ThreatQuotient

A Securonix Company

Reversinglabs CDF

Version 1.1.0

July 22, 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	1.1.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The ReversingLabs CDF allows a user to ingest information on all the YARAs in the engine, as well as any information associated with matched malware samples.

ReversingLabs has a "hash harvesting" functionality. They have hundreds of millions of malware samples. A ReversingLabs customer can place a certain number of YARA signatures into their analytic engine. When a YARA signature is being run on the analytic engine, it is being run against the hundreds of millions of malware samples. If there is a match, the malware sample information is provided by ReversingLabs. This CDF will log into ReversingLabs and download information on all the YARAs in the engine. Additionally, any information associated with matched malware samples will be downloaded.

The Reversing Labs feed utilizes the following endpoints:

- **ReversingLabs** - returns data about Yara Signatures.
- **ReversingLabs Specific Yara Indicators (supplemental)** - returns data about Indicators matching a specified Yara Signature.
- **ReversingLabs Specific Yara Value (supplemental)** - returns the Yara Signature's content string.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Signatures
  - Signature Attributes

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 feed 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 feed and will require user confirmation before proceeding.

6. The feed will be added to the integrations page. You will still need to configure and then enable the feed.

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:

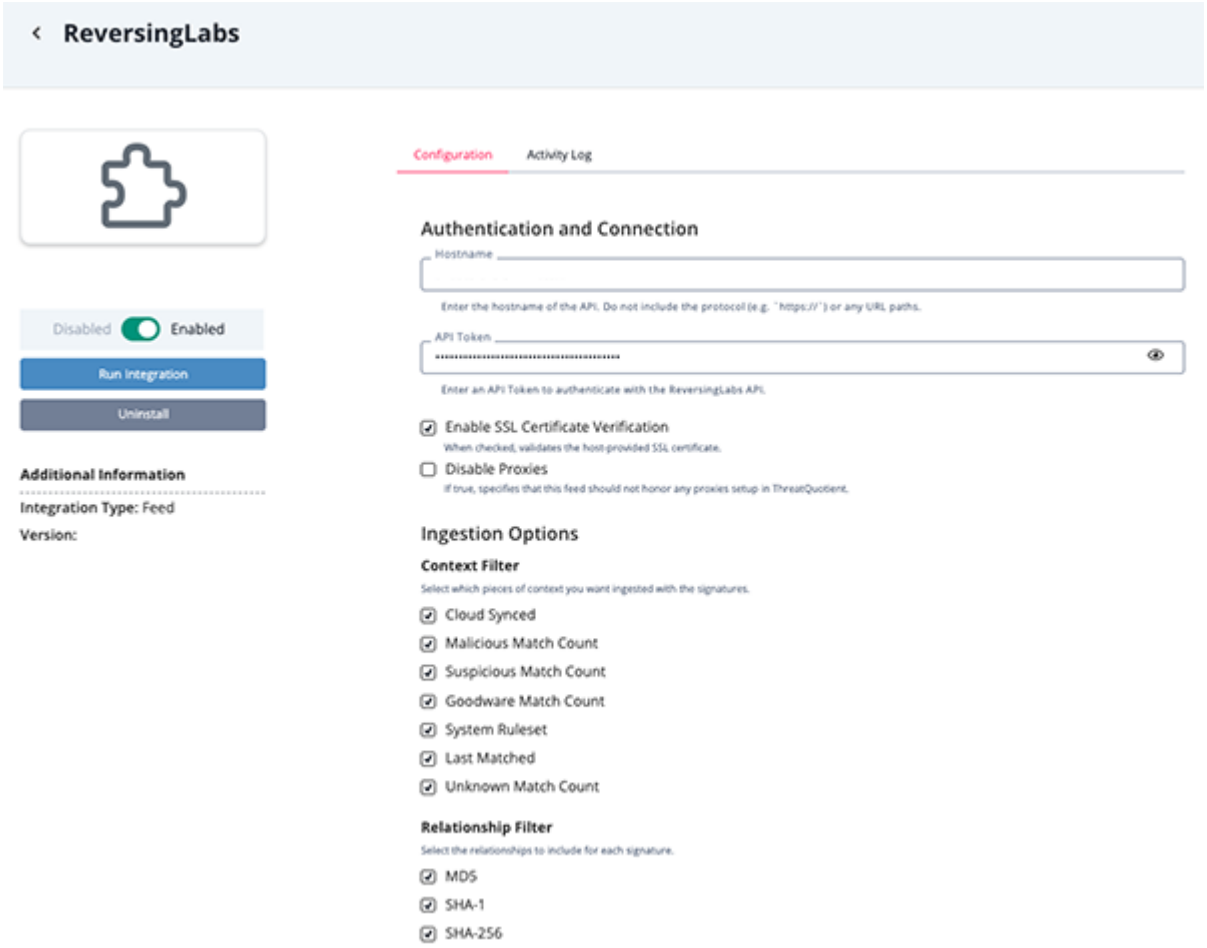
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
Host FQDN	Your Host Domain Name for ReversingLabs.
API Token	Your ReversingLabs API Token Credential.
Verify SSL Certificate Verification	Enable this option to have the integration verify the server's SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.
Context Filter	Select which pieces of context to ingest with the signatures. Options include: ◦ Cloud Synced *(default)* ◦ Malicious Match Count *(default)* ◦ Suspicious Match Count *(default)* ◦ Goodware Match Count *(default)* ◦ System Ruleset *(default)* ◦ Last Matched *(default)* ◦ Unknown Match Count *(default)*

PARAMETER	DESCRIPTION
Relationship Filter	Select the relationships to include for each signature. Options include: ◦ MD5 *(default)* ◦ SHA-1 *(default)* ◦ SHA-256 *(default)*



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.

ThreatQ Mapping

ReversingLabs

The ReversingLabs endpoint returns data about Yara Signatures.

`https://{{Host FDQN}}/api/yara/v2/rulesets/`

Sample Response:


```
    {
        "count": 25,
        "status": "all",
        "results": [
            {
                "status": "active",
                "known_match_count": 0,
                "cloud_synced": false,
                "malicious_match_count": 508,
                "suspicious_match_count": 0,
                "system_ruleset": false,
                "owner": "trial503",
                "last_matched": "2019-08-28T11:46:01.937420Z",
                "unknown_match_count": 0,
                "name": "Symantec"
            },
            {
                "status": "active",
                "known_match_count": 0,
                "cloud_synced": false,
                "malicious_match_count": 368,
                "suspicious_match_count": 0,
                "system_ruleset": false,
                "owner": "trial503",
                "last_matched": "2019-12-05T13:06:01.016378Z",
                "unknown_match_count": 0,
                "name": "CVE20180802ExploitRtfOPS"
            },
            ...
        ]
        "next": null,
        "source": "all",
        "type": "my",
        "previous": null
    }
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].name	Signature.name	YARA	N/A	Symantec	N/A
.results[].cloud_synced	Signature.Attribute	Cloud Synced	N/A	"False"	Updatable. User-configurable.
.results[].malicious_match_count	Signature.Attribute	Malicious Match Count	N/A	508	Updatable. User-configurable.
.results[].suspicious_match_count	Signature.Attribute	Suspicious Match Count	N/A	0	Updatable. User-configurable.
.results[].goodware_match_count	Signature.Attribute	Goodware Match Count	N/A	5	Updatable. User-configurable.
.results[].system_ruleset	Signature.Attribute	System Ruleset	N/A	"False"	Updatable. User-configurable.
.results[].last_matched	Signature.Attribute	Last Matched	N/A	2019-08-28T11:46:01.937420Z	Updatable. User-configurable.
.results[].unknown_match_count	Signature.Attribute	Unknown Match Count	N/A	0	Updatable. User-configurable.

ReversingLabs Specific Yara Indicators (Supplemental)

The ReversingLabs Specific Yara Indicators supplemental endpoint returns data about Indicators matching a specified Yara Signature.

`https://{{Host FDQN}}/api/yara/v2/ruleset/matches/`

Sample Response (Matches for Symantec):


```
{
        "count": 508,
        "next": null,
        "results": [
            {
                "threat_status": 3,
                "sha1": "1bbd23ab79dd40fcb5f29912713a245df60ef837",
                "sha256":
"3a1c43c01b3e5ddd6a8ecc0f4cfe67c6ecebab55d3782e211aecbd3c3c12e819",
                "created": "2019-08-28T11:46:01.937420Z",
                "file_type": "PE/Dll",
                "extracted_file_count": 1,
                "rule": "Symantec_KwampirsDrprPyld",
                "filename": "1bbd23ab79dd40fcb5f29912713a245df60ef837",
                "threat_name": "Win32.Trojan.Kwampirs",
                "downloadable": true,
                "file_size": 261120,
                "threat_level": 5,
                "trust_factor": 5,
                "cloud": false,
                "md5": "c1c5a80302410f8d9ca59bb84c2db05a"
            },
            {
                "threat_status": 3,
                "sha1": "1b5b446436de6d0bc88ecda5868adbce2daaef97",
                "sha256":
"7ac6be557f128d4b3cbfaebbb918dc7cd44e48acd797533ea28698491503b4a2",
                "created": "2019-08-28T11:17:02.653525Z",
                "file_type": "PE/Dll",
                "extracted_file_count": 1,
                "rule": "Symantec_KwampirsDrprPyld",
                "filename": "1b5b446436de6d0bc88ecda5868adbce2daaef97",
                "threat_name": "Win32.Trojan.Kwampirs",
                "downloadable": true,
                "file_size": 261120,
                "threat_level": 5,
                "trust_factor": 5,
                "cloud": false,
                "md5": "74bb0f8a4865571477b1aa4975980128"
            },
            ...
        ],
```

```
        "previous": null
    }
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].sha1	Indicator.Value	SHA-1	.results[].created	1bbd23ab79dd40fcb5f29912713a245df60ef837	User-Configurable.
.results[].sha256	Indicator.Value	SHA-256	.results[].created	3a1c43c01b3e5ddd6a8ecc0f4cfe67c6ecebab55d3782e211aecbd3c3c12e819	User-Configurable.
.results[].md5	Indicator.Value	MD5	.results[].created	c1c5a80302410f8d9ca59bb84c2db05a	User-Configurable.
.results[].file_type	Indicator.Attribute	File Type	.results[].created	Text/PowerShell	N/A
.results[].classification	Indicator.Attribute	Classification	.results[].created	Malicious	Updatable. Based on `ReversingLabs Classification Mapping`
.results[].classification_result	Indicator.Attribute	Threat Name	.results[].created	Script-PowerShell.Trojan.CobaltStrike	N/A
.results[].riskscore	Indicator.Attribute	Risk Score	.results[].created	10	Updatable.

ReversingLabs Classification Mapping

REVERSINGLABS CLASSIFICATION ID	REVERSINGLABS CLASSIFICATION
1	Goodware
2	Suspicious
3	Malicious

ReversingLabs Specific Yara Value (Supplemental)

The Reversing Labs Specific Yara Value supplemental endpoint returns the Yara Signature's content string.

`https://{{Host FDQN}}/api/yara/ruleset/content/`

Sample Response (Matches for Symantec):


```
    {
        "code": 200,
        "detail": {
            "content": "rule Symantec_KwampirsDrprPyld\n{\nmeta:\ncopyright =
\"Symantec\"\nfamily = \"Kwampirs\"\ndescription = \"Kwampirs dropper and main
payload
                components\"\nAuthor = \"CTM-DG\"\nstrings:\n$pubkey =\n{\n06
02 00 00 00 A4 00 00 52 53 41 31 00 08 00 00\n01 00 01 00 CD 74 15 BC 47 7E 0A
5E E4 35 22 A5\n97 0C
                65 BE E0 33 22 F2 94 9D F5 40 97 3C 53 F9\nE4 7E DD 67 CF 5F
0A 5E F4 AD C9 CF 27 D3 E6 31\n48 B8 00 32 1D BE 87 10 89 DA 8B 2F 21 B4 5D
0A\nCD 43 D7 B4 75 C9 19
                FE CC 88 4A 7B E9 1D 8C 11\n56 A6 A7 21 D8 C6 82 94 C1 66 11
08 E6 99 2C 33\n02 E2 3A 50 EA 58 D2 A7 36 EE 5A D6 8F 5D 5D D2\n9E 04 24 4A CE
4C B6 91 C0 7A C9 5C
                E7 5F 51 28\n4C 72 E1 60 AB 76 73 30 66 18 BE EC F3 99 5E
4B\n4F 59 F5 56 AD 65 75 2B 8F 14 0C 0D 27 97 12 71\n6B 49 08 84 61 1D 03 BA A5
42 92 F9 13 33 57 D9\n59
                B3 E4 05 F9 12 23 08 B3 50 9A DA 6E 79 02 36\nEE CE 6D F3 7F
8B C9 BE 6A 7E BE 8F 85 B8 AA 82\nC6 1E 14 C6 1A 28 29 59 C2 22 71 44 52 05 E5
E6\nFE 58 80 6E D4 95
                2D 57 CB 99 34 61 E9 E9 B3 3D\n90 DC 6C 26 5D 70 B4 78 F9 5E
C9 7D 59 10 61 DF\nF7 E4 0C B3\n}\n$network_xor_key =\n{\nB7 E9 F9 2D F8 3E 18
57 B9 18 2B 1F 5F D9
                A5 38\nC8 E7 67 E9 C6 62 9C 50 4E 8D 00 A6 59 F8 72 E0\n91 42
FF 18 A6 D1 81 F2 2B C8 29 EB B9 87 6F 58\nC2 C9 8E 75 3F 71 ED 07 D0 AC CE 28
A1 E7 B5 68\nCD CF F1
                D8 2B 26 5C 31 1E BC 52 7C 23 6C 3E 6B\n8A 24 61 0A 17 6C E2
BB 1D 11 3B 79 E0 29 75 02\nD9 25 31 5F 95 E7 28 28 26 2B 31 EC 4D B3 49 D9\n62
F0 3E D4 89 E4 CC F8 02
                41 CC 25 15 6E 63 1B\n10 3B 60 32 1C 0D 5B FA 52 DA 39 DF D1
42 1E 3E\nBD BC 17 A5 96 D9 43 73 3C 09 7F D2 C6 D4 29 83\n3E 44 44 6C 97 85 9E
7B F0 EE 32 C3 11 41 A3
                6B\nA9 27 F4 A3 FB 2B 27 2B B6 A6 AF 6B 39 63 2D 91\n75 AE 83
2E 1E F8 5F B5 65 ED B3 40 EA 2A 36 2C\nA6 CF 8E 4A 4A 3E 10 6C 9D 28 49 66 35
83 30 E7\n45 0E 05 ED 69
                8D CF C5 40 50 B1 AA 13 74 33 0F\nDF 41 82 3B 1A 79 DC 3B 9D
C3 BD EA B1 3E 04 33\n}\n$decrypt_string =\n{\n85 DB 75 09 85 F6 74 05 89 1E B0
01 C3 85 FF 74\n4F F6 C3
                01 75 4A 85 F6 74 46 8B C3 D1 E8 33 C9\n40 BA 02 00 00 00 F7
E2 0F 90 C1 F7 D9 0B C8 51\nE8 12 28 00 00 89 06 8B C8 83 C4 04 33 C0 85 DB\n74
16 8B D0 83 E2 0F 8A 92
```

```
                1C 33 02 10 32 14 38\n40 88 11 41 3B C3 72 EA 66 C7 01 00 00
B0 01 C3\n32 C0 C3\n}\n$init_strings =\n{\n55 8B EC 83 EC 10 33 C9 B8 0D 00 00
00 BA 02 00\n00 00 F7 E2
                0F 90 C1 53 56 57 F7 D9 0B C8 51 E8\nB3 27 00 00 BF 05 00 00
00 8D 77 FE BB 4A 35 02\n10 2B DE 89 5D F4 BA 48 35 02 10 4A BB 4C 35 02\n10 83
C4 04 2B DF A3 C8 FC 03
                10 C7 45 FC 00 00\n00 00 8D 4F FC 89 55 F8 89 5D F0 EB 06\n}
\ncondition:\n2 of them\n}",
            "name": "Symantec"
        }
    }
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.detail.content	Signature.Value	YARA	N/A	Some Yara String...	N/A

Average Feed Run

METRIC	RESULT
Run Time	1 min
Indicators	729
Indicator Attributes	2,890
Signatures	1
Signatures Attributes	6

Change Log

- **Version 1.1.0**
  - Updated the integration's endpoints to use ReversingLabs API v2.
  - Added the following configuration parameters:
    - **Context Filter** - select which pieces of context to ingest with the signatures.
    - **Relationship Filter** - select the relationships to include for each signature.
  - Added ingestion rules for attributes.
  - Updated the minimum ThreatQ version to 5.12.0.
- **Version 1.0.3**
  - Added new configuration parameter: **Disable Proxies**.
  - Added User-Agent string to all requests.
- **Version 1.0.2**
  - Updated the integration to ensure Verify SSL configuration is applied properly to all feeds.
- **Version 1.0.1**
  - Added a new configuration option: **Verify SSL**.
- **Version 1.0.0**
  - Initial release