ThreatQuotient

ThreatQuotient for URLScan.io Operation

Version 1.0.0

August 21, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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.

Last Updated: Wednesday, August 21, 2019

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

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

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for URLScan.io Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

1.4 Scope

This document covers the implementation of the ThreatQuotient for URLScan.io Operation only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 4.20.x or greater	
ThreatQuotient for URLScan.io Operation	1.0.0	

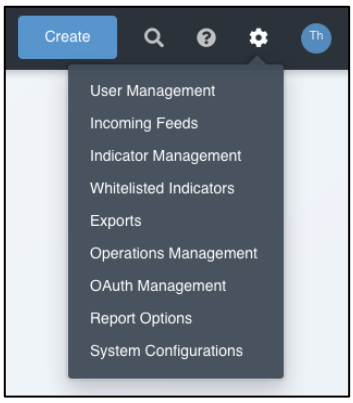
2 ThreatQuotient for URLScan.io Operation Installation

2.1 Setting up the Integration

Ensure the file `tq_op_urlscan_io-1.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for URLScan.io Operation is being installed/upgraded.

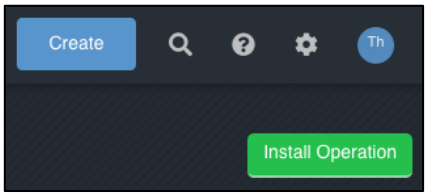
1. Navigate to the **Settings icon** > **Operations Management**.

Figure 1: Operations Management – Install



2. Click **Install Operation** in the upper right corner.

Figure 2: Install Operation



3. Drag the `tq_op_urlscan_io-1.0.0-py3-none-any.whl` to the Add Operation Popup or **Click to Browse** to the required file.
4. Click **Install** or **Upgrade**.

You may be presented with **OPERATION ALREADY INSTALLED** as shown below.

Figure 3: Add Operation

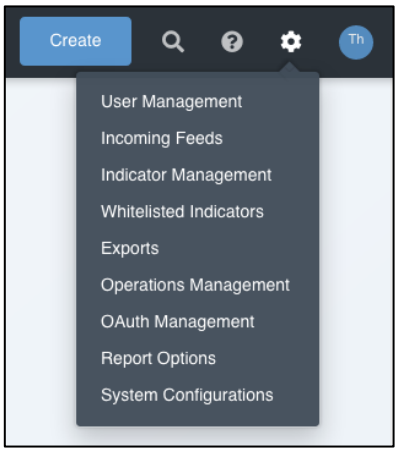
Installation/Upgrade is now complete.

2.2 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for URLScan.io Operation.

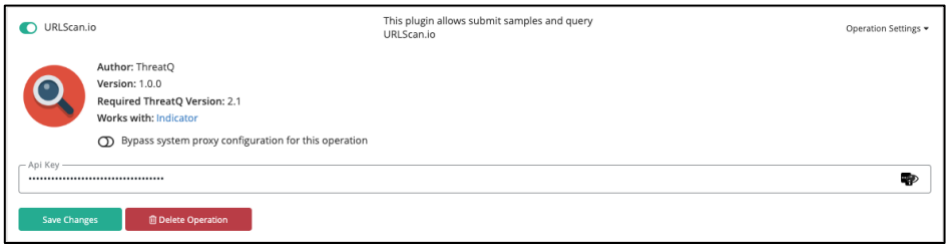
1. Navigate to the **Settings icon** > **Operations Management.**

Figure 4: Operations Management – Configuration



2. Expand the **URLScan.io** configuration.

Figure 5: Operation Configuration



3. Enter your **URLScan.io API Key** into the **API Key** field.
4. Click **Save Changes**.
5. Click the toggle button next to the **URLScan io** name to enable the operation.

2.3 Using the Operation

The following section covers the use of the ThreatQuotient for URLScan.io Operation.

2.3.1 Submit

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

Applies to: URL - FQDN - IP Address

Parameters

The following parameters allow you to specify scanning options before sending the scan:

- **Public**: Enable this if you want the scan to be visible publicly.
  - Default: False (unchecked)
- **Tags**: A list of tags to add to the submission (line-separated)

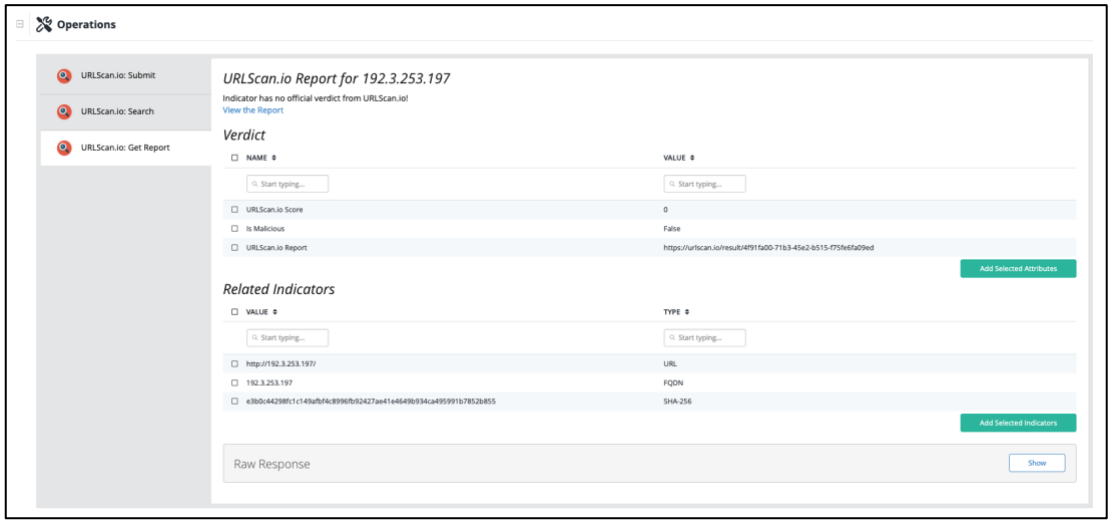
Figure 6: URLScan io Operation Submit Example

2.3.2 Get Reports

This action will get a report for any scan IDs found in the indicator's attributes (*see Submit*).

Applies to: URL - FQDN - IP Address

Figure 7: URLScan io Operation Get Reports Example



2.3.3 Search

This action will query URLScan.io for a specific indicator found in any public submission reports.

Applies to: URL - FQDN - IP Address - SHA-256

Figure 8: URLScan io Operation Search Example

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.