

ThreatQuotient



URLScan.io Operation User Guide

Version 1.0.2

November 03, 2023

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	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
Actions	9
Submit	9
Parameters	9
Example	10
Get Reports	11
Example	11
Search	12
Example - Single Result.....	12
Example - Multiple Results	13
Change Log	14

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 © 2023 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: 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 1.0.2

**Compatible with ThreatQ
Versions** $\geq 4.0.0$

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 or FQDN to URLScan.io. Once submitted, an attribute called "URLScan.io ID" will be added to the indicator.

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 or FQDN to URLScan.io. Once submitted, an attribute called "URLScan.io ID" will be added to the indicator	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.

Parameters

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.

Example

AV AlienVault OTX Pulse: Query

URLScan.io: Search

URLScan.io: Get Report

URLScan.io: Submit

Successfully submitted sample to URLScan.io [ID: ce1cf67d-5843-436a-92c2-e67a24ec85bc]

Raw Response

Show

Search

The Search action queries URLScan.io for a specific indicator found in any public submission reports.

Example - Single Result

[illegible]

Example - Multiple Results

AlertVault OTX Pulse Query

URLScan.io Search

URLScan.io Get Report

URLScan.io Submit

Found 14 Submitted Task(s) for newrivoc.com

Showing Top 5 Results

Report for 3ece7c93-3613-49ff-b987-41df2a192112

View the Report

Verdict

NAME	VALUE
Country Code	US
Age	4600
Tag	phishing
Affected Brands	discord
Category	phishing
URLScan.io Score	100
Is Malicious	True
URLScan.io Report	https://urlscan.io/results/3ece7c93-3613-49ff-b987-41df2a192112

Add Selected Indicators

Related Indicators

Showing 1 to 24 of 24

Row count: 25

VALUE	TYPE
54f028baf39b96648d9485d505007a0b7a2048770899bdcf9c22809	SHA-256
7a23450ac7214401814a044e495105116d508141195da7096d706ac	SHA-256
882d88ac328f2d40546a495a703897e88dc13d3d47c0d6b30ac6	SHA-256
x9da62879991df0c17dd34cf41447a272c79c3c163939dc0a4d034	SHA-256
a88e18915ca92da75ad314490bda93a22771ba9f8a0f002a071ad	SHA-256
3a8eac450073289a079f9c231414645a0499128c38d0303b0a070a	SHA-256
324a0f9f4023281cc49653a0c79a10d8516419705119a4b70d83d6d	SHA-256
7213c360c170d450ef8a1f8cc3dc35d935179ee8d879ebdc0dc89c3	SHA-256
21d7133f688c3d07f980633a79ac3797a7177a9d8c757095a42c129b7	SHA-256
1a7d470d64c42a1650ac2236dc4205a17ab4e40c3a06008d87c715d6	SHA-256
404702a4876a63d787d7a1315d15800c2d959d8e141959409d6d4	SHA-256
newrivoc.com	FDQN
https://newrivoc.com/assets/newPageValidation/	URL
https://newrivoc.com/assets/newPageValidation/megs/v1.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v2.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v3.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v4.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v5.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v6.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v7.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v8.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v9.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v10.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v11.png	URL
https://newrivoc.com/assets/newPageValidation/megs/v12.png	URL
192.241.218.97	IP Address

Add Selected Indicators

Report for 63388a08-683c-4bb9-8b3a-275941f2d828

Show

Report for c5a29bd2-f641-4497-9e6b-a903d9f78f2

Show

Report for da9c0c36-2152-4258-b9d4-b9046edb4396

Show

Report for 62d88789-497b-4839-85ff-464c151a58d5

Show

Raw Response

Show

URLScan.io Operation User Guide
Version 1.0.2

13

Change Log

- **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