ThreatQuotient

ReversingLabs Operation Guide

Version 1.0.0

May 21, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.34.0`

Introduction

The ReversingLabs Operation enriches ThreatQ objects with context obtained from the ReversingLabs API.

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 feed 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.
6. 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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Username	Your ReversingLabs username.
Password	Your ReversingLabs username password.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The operation provides the following actions.

ACTION	DESCRIPTION	OBJECT TYPES
Submit URL	Submit a URL to the appliance for analysis.	Indicators (URL)
Submit File	Submit a File to the appliance for analysis.	Files
URL Submission Status	Check the processing status of a submitted URL.	Indicators (URL)
Create PDF Report	Initiate the creation of a PDF analysis.	Indicators (SHA-1)
Get PDF Report	Retrieve a PDF analysis report.	Indicators (SHA-1)
Get Report Summary	Retrieve a summary of the analysis report.	Indicators (SHA-1)

Submit URL

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

```
POST https://a1000.reversinglabs.com/api/uploads/
```


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


ThreatQ 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 File

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

```
POST https://a1000.reversinglabs.com/api/uploads/
```


```
{
    "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"
    }
}
```


ThreatQ 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

URL Submission Status

This action is used to check the processing status of a submitted URL.

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


```
{
    "processing_status": "complete",
    "message": "",
    "report": {
        "discussion": [],
        "sha1": "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8",
        "sha256": "cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097c21ca49bf5425",
        "sha512":
"239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c22f9cc6bdb2dc6916d3136835ff803d9961bb7cbc7d5c3c0c80ac85a21731110
eb8779427f7d8",
        "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.

ThreatQ 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	fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8	Automatically added

Create PDF Report

This action is used to initiate the creation of a PDF analysis.

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

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

ThreatQ 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	https://a1000.reversinglabs.com/api/pdf/<sha-1>/status	Automatically added
.download_endpoint	Indicator.Attribute	ReversingLabs Report Download Link	https://a1000.reversinglabs.com/api/pdf/<sha-1>/download	Automatically added

Download PDF Report

This action is used to retrieve a PDF analysis report.

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

ThreatQ 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

This action is used to retrieve a summary of the analysis report.

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


```
{
    "count": 1,
    "next": null,
    "previous": null,
    "results": [
        {
            "id": 68891607,
            "sha1": "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8",
            "sha256": "cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097c21ca49bf5425",
            "sha512":
"239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c22f9cc6bdb2dc6916d3136835ff803d9961bb7cbc7d5c3c0c80ac85a21731110
eb8779427f7d8",
            "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": "0d6d9bbbfdceaa39131f69b37a04af230bddfa059a8f883a4a3c5bf1cb3e956",
                "sha512":
"29eb8a7c9796402cad00bcc92bddaf51a2a8f5978f98ccacb4687ee80b537d7acd2525e4d1f4157fb86a09de5c39f27ed1f2bca0e5ba21b3013
3638be5e26954",
                "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"
                ]
            }
        }
    ]
```

```
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.results[].category	Indicator.Attribute	Category	archive	N/A
.results[].file_type	Indicator.Attribute	File Type	Binary	N/A
.results[].file_subtype	Indicator.Attribute	File Subtype	Archive	N/A
.results[].identification_name	Indicator.Attribute	Identification Name	ZIP	N/A
.results[].identification_version	Indicator.Attribute	Identification Version	Generic	N/A
.results[].file_size	Indicator.Attribute	File Size	11144469	N/A
.results[].extracted_file_count	Indicator.Attribute	Extracted File Count	25	N/A
.results[].classification_reason	Indicator.Attribute	Classification Reason	user	N/A
.results[].threat_status	Indicator.Attribute	Threat Status	malicious	N/A
.results[].trust_factor	Indicator.Attribute	Trust Factor	5	N/A
.results[].threat_level	Indicator.Attribute	Threat Level	5	N/A
.results[].threat_name	Indicator.Attribute	Threat Name	Script-VBS.Trojan.Mekotio	N/A
.results[].tags.ticore[]	Indicator.Attribute	TI Score Tag	cloud	N/A
.results[].tags.user[]	Indicator.Attribute	User Tag	URL Download	N/A
.results[].sha1	Indicator.Value	SHA-1	fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8	N/A
.results[].sha256	Indicator.Value	SHA-256	cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097...	N/A
.results[].sha512	Indicator.Value	SHA-512	239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c...	N/A
.results[].md5	Indicator.Value	MD5	988604d5c50b9a95c3eff1843f1bd81c	N/A

Change Log

- **Version 1.0.0**
  - Initial Release