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

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	1.0.2
Compatible with ThreatQ Versions	>= 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

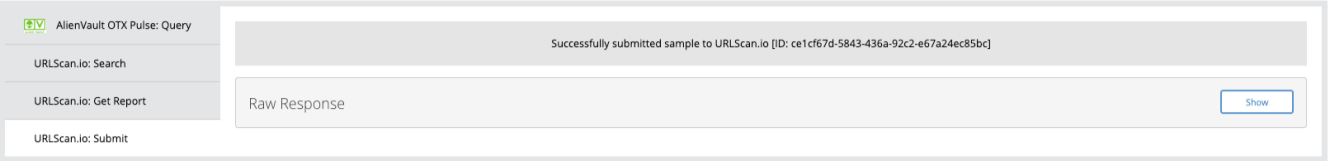
The Submit action will submit a URL or FQDN to URLScan.io. Once submitted, an attribute called "URLScan.io ID" will be added to the indicator.

Parameters

The following parameters are available for the Submit action:

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

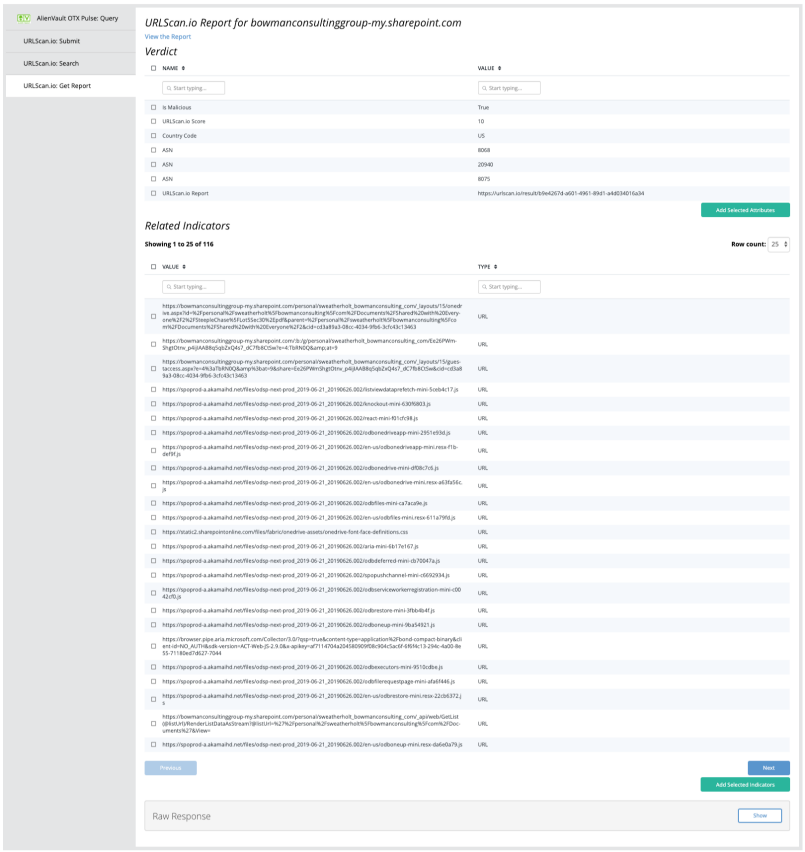
Example


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

Get Reports

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

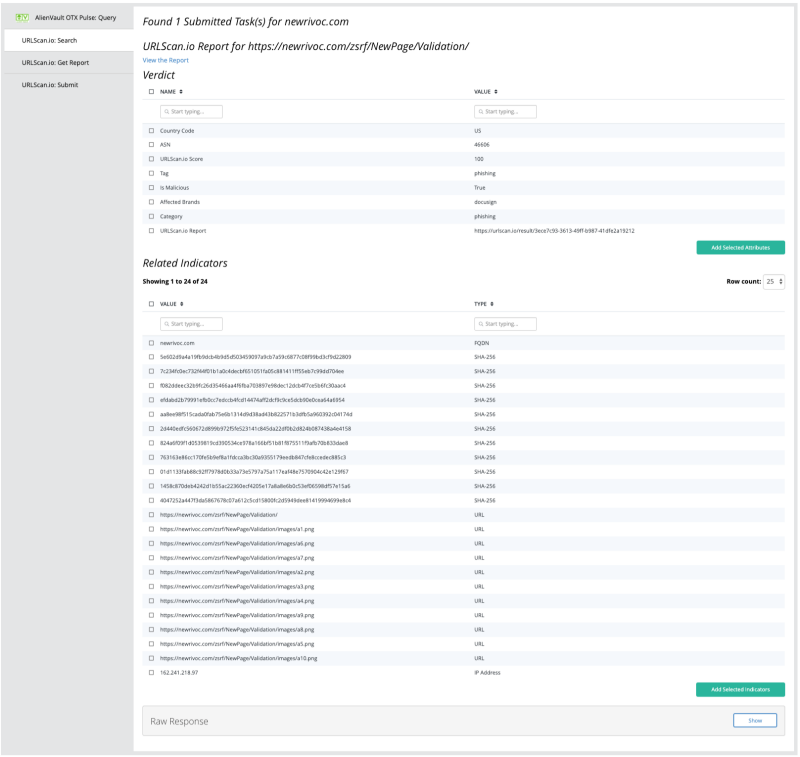
Example



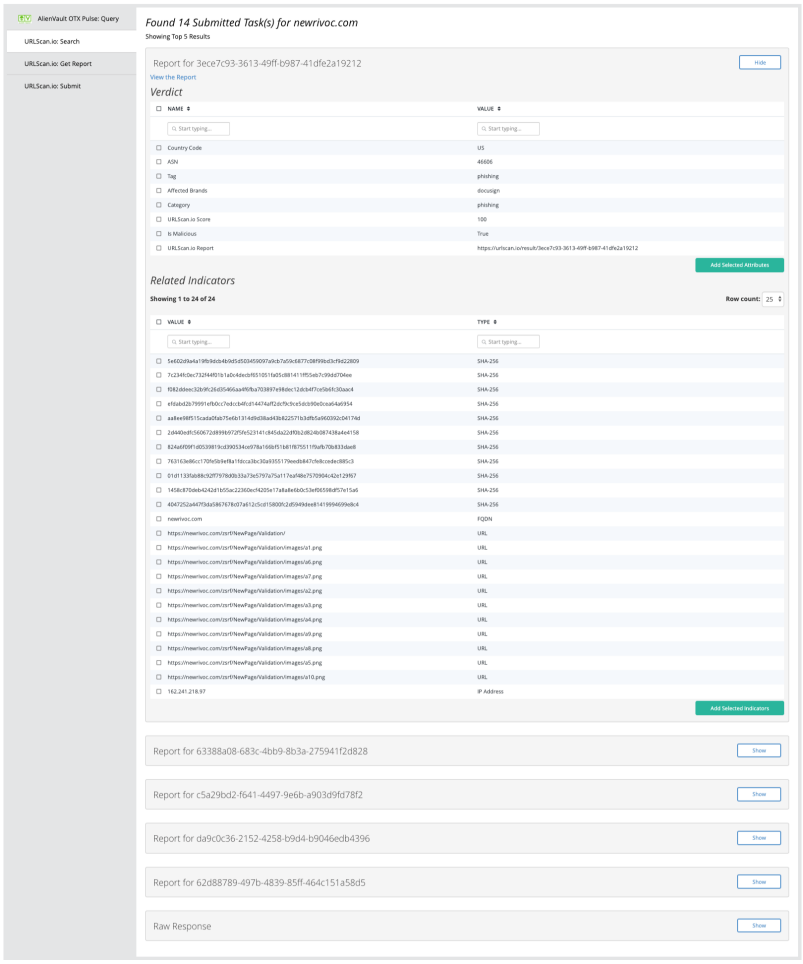
Search

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

Example - Single Result



Example - Multiple Results



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