ThreatQuotient

Shodan Action Guide

Version 1.0.2

December 06, 2022

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	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/shodan-action

Introduction

The Shodan action for ThreatQ submits a data collection of IP Address objects to the Shodan API. The Shodan API queries the submitted IPs for any services running and returns related threat intelligence to be ingested into the ThreatQ library.

The action provides the following functions:

- **Shodan** - submits an IP Address to the Shodan API to enrich the indicator with all services found by Shodan on the host.

The action is compatible with the IP Address type indicators and returns enriched indicators.

> This action is intended for use with ThreatQ TRD Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The action requires the following:

- An active ThreatQ TRD Orchestrator (TQO) license.
- A data collection containing the IP Address objects.
- A Shodan API Key.

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 action file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

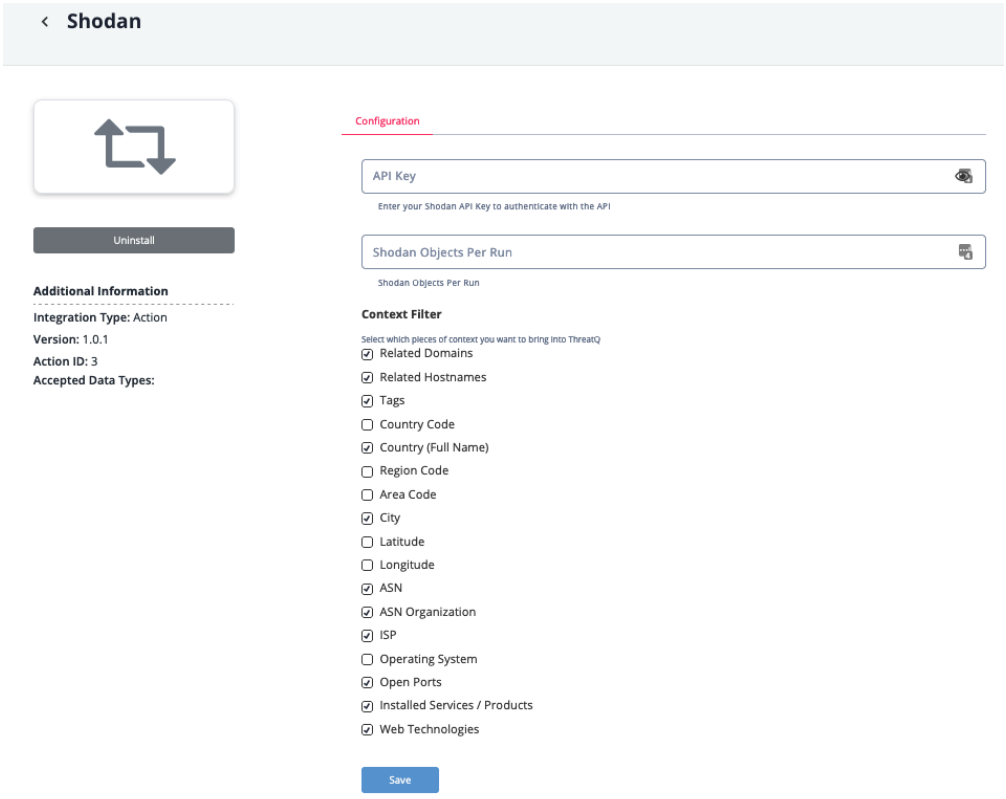
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Your Shodan API Key to authenticate with the API.
Shodan Objects Per Run	The amount of objects per run. The max value for this parameter is 50,000.
Context Filter	Select which pieces of context you want to bring into ThreatQ. Options include: ◦ Related Domains ◦ Related Hostnames ◦ Tags ◦ Country Code ◦ Longitude ◦ ASN ◦ ASN Organization ◦ ISP

PARAMETER	DESCRIPTION
	◦ Country (Full Name) ◦ Region Code ◦ Area Code ◦ City ◦ Latitude ◦ Operating System ◦ Open Ports ◦ Installed Services / Products ◦ Web Technologies



5. Review any additional settings, make any changes if needed, and click on **Save**.

Action Functions

The action provides the following function:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Shodan	Performs IP lookups using the Shodan API.	Indicator	IP Address

Shodan

The Shodan function performs IP lookups and uses the returning data to enrich system indicators.

```
GET https://api.shodan.io/shodan/host/{{ip}}
```

Sample Response:


```
{
  "region_code": "25",
  "tags": ["self-signed"],
  "ip": 2956492918,
  "area_code": null,
  "domains": ["128bit.ee"],
  "hostnames": ["128bit.ee"],
  "country_code": "IT",
  "org": "Lasi SA",
  "data": [
    {
      "ip": 2956492918,
      "hash": 1132111599,
      "port": 443,
      "transport": "tcp",
      "location": {
        "city": "Milan",
        "region_code": "25",
        "area_code": null,
        "longitude": 9.18951,
        "country_name": "Italy",
        "country_code": "IT",
        "latitude": 45.46427
      },
      "product": "nginx",
      "http": {
        "status": 200,
        "robots_hash": null,
        "redirects": [],
```

```
      "securitytxt": null,
      "title": null,
      "sitemap_hash": null,
      "robots": null,
      "server": "nginx",
      "headers_hash": -723384840,
      "host": "176.56.128.118",
      "html": "",
      "location": "/",
      "securitytxt_hash": null,
      "sitemap": null,
      "html_hash": 0
    },
    "tags": ["self-signed"],
    "timestamp": "2022-04-14T22:41:52.130646",
    "ssl": {
      "chain_sha256": [
        "a9033f37cf0e5f652e17d3bdb4da913b63c1e2491e5f2c037f048e5e6e223000"
      ],
      "jarm": "2ad2ad0002ad2ad0002ad2ad2ad2ade1a3c0d7ca6ad8388057924be83dfc6a",
      "chain": [
        "-----BEGIN CERTIFICATE-----
\nMIIDzzCCAregAwIBAgIUBeABPSia7G4H8wZZ2PMX7qA9QnowDQYJKoZIhvcNAQEL\nBQAwdzELMAkGA1UEBhMCR0
IxDzANBgNVBAgMBkxvbmRvbjEPMA0GA1UEBwwGTG9u\nZG9uMRgwFgYDVQQKDA9HbG9iYWwgU2VjdXJpdHkxFjAUBg
NVBAsMDUlUIERlcGFy\ndG1lbnQxFDASBgNVBAMMC2V4YW1wbGUuY29tMB4XDTIyMDQxMjEyMjQ1N1oXDTIz\nMDQx
MjEyMjQ1N1owdzELMAkGA1UEBhMCR0IxDzANBgNVBAgMBkxvbmRvbjEPMA0G\nA1UEBwwGTG9uZG9uMRgwFgYDVQQK
DA9HbG9iYWwgU2VjdXJpdHkxFjAUBgNVBAsM\nDUlUIERlcGFydG1lbnQxFDASBgNVBAMMC2V4YW1wbGUuY29tMIIB
IjANBgkqhkiG\n9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4q3GumzgU1ZB9lgGyTTI3v4xueDuJdBgMMan\n8jsvw388KR
ALrZkpYf2fgSB3Shg1CuWmIRywk5fq13BAlRGX/Y2mqrNyxmEhPJMx\nlN0D5pWZWcmy/eGehPZgoqItbZvWZ1BKH/
gTzRdg+OjQ/j4WxQvl97lgLKYzmgzy\nvpTSCoiAowC8rloiq3uL/cKzKNCsyZ2qB27CgAVVB7PGw0QbdNDWuCUf2Y
pN8l2U\nL7PqlcP3qNuwQoUd/DhvF4GEuIEUvF3BvvsaqsnrF3jZ3La9zaMbJkEtne6YwD9O\nocj+W4/ZCzXPNtwv
1koEnHgH+OMyINAjoC5kR5jpf3pg1YYaewIDAQABo1MwUTAd\nBgNVHQ4EFgQUjeNmtcFNp8jQgahJ33cPIdcnOvEw
HwYDVR0jBBgwFoAUjeNmtcFN\np8jQgahJ33cPIdcnOvEwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOC
\nAQEAfqdjComaUsBxvgu2NhvFH7KIBwTJ6KiHwsZH48xxMO5RbInASlABmAUxrXWW\nC5yFhl+5ajq++PaCYUF2xL
ax1/B4edVQ93yNmwu1/JaxxoiJv0m0CiORCgPG5TEN\nfhPkaGMvysEpuRDYv/yM9ccYMheDEdqxIA7Ve3MK8Q6JkV
iTHwKxCmosPP4Jh6C6\n6iTw7AoKFe4bf67JVanOMffchsxsDFuzvyFCE+EAJc+Gn+bEqrNnreaoVfUjkd+9\nrLo7
4HwwZGXOi55fskz6+CRS2R1oatk/K88oQiHtCr+E8VVTr5zXnqFOs6o1L8As\nSh3JJnpnHUE8AcGh2Fv3xE/SFg==
\n-----END CERTIFICATE-----\n"
      ],
      "dhparams": null,
      "versions": [
        "-TLSv1",
        "-SSLv2",
        "-SSLv3",
        "-TLSv1.1",
        "TLSv1.2",
        "-TLSv1.3"
      ],
      "acceptable_cas": [],
      "tlsext": [
        {
          "id": 65281,
          "name": "renegotiation_info"
        },
        {
          "id": 11,
          "name": "ec_point_formats"
        },
        {
          "id": 35,
          "name": "session_ticket"
```

```
        }
      ],
      "alpn": ["http/1.1"],
      "cert": {
        "sig_alg": "sha256WithRSAEncryption",
        "issued": "20220412122457Z",
        "expires": "20230412122457Z",
        "pubkey": {
          "bits": 2048,
          "type": "rsa"
        },
        "version": 2,
        "extensions": [
          {
            "data": "\\x04\\x14\\x8d\\xe3f\\xb5\\xc1M\\xa7\\xc8\\xd0\\x81\\xa8I\\xdfw\
\x0f!\\xd7\\':\\xf1",
            "name": "subjectKeyIdentifier"
          },
          {
            "data": "0\\x16\\x80\\x14\\x8d\\xe3f\\xb5\\xc1M\\xa7\\xc8\\xd0\\x81\\xa8I\
\xdfw\\x0f!\\xd7\\':\\xf1",
            "name": "authorityKeyIdentifier"
          },
          {
            "critical": true,
            "data": "0\\x03\\x01\\x01\\xff",
            "name": "basicConstraints"
          }
        ],
        "fingerprint": {
          "sha256": "a9033f37cf0e5f652e17d3bdb4da913b63c1e2491e5f2c037f048e5e6e223000",
          "sha1": "55fa46031f38791fcf160902656b539e89969810"
        },
        "serial": 335404287020739000561981689405646124563088840 90,
        "issuer": {
          "C": "GB",
          "CN": "example.com",
          "L": "London",
          "O": "Global Security",
          "ST": "London",
          "OU": "IT Department"
        },
        "expired": false,
        "subject": {
          "C": "GB",
          "CN": "example.com",
          "L": "London",
          "O": "Global Security",
          "ST": "London",
          "OU": "IT Department"
        }
      },
      "cipher": {
        "version": "TLSv1/SSLv3",
        "bits": 256,
        "name": "ECDHE-RSA-AES256-GCM-SHA384"
      },
      "trust": {
        "revoked": false,
        "browser": null
      },
```

```
        "handshake_states": [
          "before/connect initialization",
          "SSLv2/v3 write client hello",
          "SSLv2/v3 read server hello",
          "SSLv3/TLS read server hello",
          "SSLv3/TLS read server certificate",
          "SSLv3/TLS read server key exchange",
          "SSLv3/TLS read server done",
          "SSLv3/TLS write client key exchange",
          "SSLv3/TLS write change cipher spec",
          "SSLv3/TLS write finished",
          "SSLv3/TLS flush data",
          "SSLv3/TLS read server session ticket",
          "SSLv3/TLS read finished",
          "SSL negotiation finished successfully"
        ],
        "ja3s": "e35df3e00ca4ef31d42b34bebaa2f86e",
        "ocsp": {}
      },
      "hostnames": [],
      "org": "Lasi SA",
      "data": "HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: Thu, 14 Apr 2022 22:41:52
GMT\r\nContent-Type: text/html; charset=UTF-8\r\nTransfer-Encoding: chunked\r\nConnection:
keep-alive\r\n\r\n",
      "asn": "AS12637",
      "cpe23": ["cpe:2.3:a:igor_sysoev:nginx"],
      "isp": "SEEWEB s.r.l.",
      "cpe": ["cpe:/a:igor_sysoev:nginx"],
      "domains": [],
      "ip_str": "176.56.128.118",
      "os": null,
      "_shodan": {
        "id": "3153f648-fe43-41af-b3bc-72a0508e1ec7",
        "ptr": true,
        "options": {},
        "module": "https",
        "crawler": "91597136eb9b132d7cc954511e0d9cbe7ce2e377"
      },
      "opts": {
        "vulns": [],
        "heartbleed": "2022/04/14 22:42:06 176.56.128.118:443 - SAFE\n"
      }
    },
    {
      "_shodan": {
        "id": "00633169-f138-4344-ba79-6b46ba65debe",
        "ptr": true,
        "options": {},
        "module": "auto",
        "crawler": "240a12b6c2ac5dba30ed961e4ab8f056540fdaf0"
      },
      "hash": 0,
      "os": null,
      "opts": {},
      "timestamp": "2022-04-16T19:16:39.858796",
      "isp": "SEEWEB s.r.l.",
      "asn": "AS12637",
      "hostnames": [],
      "location": {
        "city": "Milan",
        "region_code": "25",
```

```
        "area_code": null,
        "longitude": 9.18951,
        "country_name": "Italy",
        "country_code": "IT",
        "latitude": 45.46427
      },
      "ip": 2956492918,
      "domains": [],
      "org": "Lasi SA",
      "data": "",
      "port": 2000,
      "transport": "tcp",
      "ip_str": "176.56.128.118"
    },
    {
      "ip": 2956492918,
      "_shodan": {
        "id": "b0baecc9-252e-4cba-90ac-03e607e87eac",
        "ptr": true,
        "options": {},
        "module": "http-simple-new",
        "crawler": "cdd92e2d835a37d2798fa6c7105171f4d214012f"
      },
      "product": "nginx",
      "http": {
        "status": 403,
        "robots_hash": null,
        "redirects": [],
        "securitytxt": null,
        "title": "403 Forbidden",
        "sitemap_hash": null,
        "robots": null,
        "server": "nginx",
        "headers_hash": -1002489980,
        "host": "176.56.128.118",
        "html": "<html>\r\n<head><title>403 Forbidden</title></head>\r\n<body
bgcolor=\"white\">\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx</
center>\r\n</body>\r\n</html>\r\n<!-- a padding to disable MSIE and Chrome friendly error
page -->\r\n<!-- a padding to disable MSIE and Chrome friendly error page -->\r\n<!-- a
padding to disable MSIE and Chrome friendly error page -->\r\n<!-- a padding to disable
MSIE and Chrome friendly error page -->\r\n<!-- a padding to disable MSIE and Chrome
friendly error page -->\r\n<!-- a padding to disable MSIE and Chrome friendly error page
-->\r\n",
        "location": "/",
        "components": {},
        "securitytxt_hash": null,
        "sitemap": null,
        "html_hash": 1965132531
      },
      "os": null,
      "opts": {},
      "timestamp": "2022-04-11T09:34:51.435080",
      "isp": "SEEWEB s.r.l.",
      "cpe": ["cpe:/a:igor_sysoev:nginx"],
      "ip_str": "176.56.128.118",
      "asn": "AS12637",
      "hostnames": [],
      "cpe23": ["cpe:2.3:a:igor_sysoev:nginx"],
      "org": "Lasi SA",
      "domains": [],
      "hash": -435134027,
```

```
      "data": "HTTP/1.1 403 Forbidden\r\nServer: nginx\r\nDate: Mon, 11 Apr 2022 09:34:51
GMT\r\nContent-Type: text/html\r\nContent-Length: 564\r\nConnection: keep-alive\r\n\r\n",
      "port": 5000,
      "transport": "tcp",
      "location": {
        "city": "Milan",
        "region_code": "25",
        "area_code": null,
        "longitude": 9.18951,
        "country_name": "Italy",
        "country_code": "IT",
        "latitude": 45.46427
      }
    },
    {
      "_shodan": {
        "id": "6b01d22b-22a4-4c60-a2b3-c82793ca0635",
        "ptr": true,
        "options": {},
        "module": "https-simple-new",
        "crawler": "dfd12d70c30ccb3812bf26f89905deeb85e98c77"
      },
      "http": {
        "status": 200,
        "robots_hash": null,
        "redirects": [],
        "securitytxt": null,
        "title": "3CX Phone System Management Console",
        "sitemap_hash": null,
        "robots": null,
        "favicon": {
          "data": "iVBORw0KGgoAAAANSUhEUgAAACAAAAAgEAYAAAAj6qa3AAAABmJLR0T///////
8JWPfcAAAACXBI\nWXMAAABIAAA
ASABGyWs+AAAACXZwQWcAAAAgAAAAIACH+pydAAADfUlEQVRo3s2ZXUgUURTH98
OW\nakkpYh+KRSnFrNRQSQItKykLetAKSqQIIsWHyiSjXG0Fc1VKi1ALi9TKtC0zKgMp0MogISItMwoq\nNsM0kyTN
dMMe/meEGWbTdfaMnZcfO8Pec8//3nPmfmg1bprJVFra3i78WnoOrI8DA3zdbc89K4kB\n05rBUU1PT2pqcPDUW9Qp
61BHClhIAvx+wCvArkYwIV14Ih4QFQSQV7x6EVhj5xVgjgHMPg0GXlTa\nolZpA+IR8C8G65+Ay27wClKrB/cuBH86
3E0JhSkgtfdpYC51YTCWV4D4q2DSY+GJuymhWAB5xeu6\nwMoIXgEMO8Ajb8CITHdbUJwCUhOPgDkEtG8EIwt5BWmI
ApOoWPYbJ0oJD6eA1Bxt4IkL4I9uXn9x\no2AK1QatbaKU8LgA8orfDwXLA+jBIR4BdM+o+TBw7XbhjSsh2GaAWAhn
E3gyHmy6yeUXNv81aKWF\n2YJwl5LxdkRqXy+DuVQL+oJ4/UUPgQeyQX2VdCZ4vAi6MrFj7SfQ8hK0Pgd1Vh7vA7SA
2pMA1tUK\nb1SbAeKUGKOpWVINNm7i9e49AuY8Ahd3qi6AvBDfa8DjD0FHDK/35V/AjB5wpkl1AeStlRYwZ+aB\nzg
Zef4lGcN9+1WqAKxPXBhPVhsadYGgLr/e2bdM2A+S/yxsqQf8BXu/9VjD/6X+SAoFF4LFo0Khg\nh/9PuwKU3wHtZt
UFEI/87G9gFm2fg2J4vTdTjSmuAJ2tqgkgP+V3U/Xf/o7X+2eq/pl0gNIdIryZ\nphSILACPzgINbTx+nGawkIRuqR
PeCJ9jdgHEI+9DJ0YWH9C8hde7/S54qUoauGBsn0HJlH8FZNBu\nMM8b1A/zeO+8DW6llWbHdVfnAh6fAfK5vo78pO
fxBj6YDFq9hMAn+ocXT0fG5SgBs+mkxtTH669i\nCXhr/HRatRMh8cjrqOqmrQDX/OINvGU1aFsJjlRO9nRYsQDyU3
4zHXgk03deM8QTeO8pMGs92BXl\nbgseTgFf6kjOWXDuW57A/9DmqYj2Ck2rhDeq3QuIR35GL3iYRiCMKXDB7tEVXB
ndTY7lT/WOUK8s\ncMFo86bJ8gMN4ZNv0R37UAamktAfY5VejipMgUA6YbE4QGMiT+DDFtDmBF8UeKrlSS+EJJsYOs
sr\nt4GJ13gCF+w8BX7QjwTpUjrygv0FK7crLMjvW2oAAABZelRYdFNvZnR3YXJlAAB42vPMTUxP9U1M\nz0zOVjDT
M9KzUDAw1Tcw1zc0Ugg0NFNIy8xJtdIvLS7SL85ILErV90Qo1zXTM9Kz0E/JT9bPzEtJ\nrdDLKMnNAQCtThisdBUu
awAAACF6VFh0VGh1bWI6OkRvY3VtZW50OjpQYWdlcwAAeNozBAAAMgAy\nDBLihAAAACF6VFh0VGh1bWI6OkltYWdl
OjpoZWlnaHQAAHjaMzMyAQABPQCdhy3QKAAAACB6VFh0\nVGh1bWI6OkltYWdlOjpXaWR0aAAAeNozNrcAAAFCAKPM
ZvwvAAAAInpUWHRUaHVtYjo6TWltZXR5\ncGUAAHjay8xNTE/VL8hLBwARewN4XzlH4gAAACB6VFh0VGh1bWI6Ok1U
aW1lAAB42jM0MTUxMzcz\nNrMAAAtIAhNXXjtGAAAAGXpUWHRUaHVtYjo6U2l6ZQAAeNozNMpOAgAClgExPX1XPQAA
ABx6VFh0\nVGh1bWI6OlVSSQAAeNpLy8xJtdLX1wcADJoCaJRAUaoAAAAASUVORK5CYII=\n",
          "hash": 970132176,
          "location": "https://176.56.128.118:5001/favicon.ico"
        },
        "headers_hash": -433350924,
        "host": "176.56.128.118",
        "html": "<!doctype html><html ng-app=\"app\" ng-csp=\"no-unsafe-eval\"
lang=\"en\"><head><meta charset=\"UTF-8\"><title>3CX Phone System Management Console</
```

```
title><link rel=\"icon\" type=\"image/x-icon\" href=\"/favicon.ico\"><meta
name=\"viewport\" content=\"width=device-width,initial-scale=1,maximum-scale=1\"/><base
href=\"/\"><link href=\"992.9980c355.bundle.css\" rel=\"stylesheet\"><link
href=\"main.a20588e2.bundle.css\" rel=\"stylesheet\"></head><body><noscript><div
style=\"display: flex; align-items: center; justify-content: center; height: 100%\"><h1
class=\"padding20\">You must have JavaScript enabled to use this app.</h1></div></
noscript><div ng-controller=\"AppCtrl\" id=\"content\" class=\"h-full\" ui-view
style=\"display: flex; overflow: hidden\"></div><script defer=\"defer\"
src=\"runtime.3819602b.bundle.js\"></script><script defer=\"defer\"
src=\"992.04ab934f.bundle.js\"></script><script defer=\"defer\"
src=\"main.df5528a8.bundle.js\"></script></body></html>",
        "location": "/",
        "components": {
          "AngularJS": {
            "categories": ["JavaScript frameworks"]
          }
        },
        "securitytxt_hash": null,
        "server": "nginx",
        "sitemap": null,
        "html_hash": -723903722
      }
  ],
  "asn": "AS12637",
  "city": "Milan",
  "latitude": 45.46427,
  "isp": "SEEWEB s.r.l.",
  "longitude": 9.18951,
  "last_update": "2022-04-16T19:16:39.858796",
  "country_name": "Italy",
  "ip_str": "176.56.128.118",
  "os": null,
  "ports": [2000, 5000, 443, 5060, 5001]
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
`.region_code`	Indicator.Attribute	Region Code	N/A	N/A	`NA`	If enabled
`.area_code`	Indicator.Attribute	Area Code	N/A	N/A	N/A	If enabled
`.country_code`	Indicator.Attribute	Country Code	N/A	N/A	`CH`	If enabled
`.org`	Indicator.Attribute	ASN Organization	N/A	N/A	`Lasi SA`	If enabled
`.city`	Indicator.Attribute	City	N/A	N/A	`Milan`	If enabled
`.isp`	Indicator.Attribute	ISP	N/A	N/A	`SEEWEB s.r.l.`	If enabled
`.longitude`	Indicator.Attribute	Longitude	N/A	N/A	`83.1`	If enabled
`.latitude`	Indicator.Attribute	Latitude	N/A	N/A	`-45.2`	If enabled
`.country_name`	Indicator.Attribute	Country	N/A	N/A	`China`	If enabled
`.os`	Indicator.Attribute	Operating System	N/A	N/A	`Windows`	If enabled
`.ports[]`	Indicator.Attribute	Open Port	N/A	N/A	`8001`	If enabled
`.data[].product`	Indicator.Attribute	Installed Service	N/A	N/A	`nginx`	If enabled
`.data[].http.components.[KEY]`	Indicator.Attribute	Web Technology	N/A	N/A	`AngularJS`	If enabled
`.tags[]`	Indicator.Tag	N/A	N/A	N/A	`self-signed`	If enabled
`.domains[]`	Indicator.Indicator	FQDN	N/A	N/A	N/A	If enabled
`.hostnames[]`	Indicator.Indicator	FQDN	N/A	N/A	N/A	If enabled
`.asn`	Indicator.Indicator	ASN	N/A	N/A	`AS12637`	If enabled

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	5 minutes
Indicators	351
Indicator Attributes	4,178

Use Case Example

1. A user submits an IP Address using the Shodan action to the Shodan API.
2. The Shodan API queries the submitted IP Address for service data.
3. The action returns indicators enriched with service data from the Shodan API.

Known Issues / Limitations

- The action is limited based on your Shodan rate limit. This rate limit is based on your Shodan subscription type.

Change Log

- **Version 1.0.2**
  - Initial release to the ThreatQ Marketplace.