ThreatQuotient

A Securonix Company

UrlScan.io Operation

Version 1.1.0

March 23, 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.

Copyright © 2026 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	1.1.0
Compatible with ThreatQ Versions	>= 5.9.0
Support Tier	ThreatQ Supported

Introduction

The URLScan.io Operation for ThreatQuotient enables a ThreatQ user to submit URLs to URLScan.io, as well as query URLScan.io for any results on a URL.

The operation provides the following actions:

- **Search** - queries URLScan.io for a specific indicator found in any public submission reports.
- **Get Report** - retrieves a report for any scan IDs found in the indicator's attributes.
- **Submit** - submits a URL, FQDN,or IP Address to URLScan.io.

The integration is compatible with the following indicator types:

- FQDN
- IP Address
- SHA-256
- URL

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
API Key	Your URLScan.io API key.

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 UrlScan.io operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Submit	Submits a URL, FQDN, or IP Address to URLScan.io.	Indicator	FQDN, IP Address, URL
Get Reports	Retrieves a report for any scan IDs found in the indicator's attributes.	Indicator	FQDN, IP Address, URL
Search	Queries URLScan.io for a specific indicator found in any public submission reports.	Indicator	FQDN, IP Address, SHA-256, URL

Submit

The Submit action will submit a URL or FQDN to URLScan.io. Once submitted, an attribute called `URLScan.io ID` will be added to the indicator.

`POST https://urlscan.io/api/v1/scan/`

Sample Response:

```
{
  "result": "https://urlscan.io/result/019cf79e-69b7-758f-9c94-c322af9f0006/",
  "api": "https://urlscan.io/api/v1/result/019cf79e-69b7-758f-9c94-c322af9f0006/",
  "message": "Submission successful",
  "uuid": "019cf79e-69b7-758f-9c94-c322af9f0006",
  "options": {},
  "visibility": "private",
  "url": "http://amazon.com/"
}
```

ThreatQuotient provides the following default mapping for this operation action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.uuid	Indicator.Attribute	URLScan.io ID	N/A	`019cf79e-69b7-758f-9c94-c322af9f0006`	N/A

Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following parameters are available for the Submit action:

PARAMETER	DESCRIPTION
Public	Select whether the scan will be publicly visible. This option is not enabled by default.
Tags	Enter one or more tags, in line-separated format, to be added to the submission.

Get Reports

The Get Reports action will retrieve a report for any scan IDs found in the indicator's attributes.

`GET https://urlscan.io/api/v1/result/{uuid}`

Sample Response:


```
{
  "task": {
    "uuid": "019cf7ef-8a8c-7618-a8c1-cd3b11390427",
    "url": "http://threatq.com/",
    "reportURL": "https://urlscan.io/result/019cf7ef-8a8c-7618-a8c1-cd3b11390427/",
    "screenshotURL": "https://urlscan.io/screenshots/019cf7ef-8a8c-7618-a8c1-cd3b11390427.png"
  },
  "page": {
    "domain": "www.threatq.com",
    "ip": "198.202.211.1",
    "asn": "AS209242",
    "asnname": "CLOUDFLARESPECTRUM Cloudflare London, LLC, US",
    "country": "US",
    "city": "",
    "tlsAgeDays": 31,
    "tlsValidDays": 90,
    "url": "https://www.threatq.com/",
    "title": "ThreatQ Threat Intelligence Platform I ThreatQuotient"
  },
  "verdicts": {
    "urlscan": {
      "tags": [],
      "hasVerdicts": false,
      "categories": [],
      "score": 0,
      "brands": [],
      "malicious": false
    },
    "engines": {
      "tags": ["urlscan-ml", "urlscan-ml-60c5e22"],
      "benignTotal": 0,
      "hasVerdicts": true,
      "enginesTotal": 0,
      "categories": [],
      "maliciousTotal": 0,
      "score": -100,
      "maliciousVerdicts": [],
      "benignVerdicts": [],
      "malicious": false
    },
    "overall": {
      "tags": [],
      "hasVerdicts": true,
      "categories": [],
      "score": 0,
      "brands": [],
      "malicious": false
    },
    "community": {
      "votesBenign": 0,
      "votesMalicious": 0,
      "hasVerdicts": false,
      "votesTotal": 0,
      "score": 0,
      "malicious": false,
```

```
    "categories": [],
    "brands": []
  }
},
"stats": {
  "ipStats": [
    {
      "ip": "198.202.211.1",
      "domains": ["threatq.com", "www.threatq.com"],
      "asn": {
        "asn": "209242",
        "name": "CLOUDFLARESPECTRUM Cloudflare London"
      },
      "requests": 2,
      "geoip": {
        "country": "US",
        "region": "",
        "city": "",
        "ll": [37.751, -97.822]
      }
    }
  ]
},
"meta": {
  "processors": {
    "rdns": {
      "data": [
        {
          "ip": "192.178.155.95",
          "ptr": "yuiadrs-in-f95.1e100.net"
        }
      ]
    },
    "wappa": {
      "data": [
        {
          "app": "Sentry",
          "confidenceTotal": 100,
          "categories": [
            {
              "name": "Issue trackers"
            }
          ]
        }
      ]
    }
  }
},
"data": {
  "links": [
    {
      "href": "https://www.securonix.com/breach-ready-board-ready-ai-powered",
      "text": "LEARN MORE"
    }
  ]
},
"lists": {
  "domains": ["cdn.prod.website-files.com"],
  "linkDomains": ["www.securonix.com"],
  "urls": ["https://www.threatq.com/"],
  "hashes": [
    "8bbdc45c5dc033a915a5ded5a130a7ec41c10b0e9c7d398013e008356c3858c9"
  ],
  "ips": ["3.160.5.91"]
```

```
  }
}
```

The following parameters are available for the Get Reports action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.page.domain	Related Indicator.Value	FQDN	N/A	www.threatq.com	Submission Indicators
.page.ip	Related Indicator.Value	IP Address	N/A	198.202.211.1	Submission Indicators
.page.asn	Related Indicator.Value	ASN	N/A	209242	Submission Indicators; removes the AS prefix
.page.url	Related Indicator.Value	URL	N/A	https://www.threatq.com/	Submission Indicators
.page.asn	Indicator.Attribute	ASN	N/A	209242	Verdict Metadata; removes the AS prefix
.page.asnname	Indicator.Attribute	AS Organization	N/A	CLOUDFLARESPECTRUM Cloudflare London, LLC, US	Verdict Metadata
.page.title	Indicator.Attribute	Site Title	N/A	ThreatQ Threat Intelligence Platform I ThreatQuotient	Verdict Metadata
.page.country	Indicator.Attribute	Country Code	N/A	US	Verdict Metadata
.page.tlsAgeDays	Indicator.Attribute	TLS Age	N/A	31	Verdict Metadata
.page.tlsValidDays	Indicator.Attribute	TLS Valid Days	N/A	90	Verdict Metadata
.verdicts.overall.score	Indicator.Attribute	URLScan.io Score	N/A	0	Verdict Metadata
.verdicts.overall.malicious	Indicator.Attribute	Is Malicious	N/A	false	Verdict Metadata
.task.uuid	Indicator.Attribute	URLScan.io Report	N/A	019cf7ef-8a8c-7618-a8c1-cd3b11390427	Verdict Metadata; used to build the report URL
.stats.ipStats[].ip	Related Indicator.Value	IP Address	N/A	198.202.211.1	IP Details
.meta.processors.rdns.data[].ptr	Related Indicator.Value	FQDN	N/A	yuiadrs-in-f95.1e100.net	Reverse DNS
.data.links[].href	Related Indicator.Value	URL	N/A	https://www.securonix.com/breach-ready-board-ready-ai-powered	Outgoing Links

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.stats.ipStats[].ip	Related Indicator.Value	IP Address	N/A	198.202.211.1	GeoIP Data
.meta.processors.wappa.data[].app	Indicator.Attribute	Technology	N/A	Sentry	Technologies
.lists.domains[]	Related Indicator.Value	FQDN	N/A	cdn.prod.website-files.com	All Indicators
.lists.linkDomains[]	Related Indicator.Value	FQDN	N/A	www.securonix.com	All Indicators
.lists.urls[]	Related Indicator.Value	URL	N/A	https://www.threatq.com/	All Indicators
.lists.hashes[]	Related Indicator.Value	SHA-256	N/A	8bbdc45c5dc033a915a5ded5a130a7ec41c10b0e9c7d398013e008356c3858c9	All Indicators
.lists.ips[]	Related Indicator.Value	IP Address	N/A	3.160.5.91	All Indicators

Search

The Search action queries URLScan.io for a specific indicator found in any public submission reports. For each exact match, the operation then retrieves the full report and renders it using the same output as the Get Report action.

> The operation applies the same mappings shown in the **Get Report** section above.

```
GET https://urlscan.io/api/v1/search/?q={indicator}
```

Sample Response:


```
{
  "results": [
    {
      "task": {
        "url": "http://threatq.com/",
        "visibility": "private",
        "apexDomain": "threatq.com",
        "method": "api",
        "uuid": "019cf7ef-8a8c-7618-a8c1-cd3b11390427",
        "domain": "threatq.com",
        "time": "2026-03-16T18:36:54.339Z"
      },
      "stats": {
        "encodedDataLength": 8599910,
        "requests": 91,
        "dataLength": 13183123,
        "uniqCountries": 2,
        "uniqIPs": 23
      },
      "page": {
        "tlsAgeDays": 31,
        "language": "en",
        "domainAgeDays": 2855,
        "mimeType": "text/html",
        "status": "200",
        "ip": "198.202.211.1",
        "tlsIssuer": "WE1",
        "domain": "www.threatq.com",
        "url": "https://www.threatq.com/",
        "title": "ThreatQ Threat Intelligence Platform I ThreatQuotient",
        "tlsValidFrom": "2026-02-13T14:55:47.000Z",
        "asn": "AS209242",
        "tlsValidDays": 90,
        "apexDomain": "threatq.com",
        "redirected": "sub-domain",
        "country": "US",
        "server": "cloudflare",
        "apexDomainAgeDays": 4105,
        "asnname": "CLOUDFLARESPECTRUM Cloudflare London, LLC, US"
      },
      "_id": "019cf7ef-8a8c-7618-a8c1-cd3b11390427",
      "screenshot": "https://urlscan.io/screenshots/019cf7ef-8a8c-7618-a8c1-cd3b11390427.png",
      "_score": null,
      "submitter": {},
      "sort": [1773686214339, "019cf7ef-8a8c-7618-a8c1-cd3b11390427"],
      "result": "https://urlscan.io/api/v1/result/019cf7ef-8a8c-7618-a8c1-cd3b11390427/"
    }
  ]
```

```
}
```

Change Log

- **Version 1.1.0**
  - The following additional context will now be included in returned reports:
    - Reverse DNS
    - Geolocation Info
    - Outgoing Links
    - Tech Stack Analysis
    - List of all extracted indicators
    - Screenshot of page
  - Updated the minimum ThreatQ version to 5.9.0.
- **Version 1.0.2**
  - Corrected version number displayed after installation.
  - Fixed an issue where the schema was stripped from URLs.
  - Fixed an issue where the integration did not honor customer-set proxy configurations.
- **Version 1.0.0**
  - Initial release