ThreatQuotient

A Securonix Company

ReversingLabs Action Bundle

Version 1.0.0

April 13, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ReversingLabs Action Bundle enables seamless integration between ThreatQ and ReversingLabs Spectra Analyze, allowing analysts to enrich indicators with advanced threat intelligence and malware analysis data. This bundle automates the enrichment of URLs, FQDNs, and file hashes by submitting supported indicators to the ReversingLabs API and ingesting the resulting classification and contextual analysis back into ThreatQ.

The integration provides the following actions:

- **ReversingLabs - Hash Enrichment** - looks up supported hashes in ReversingLabs and ingests summary and classification context.
- **ReversingLabs - Submit URL** - submits a URL or FQDN to ReversingLabs and stores the returned Submission ID on the original indicator.
- **ReversingLabs - URL Report** - uses the stored ReversingLabs Submission ID to fetch the URL analysis report and ingest the returned context.

The integration supports and returns enrichment for the following indicator types:

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

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 ReversingLabs API token.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - URL
  - MD5
  - SHA-1
  - SHA-256
  - SHA-512

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
6. Select the individual action to install, when prompted, and click **Install**.

   > 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.

The action(s) will be installed on your ThreatQ instance. You will still need to configure the action(s).

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:

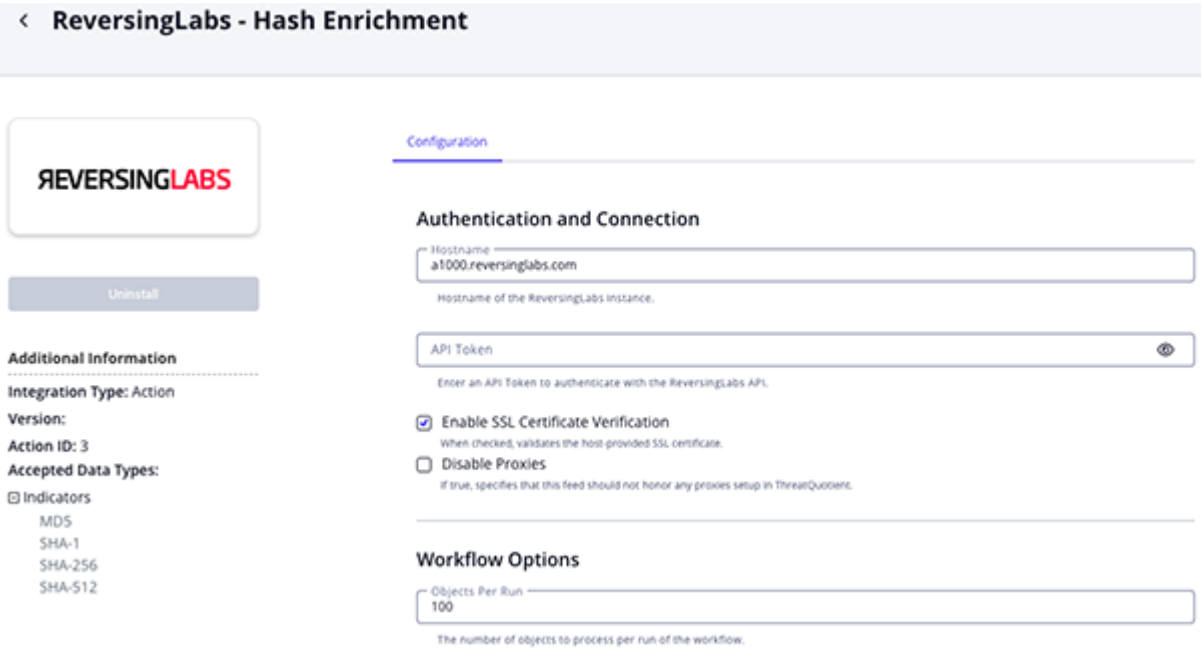
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   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.

Hash Enrichment Parameters

PARAMETER	DESCRIPTION
Hostname	Enter the hostname for the ReversingLabs instance. The default is `a1000.reversinglabs.com`.
API Token	Enter your ReversingLabs API token.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.

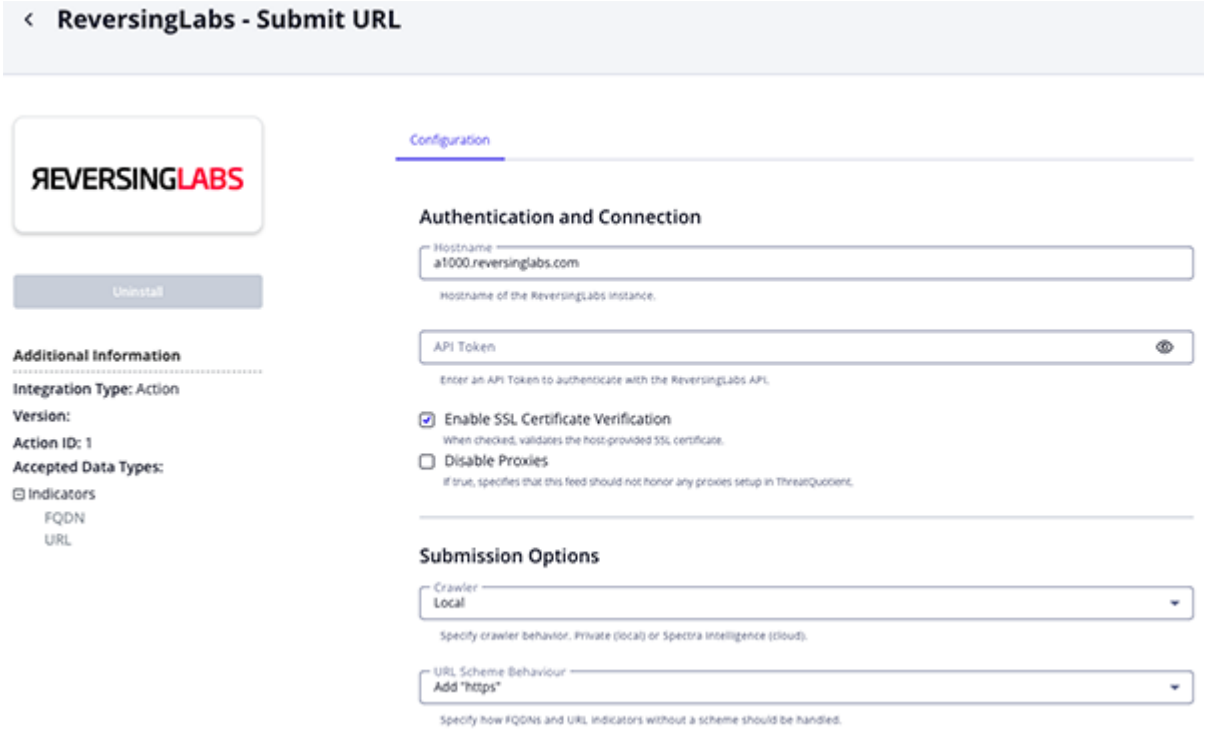
PARAMETER	DESCRIPTION
Objects per Run	Enter the number of objects to process per run of the workflow. The default is `100`.



Submit URL Parameters

PARAMETER	DESCRIPTION
Hostname	Enter the hostname for the ReversingLabs instance. The default is `a1000.reversinglabs.com`.
API Token	Enter your ReversingLabs API token.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.

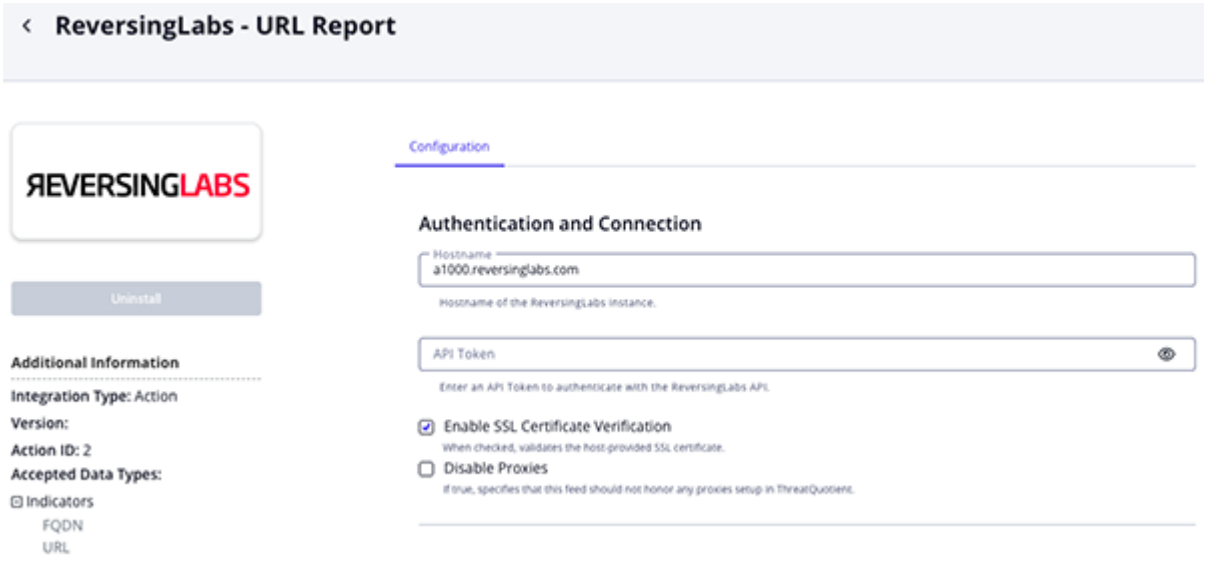
PARAMETER	DESCRIPTION
Crawler	Specify the crawler behavior. Options include: ◦ Local - uses the private crawler. ◦ Cloud - uses Spectra Intelligence.
URL Scheme Behaviour	Specify how FQDNs and URL indicators without a scheme should be handled. Options include: ◦ Add "https" ◦ Add "http"
Objects per Run	Enter the number of objects to process per run of the workflow. The default is `100`.



URL Report Parameters

PARAMETER	DESCRIPTION

PARAMETER	DESCRIPTION
Hostname	Enter the hostname for the ReversingLabs instance. The default is `a1000.reversinglabs.com`.
API Token	Enter your ReversingLabs API token.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Objects per Run	Enter the number of objects to process per run of the workflow. The default is `100`.



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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
ReversingLabs - Hash Enrichment	Enriches supported hashes with ReversingLabs summary and classification data	Indicator	MD5, SHA-1, SHA-256, SHA-512
ReversingLabs - Submit URL	Submits URLs or FQDNs to ReversingLabs and stores the returned submission ID	Indicator	URL, FQDN
ReversingLabs - URL Report	Fetches URL report details using the stored submission ID	Indicator	URL, FQDN

ReversingLabs - Hash Enrichment

The ReversingLabs - Hash Enrichment action enriches supported hashes using the ReversingLabs report summary endpoint and, for supported hash types, the classification endpoint.

Request Report Summary
`POST https://{hostname}/api/samples/v2/list/`

For MD5, SHA-1, and SHA-256, the action also requests classification
`GET https://{hostname}/api/samples/v3/{hash_value}/classification/`

Sample Body:

```
{
  "hash_values": [
    "86bb5ed57999602fc4540ace6086a891c996e3f3"
  ]
}
```

Sample Response:

```
{
  "count": 1,
  "next": null,
  "previous": null,
  "results": [
    {
      "id": 68891607,
      "sha1": "fe835e0d7b9026a2ce1f0e081fcbd68ff474ffb8",
      "sha256":
"cb9af341bdc2a3352fe83b5a81109a85a9412670f2cd1c6b097c21ca49bf5425",
      "sha512":
"239459fc555e5b8b65d64448c470ff145fdaee2ea94e8218b7c22f9cc6bdb2dc6916
d3136835ff803d9961bb7cbc7d5c3c0c80ac85a21731110eb8779427f7d8",
      "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": "goodware",
      "classification_origin": {
        "sha1": "3ed9753623f756884ff9c30efceec58319ac0346",
        "sha256":
"0d6d9bbbfdceaa391310f69b37a04af230bddfa059a8f883a4a3c5bf1cb3e956",
        "sha512":
"29eb8a7c9796402cad00bcc92bddaf51a2a8f5978f98ccacb4687ee80b537d7acd25
25e4d1f4157fb86a09de5c39f27ed1f2bca0e5ba21b30133638be5e26954",
        "md5": "f831055b5bdacc126824b39363fd9894",
        "imphash": ""
      },
      "classification_reason": "user",
      "riskscore": 5,
      "tags": {
        "ticore": [
          "cloud",
          "entropy-high",
          "contains-script",
          "contains-pe"
        ],
        "user": [
          "URL Download"
        ]
      },
      "proposed_filename": "Script-VBS.Trojan.Mekotio.zip"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.category	Indicator.Attribute	Category	N/A	malicious	Updatable.
.file_type	Indicator.Attribute	File Type	N/A	PE	Updatable.
.file_subtype	Indicator.Attribute	File Subtype	N/A	32-bit	Updatable.
.identification_name	Indicator.Attribute	Identification Name	N/A	Win32.Trojan	Updatable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.identification_version	Indicator.Attribute	Identification Version	N/A	1.0	Updatable.
.file_size	Indicator.Attribute	File Size	N/A	151552	Updatable.
.extracted_file_count	Indicator.Attribute	Extracted File Count	N/A	0	Updatable.
.tags.ticore[]	Indicator.Attribute	TI Score Tag	N/A	malware	Repeated attribute.
.tags.user[]	Indicator.Attribute	User Tag	N/A	ransomware	Repeated attribute.
.first_seen	Indicator.Attribute	First Seen	N/A	2025-11-03T11:17:32Z	Updatable.
.last_seen	Indicator.Attribute	Last Seen	N/A	2026-03-15T08:44:01Z	Updatable.
.classification_reason	Indicator.Attribute	Classification Reason	N/A	Classified by ReversingLabs	Updatable.
.classification	Indicator.Attribute	Classification	N/A	Malicious	Updatable.
.data_source	Indicator.Attribute	Data Source	N/A	Spectra Analyze	Updatable.
.riskscore	Indicator.Attribute	Risk Score	N/A	9	Updatable.
.sha1	Related Indicator.Value	SHA-1	N/A	86bb5ed57999602fc4540ace6086a891c996e3f3	Added as a related indicator when present. The original hash value is not re-ingested as a related indicator.
.sha256	Related Indicator.Value	SHA-256	N/A	6f4f8404d6c0d4f21f8c9f1ed5b7b1f4a7d827c6f8f8d24a1f3f6f0b8ed0aa21	Added as a related indicator when present. The original hash value is not re-ingested as a related indicator.
.sha512	Related Indicator.Value	SHA-512	N/A	4a4e0f4c6cf4ddab0b0dd31d8a84f4e2d45a7cf1f77cf6c6f2b7d6244cf3a488b0f2f9cb75d2e97d67c302f2ad0a08f73f1ed9a31f6f7b70c381e2db2d7bb0d7	Added as a related indicator when present. The original hash value is not re-ingested as a related indicator.
.md5	Related Indicator.Value	MD5	N/A	4195192b66a50fd0641019f634d2c86c	Added as a related indicator when present. The original hash value is not re-ingested as a related indicator.

ReversingLabs - Submit URL

The ReversingLabs - Submit URL action submits the input URL or FQDN to ReversingLabs and stores the returned submission ID as an attribute on the original indicator.

> If the input is an FQDN or URL without a scheme, the action prepends either `https://` or `http://` based on the configured `URL Scheme Behaviour` or the indicator's existing `Scheme` attribute.

`POST https://{hostname}/api/submit/url/`

Sample Body:

```
{
  "url": "https://example.com",
  "comment": "Submitted by ThreatQ",
  "crawler": "local"
}
```

Sample Response:

```
{
    "code": 201,
    "message": "Done.",
    "detail": {
        "id": 25092149,
        "user": 889,
        "created": "2026-04-02T08:29:08.779063Z",
        "filename": "https://www.youtube.com/"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.detail.id`	`Indicator.Attribute`	`ReversingLabs Submission ID`	`N/A`	`718433`	`Added to the original URL or FQDN indicator. Updatable.`

ReversingLabs - URL Report

The ReversingLabs - URL Report action fetches the URL analysis report for a previously submitted URL or FQDN using the `ReversingLabs Submission ID` attribute on the original indicator.

> This action uses the `ReversingLabs Submission ID` attribute stored on the original URL or FQDN indicator by the **ReversingLabs - Submit URL** action.

`GET https://{hostname}/api/uploads/v2/url-samples/{submission_id}`

Sample Response:


```
{
  "processing_status": "complete",
  "message": "",
  "report": {
    "id": 143872354,
    "sha1": "8bc58d0bef541168f7bde087486a32778b176fcc",
    "sha256": "b008be369fecaf0da3ee04d123c186dc4d676e9d5cc390cb81ff1982827f82e8",
    "sha512":
"fb3c8b35240233b14d00a038e45b429bfe04039a4f5c27dc62a6b2c61d80effc45fcd6811247eae6179b068fcab1d3
    "md5": "2a0b03d31b7cd7fcf108a6eb4cb73700",
    "imphash": "",
    "category": "application",
    "file_type": "ELF32 Little",
    "file_subtype": "Exe",
    "identification_name": "",
    "identification_version": "",
    "file_size": 132404,
    "extracted_file_count": 0,
    "local_first_seen": "2025-06-22T05:55:33.153256Z",
    "local_last_seen": "2025-07-23T12:32:48.799392Z",
    "classification_origin": null,
    "classification_reason": "antivirus",
    "classification": "malicious",
    "riskscore": 10,
    "classification_result": "Linux.Trojan.DDOSAgent",
    "networkthreatintelligence": {
      "sha1": "814e3da8a8874e44e31d1c4716b05cfafe4448e2",
      "base64": "aHR0cDovLzMxLjE3MC4yMi4yMDUvYmlucy93aGlzcGVyLnNoNA",
      "analysis": {
        "first_analysis": "2025-02-25T17:09:34",
        "last_analysis": {
          "analysis_id": "175327380653814e",
          "analysis_time": "2025-07-23T12:30:52",
          "http_response_code": 200,
          "availability_status": "online",
          "domain": "31.170.22.205",
```

```
        "serving_ip_address": "31.170.22.205"
      },
      "analysis_count": 5,
      "statistics": {
        "unknown": 0,
        "suspicious": 0,
        "malicious": 1,
        "total": 2,
        "goodware": 1
      },
      "top_threats": [
        {
          "threat_name": "Linux.Trojan.DDOSAgent",
          "files_count": 1,
          "risk_score": 10
        }
      ]
    },
    "third_party_reputations": {
      "sources": [
        {
          "source": "0xSI_f33d",
          "update_time": "2025-07-23T05:21:25",
          "detection": "undetected"
        },
        {
          "source": "adminus_labs",
          "update_time": "2025-07-23T10:34:20",
          "detection": "malicious",
          "detect_time": "2025-06-24T04:53:23"
        },
        {
          "source": "alphamountain",
          "update_time": "2025-07-23T10:30:06",
          "detection": "malicious",
          "categories": [
            "phishing",
            "spam"
          ],
          "detect_time": "2025-07-23T10:30:06"
        }
      ],
      "statistics": {
        "total": 21,
        "malicious": 6,
        "clean": 0,
        "suspicious": 0,
        "undetected": 15
      }
    },
    "last_seen": "2025-07-23T12:38:02",
    "first_seen": "2025-02-25T17:09:34",
```

```
      "classification": "malicious",
      "reason": "third_party_reputation",
      "threat_level": 5,
      "threat_name": "Web.Hyperlink.Blacklisted",
      "categories": [
        "phishing",
        "malicious_web_sites",
        "spam"
      ],
      "requested_url": "http://31.170.22.205/bins/whisper.sh4"
    },
    "domainthreatintelligence": {}
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.report.category	Indicator.Attribute	Category	N/A	malware	Added when .processing_status is complete. Updatable.
.report.local_first_seen	Indicator.Attribute	First Seen	N/A	2026-03-20T05:43:51Z	Added when .processing_status is complete. Updatable.
.report.local_last_seen	Indicator.Attribute	Last Seen	N/A	2026-03-21T05:43:51Z	Added when .processing_status is complete. Updatable.
.report.networkthreatintelligence.analysis.first_analysis	Indicator.Attribute	First Analysis	N/A	2026-03-20T05:43:51Z	Added when .processing_status is complete. Updatable.
.report.networkthreatintelligence.analysis.last_analysis.analysis_time	Indicator.Attribute	Last Analysis	N/A	2026-03-21T07:15:29Z	Added when .processing_status is complete. Updatable.
.report.networkthreatintelligence.analysis.last_analysis.availability_status	Indicator.Attribute	Last Analysis Availability Status	N/A	alive	Added when .processing_status is complete. Updatable.
.report.classification	Indicator.Attribute	Classification	N/A	Malicious	Added when .processing_status is complete. Updatable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.report.networkthreatintelligence.reason	Indicator.Attribute	Classification Reason	N/A	Detected as suspicious by network threat intelligence	Added when .processing_status is complete. Updatable.
.report.riskscore	Indicator.Attribute	Risk Score	N/A	9	Added when .processing_status is complete. Updatable.
.report.classification_result	Indicator.Attribute	Classification Result	N/A	malicious	Added when .processing_status is complete. Updatable.
.message	Indicator.Attribute	ReversingLabs Processing Message	N/A	Unable to process submitted URL	Added when .processing_status is error. Updatable.
.report.sha1	Related Indicator.Value	SHA-1	N/A	86bb5ed57999602fc4540ace6086a891c996e3f3	Added when .processing_status is complete.
.report.sha256	Related Indicator.Value	SHA-256	N/A	6f4f8404d6c0d4f21f8c9f1ed5b7b1f4a7d827c6f8f8d24a1f3f6f0b8ed0aa21	Added when .processing_status is complete.
.report.sha512	Related Indicator.Value	SHA-512	N/A	4a4e0f4c6cf4ddab0b0dd31d8a84f4e2d45a7cf1f77cf6c6f2b7d6244cf3a488b0f2f9cb75d2e97d67c302f2ad0a08f73f1ed9a31f6f7b70c381e2db2d7bb0d7	Added when .processing_status is complete.
.report.md5	Related Indicator.Value	MD5	N/A	4195192b66a50fd0641019f634d2c86c	Added when .processing_status is complete.
.report.networkthreatintelligence.analysis.last_analysis.serving_ip_address	Related Indicator.Value	IP Address	N/A	118.189.81.19	Added when .processing_status is complete.
.report.networkthreatintelligence.analysis.last_analysis.domain	Related Indicator.Value	FQDN	N/A	cracking.to	Added when .processing_status is complete and only if the value differs from the serving IP address.

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.

ReversingLabs - Hash Enrichment

METRIC	RESULT
Run Time	1 minutes
Indicators	100
Indicator Attributes	300

Known Issues / Limitations

- **ReversingLabs - URL Report** does not ingest report data until the ReversingLabs URL status API returns `processing_status = complete`.
- For URL and FQDN submissions, report data may not be available immediately after **ReversingLabs - Submit URL**, so no report is added while the submission is still processing.
- To improve reliability for URL and FQDN enrichment, run **ReversingLabs - URL Report** about 5 minutes after running **ReversingLabs - Submit URL**.

Change Log

- **Version 1.0.0**
  - Initial release