRIPTION
Tags	Optional - enter comma-separated user tags. Tags are case-sensitive and spaces and underscores are distinct.

URL Submission Status

The URL Submission Status action is used to check the processing status of a submitted URL.

`GET https://a1000.reversinglabs.com/api/uploads/v2/url-samples/<submission_id>`

Sample Response:


```
{
    "processing_status": "complete",
    "message": "",
    "report": {
        "discussion": [],
        "sha1": "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8",
        "sha256":
"cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097c21ca49bf5425",
        "sha512":
"239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c22f9cc6bdb2dc6916d3136835ff
803d9961bb7cbc7d5c3c0c80ac85a21731110eb8779427f7d8",
        "md5": "988604d5c50b9a95c3eff1843f1bd81c",
        "file_size": 11144469,
        "extracted_file_count": 25,
        "local_first_seen": "2021-04-27T09:25:23.652359Z",
        "local_last_seen": "2021-04-27T11:58:11.177472Z",
        "relationship_hash": "e9cec5b0f4c164d9578ed15ad268ef8082ecba86",
        "classification_source": 516,
        "trust_factor": 5,
        "threat_level": 5
    }
}
```


JSON trimmed for exemplification purposes.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.report.sha1	Indicator.Value	SHA-1	N/A	fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8	Automatically added
.report.sha256	Indicator.Value	SHA-256	N/A	b008be369fecaf0da3ee04d123c186dc4d676e9d5cc390cb81ff1982827f82e8	Automatically added
.report.networkthreatintelligence.analysis.last_analysis.serving_ip_address	Indicator.Value	IP Address	N/A	31.170.22.205	N/A
.report.networkthreatintelligence.analysis.last_analysis.domain	Indicator.Value	FQDN/IP Address	N/A	31.170.22.205	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.report.networkthreat intelligence.analysis.first _analysis	Indicator.Attribute	First Analysis	N/A	2025-02-25T17:09:34	N/A
.report.networkthreatin telligence.analysis.last_ analysis.analysis_time	Indicator.Attribute	Last Analysis	N/A	2025-07-23T12:30:52	N/A
.report.networkthreatin telligence.analysis.last_ analysis.availability_status	Indicator.Attribute	Last Analysis Availability Status	N/A	online	N/A
.report.networkthreat intelligence.classification	Indicator.Attribute	Classification	N/A	Malicious	Title cased
.report.networkthreat intelligence.reason	Indicator.Attribute	Classification Reason	N/A	third_party_reputation	N/A
.report.networkthreat intelligence.networkth reatintelligence.third_ party_reputations.sources.*	N/A	N/A	N/A	N/A	Entries added to a tabel if `.detection` is not `undetected`

Create PDF Report

The Create PDF Report action is used to initiate the creation of a PDF analysis.

`GET https://a1000.reversinglabs.com/api/pdf/<hash>/create`

Sample Response:

```
{
    "status_endpoint": "/api/pdf/fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8/
status",
    "download_endpoint": "/api/pdf/fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8/
download"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.status_endpoint	Indicator.Attribute	ReversingLabs Report Status Link	N/A	https://a1000.reversinglabs.com/api/pdf/<hash>/status	Automatically added
.download_endpoint	Indicator.Attribute	ReversingLabs Report Download Link	N/A	https://a1000.reversinglabs.com/api/pdf/<hash>/download	Automatically added

Get PDF Report

The Get PDF Report action is used to retrieve a PDF analysis report.

`GET https://a1000.reversinglabs.com/api/pdf/<sha-1>/download`

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
<returned_bytes>	Attachment.Data	ReversingLabs Report - <sha-1>.pdf	N/A	Automatically added

Get Report Summary

The Get Report Summary action is used to retrieve a summary of the analysis report.

`POST https://a1000.reversinglabs.com/api/samples/v2/list/`

Sample Body:

```
{
  "hash_values": [
    "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8"
  ]
}
```

Sample Response:


```
{
    "count": 1,
    "next": null,
    "previous": null,
    "results": [
        {
            "id": 68891607,
            "sha1": "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8",
            "sha256":
"cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097c21ca49bf5425",
            "sha512":
"239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c22f9cc6bdb2dc6916d3136835ff
803d9961bb7cbc7d5c3c0c80ac85a21731110eb8779427f7d8",
            "md5": "988604d5c50b9a95c3eff1843f1bd81c",
            "imphash": "",
            "category": "archive",
            "file_type": "Binary",
            "file_subtype": "Archive",
            "identification_name": "ZIP",
            "identification_version": "Generic",
            "file_size": 11144469,
            "extracted_file_count": 25,
            "local_first_seen": "2021-04-27T09:25:23.652359Z",
            "local_last_seen": "2021-04-27T11:58:11.177472Z",
            "classification_origin": {
                "sha1": "3ed9753623f756884ff9c30efceec58319ac0346",
                "sha256":
"0d6d9bbbfdceaa391310f69b37a04af230bddfa059a8f883a4a3c5bf1cb3e956",
                "sha512":
"29eb8a7c9796402cad00bcc92bddaf51a2a8f5978f98ccacb4687ee80b537d7acd2525e4d1f415
7fb86a09de5c39f27ed1f2bca0e5ba21b30133638be5e26954",
                "md5": "f831055b5bdacc126824b39363fd9894",
                "imphash": ""
            },
            "classification_reason": "user",
```

```
            "threat_status": "malicious",
            "trust_factor": 5,
            "threat_level": 5,
            "threat_name": "Script-VBS.Trojan.Mekotio",
            "tags": {
                "ticore": [
                    "cloud",
                    "entropy-high",
                    "contains-script",
                    "contains-pe"
                ],
                "user": [
                    "URL Download"
                ]
            }
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].classification	Indicator.Attribute	Classification	N/A	Goodware	Title cased.
.results[].category	Indicator.Attribute	Category	N/A	archive	N/A
.results[].file_type	Indicator.Attribute	File Type	N/A	Binary	N/A
.results[].file_subtype	Indicator.Attribute	File Subtype	N/A	Archive	N/A
.results[].identification_name	Indicator.Attribute	Identification Name	N/A	ZIP	N/A
.results[].identification_version	Indicator.Attribute	Identification Version	N/A	Generic	N/A
.results[].file_size	Indicator.Attribute	File Size	N/A	11144469	N/A
.results[].extracted_file_count	Indicator.Attribute	Extracted File Count	N/A	25	N/A
.results[].classification_reason	Indicator.Attribute	Classification Reason	N/A	user	N/A
.results[].riskscore	Indicator.Attribute	Risk Score	N/A	5	N/A
.results[].tags.ticore[]	Indicator.Attribute	TI Score Tag	N/A	cloud	N/A
.results[].tags.user[]	Indicator.Attribute	User Tag	N/A	URL Download	N/A
.results[].sha1	Indicator.Value	SHA-1	N/A	fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8	N/A
.results[].sha256	Indicator.Value	SHA-256	N/A	cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097...	N/A
.results[].sha512	Indicator.Value	SHA-512	N/A	239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c...	N/A
.results[].md5	Indicator.Value	MD5	N/A	988604d5c50b9a95c3eff1843f1bd81c	N/A

Get Classification

The Get Classification action retrieves classified information.

```
GET https://a1000.reversinglabs.com'api/samples/v3/<hash_value>/classification/
```

Sample Response:


```
{
  "classification": "goodware",
  "riskscore": 5,
  "first_seen": "2021-09-03T10:33:07",
  "last_seen": "2021-09-04T11:18:47",
  "classification_result": null,
  "classification_reason": "Antivirus",
  "classification_origin": null,
  "cloud_last_lookup": null,
  "data_source": "CLOUD",
  "sha1": "4cadcdb42dbfb6206b3dc17428d002e8b8645d1c",
  "sha256": "de4a002200e69ec3a058200a89707e225bc7c7e5b3393a0ec2743be21c49ef88",
  "sha512":
"0878015ce2bb5b56dc79206543174e91a205f9ef351887304b5feffad04587ed3eef4e58e5bbaa
56e5fa9432ed18857aadcbecfe7047ebfc172e9bc16984d41c",
  "md5": "2aa5c329c1f9685eee80ce1e3ae62588"
}
```


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[].sha1	Indicator.Value	SHA-1	N/A	fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8	N/A
.data[].sha256	Indicator.Value	SHA-256	N/A	54cc3f14e3e7caf9b032743e46d0e4292d50cf70a91b6737d8b23d7f0444882a	N/A
.data[].sha512	Indicator.Value	SHA-512	N/A	0878015ce2bb5b56dc79206543174e91a205f9ef351887304b5feffa...	N/A
.data[].md5	Indicator.Value	MD5	N/A	9efb9de422b5773c7a57af13a7acea79	N/A
.data[].first_seen	Indicator.Attribute	First Seen	N/A	2021-11-17T23:53:59Z	N/A
.data[].last_seen	Indicator.Attribute	Last Seen	N/A	2022-03-22T17:08:30Z	N/A
.data[].classification_reason	Indicator.Attribute	Classification Reason	N/A	Threat Signature	N/A
.data[].classification	Indicator.Attribute	Classification	N/A	Goodware	Title cased.
.data[].data_source	Indicator.Attribute	Data Source	N/A	CLOUD	N/A
.data[].riskscore	Indicator.Attribute	Risk Score	N/A	5	N/A

Reanalyze Sample

The Reanalyze Sample action will attempt to send previously uploaded files to be analyzed again in cloud.

`POST https://a1000.reversinglabs.com/api/samples/v2/list/`

Sample Body:

```
{
  "analysis": "cloud",
  "hash_value": [
    "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8"
  ]
}
```

Sample Response:

```
{
  "results": [
    {
      "detail": {
        "md5": "43cd20cee5136e648b047f747f9eb155",
        "sha1": "05e9a15a288b6b8bb97577d2ef4f93e346823fa2",
        "sha512":
"338446b5b3f09c0a26bf948253e947960a1885a89badb14549aa70acdae629b971727f04762b4a
87f2321d718b6a3d4b7b4e86bb4220c94dafc5ec17fd309191",
        "sha256":
"0fbd80ed779dd12d473a7d080dac53bda0f973dc2418eab7fc4b82faa07d2f29",
        "imphash": ""
      },
      "analysis": [
        {
          "code": 201,
          "name": "cloud",
          "message": "Sample is queued for analysis."
        }
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].detail.sha1	Indicator.Value	SHA-1	N/A	05e9a15a288b6b8bb97577d2ef4f93e346823fa2	N/A
.results[].detail.sha256	Indicator.Value	SHA-256	N/A	0fbd80ed779dd12d473a7d080dac53bda0f973dc2418eab7fc4b82faa07d2f29	N/A
.results[].detail.sha512	Indicator.Value	SHA-512	N/A	338446b5b3f09c0a26bf948253e947960a1885a89badb14549aa70acdae62...	N/A
.results[].detail.md5	Indicator.Value	MD5	N/A	43cd20cee5136e648b047f747f9eb155	N/A

Known Issues / Limitations

- The **Reanalyze Sample** action will only work if the file is already present in the Reversing Labs console. Some files can be manually fetched in the console.

Change Log

- **Version 1.4.0**
  - Upgraded the integration to use ReversingLabs API v2.
  - Added a new action: **Reanalyze Sample** - attempts to send previously uploaded files to be analyzed again in cloud.
  - Added the following new configuration parameter:
    - **API Token** - the API Token to authenticate with the ReversingLabs API.
  - Removed the following configuration parameters:
    - Username
    - Password
  - Updated the minimum ThreatQ version to 5.12.0.
  - Added a new entry to the **Known Issues / Limitations** section of the user guide: the **Reanalyze Sample** action will only work if the file is already present in the Reversing Labs console. Some files can be manually fetched in the console.
- **Version 1.3.0**
  - Added new Action: **Get Classified** for TiCloud support.
- **Version 1.2.0**
  - Added `Hostname` and `Verify SSL` parameters to the configuration page.
- **Version 1.1.0**
  - Added support for additional hash types.
- **Version 1.0.0**
  - Initial Release