ThreatQuotient

Shodan Operation User Guide

Version 2.1.0

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	2.1.0
Compatible with ThreatQ Versions	>= 4.0.0
Support Tier	ThreatQ Supported

Introduction

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

The operation provides the following action:

- **Query -** queries Shodan for any context it has on the given object.

The operation is compatible with FQDN, IP Address, and URL type Indicators

Prerequisites

You must register for a free account with Shodan at https://www.shodan.io/ in order to receive an API Key. The API Key is required when configuring the operation.

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Token	Your Shodan API Key. See the Prerequisites chapter for details on obtaining a Shodan 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 operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	This action queries Shodan for any context it has on the given object	Indicators	FQDN, IP Address, URL

Query

The Query action quiries Shodan for any context it has on the given FQDN, IP Address, or URL.

URLs, FQDNs

The following endpoint is queried for URLs and FQDNs:

`GET https://api.shodan.io/shodan/host/search`

IP Addresses

The following endpoint is queried for IP Addresses:

`GET https://api.shodan.io/shodan/host/<IP Address>`

Sample Response (both endpoints):

```
{
    "matches": [
        {
            "_shodan": {
                "crawler": "5faf2928ceb560cb4276cc1b4660b2d763cc6397",
                "id": "e57d03a2-be0e-4d1e-b9d5-1126d5aaccba",
                "module": "dht",
                "options": {},
                "ptr": true
            },
            "asn": "AS5650",
            "data": "DHT
Nodes\n71.10.99.93\t17304\n238.52.42.184\t45425\n187.186.123.66\t7914\n105.249.
52.87\t44848\n...",
            "domains": ["frontiernet.net"],
            "hash": 751499058,
            "hostnames": ["47-189-204-206.dlls.tx.frontiernet.net"],
            "ip_str": "47.189.204.206",
            "ip": 800967886,
            "isp": "Frontier Communications",
            "location": {
                "area_code": 281,
                "city": "League City",
                "country_code": "US",
                "country_code3": "USA",
                "country_name": "United States",
                "dma_code": 618,
                "latitude": 29.517300000000006,
                "longitude": -95.0963,
                "postal_code": "77573",
                "region_code": "TX"
            },
            "org": "Frontier Communications",
            "os": null,
            "port": 6881,
            "timestamp": "2020-03-27T05:52:30.229192",
            "transport": "udp"
        }
    ],
    "total": 1
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.matches[].asn	Indicator.Value	ASN	AS5650	N/A
.matches[].cpe	Attribute.Value	CPA		N/A
.matches[].domains	Indicator.Value	FQDN	frontiernet.net	N/A
.matches[].hostnames	Indicator.Value	FQDN	47-189-204-206.dlls.tx.frontiernet.net	N/A
.matches[].http.title	Attribute.Value	HTTP Title		N/A
.matches[].http.host	Indicator.Value	IP Address		N/A
.matches[].ip_str	Indicator.Value	IP Address	47.189.204.206	N/A
.matches[].isp	Attribute.Value	ISP	Frontier Communications	N/A
.matches[].link	Attribute.Value	Link		N/A
.matches[].location.area_code	Attribute.Value	Area Code	281	N/A
.matches[].location.city	Attribute.Value	City	League City	N/A
.matches[].location.country_code	Attribute.Value	Country Code	US	N/A
.matches[].location.country_name	Attribute.Value	Country	United States	N/A
.matches[].location.postal_code	Attribute.Value	Postal Code	77573	N/A
.matches[].location.region_code	Attribute.Value	Region Code	TX	N/A
.matches[].org	Attribute.Value	Organization	Frontier Communications	N/A
.matches[].os	Attribute.Value	Operation System		N/A
.matches[].port	Attribute.Value	Port	6881	N/A
.matches[].product	Attribute.Value	Product		N/A
.matches[].tags[]	Attribute.Value	Tag		N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.matches[].transport	Attribute.Value	Transport	udp	N/A
.matches[].version	Attribute.Value	Version		N/A

Change Log

- **Version 2.1.0**
  - Initial Release
- **Version 2.0.0**
  - Beta Release