ThreatQuotient

Shodan Operation Guide

Version 2.0.0

Thursday, September 3, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 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.

Contents

Versioning

- Current integration version: 2.0.0
- Supported on ThreatQ versions: 4.25 or greater

Introduction

The Shodan Operation for ThreatQuotient enables a user to query Shodan contextual information around FQDNs and IP Addresses.

Installation

Perform the following steps to install the operation:

Note: *The same steps can be used to upgrade the operation to a new version.*

1. Log into https://marketplace.threatq.com/.
2. Locate and download the operation file.
3. Navigate back to the ThreatQ instance.
4. Click on the **Settings** icon and select **Operations Management**.
5. Click on the **Install Operation** button.
6. Upload the operation file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the operation file on your local machine

Note: *ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding.*

The operation will be added to your list of installed operations. You will still need to configure and enable the operation.

Configuration

Note: *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other operation-related credentials.*

To configure the operation:

1. Click on the **Settings** icon and select **Operations Management**.
2. Locate the operation and click on **Operation Settings**.
3. Enter the following configuration parameter:

Parameter	Description
API Token	Your Shodan API Token.

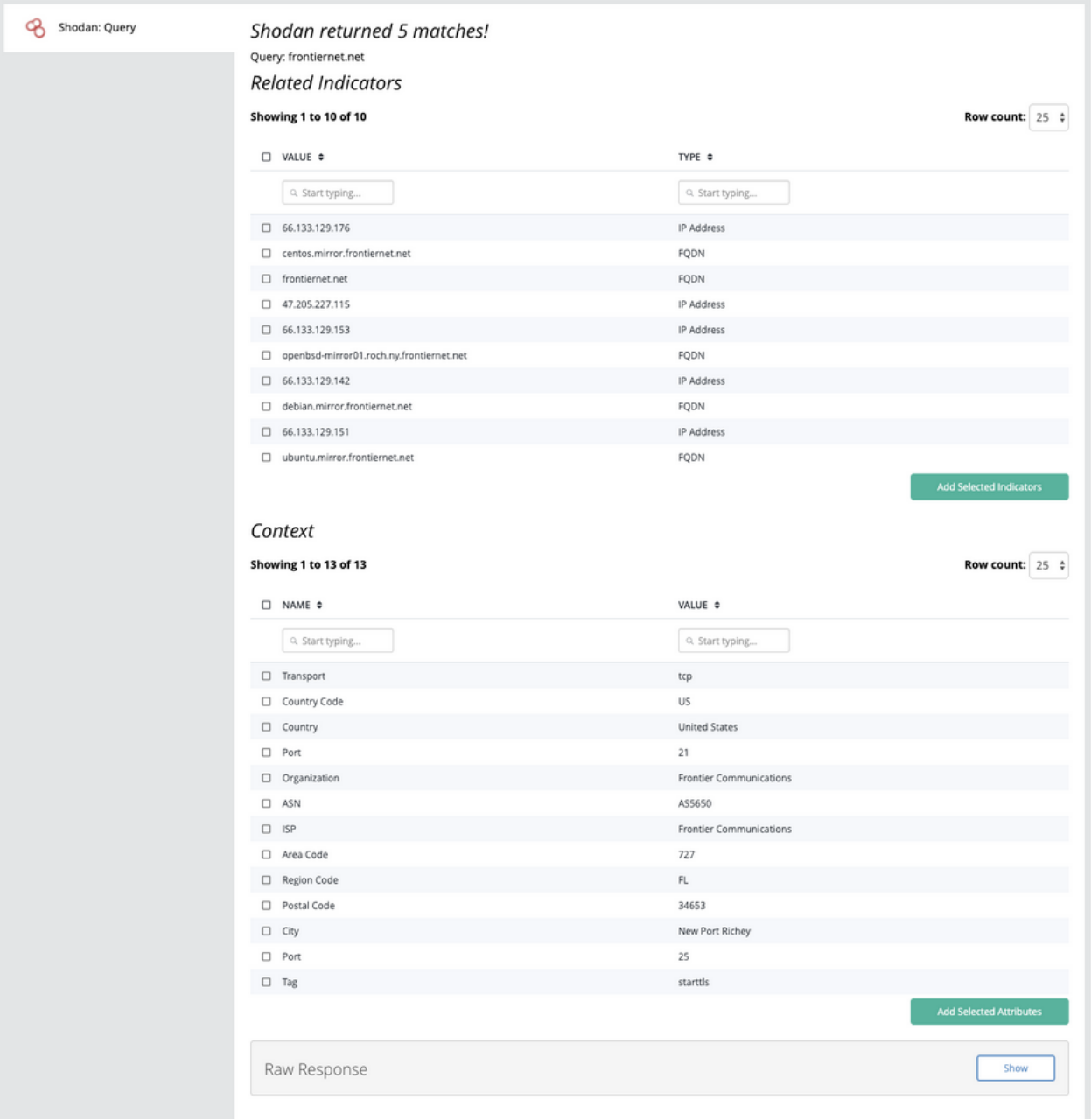
4. Click on **Save Changes**.
5. Click on the toggle switch to the left of the operation name to enable the operation

Actions

The Shodan operation comes with one action: Query.

Query

The Query action, which applies to indicators (FQDN, IP Address, URL), queries Accenture iDefense for any context available on the selected object.



Change Log

Version	Details
2.0.0	Initial Release