ThreatQuotient

Spur Operation Guide

Version 1.0.0

May 30, 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

Integration Details ... 5
Introduction ... 6
Prerequisites ... 7
Installation ... 7
Configuration ... 8
Actions ... 9
Get Context ... 10
Change Log ... 12

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	1.0.0
Compatible with ThreatQ Versions	>= 4.56.0
Support Tier	ThreatQ Supported

Introduction

Spur tracks anonymization services so that you can identify when anonymization services are touching your website, application, or network.

The Spur Operation allows analysts to perform quick context lookups for a given IP Address, bringing back anonymization information that can be used to determine if the IOC is a possible threat.

The Get Context action enables the automatic enrichment of IP Addresses in ThreatQ, using Spur's Context API. The API will tell you if the selected IOCs are used by anonymization services, as well as if the tunnels are used by a specific region, or used by a specific threat.

The operation provides the following action:

- **Get Context** - returns the context information collected by Spur about the selected IP.

The operation is compatible with the following indicator types:

- IP Address
- IPv6 Address

Prerequisites

The operation requires the following:

- A valid Spur 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 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
Spur API Key	Your Spur 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
Get Context	Performs a lookup against the Spur Context API	Indicators	IP Address, IPv6 Address

Get Context

The Get Context action performs a lookup against Spur's API to enrich an IP Address with context pertaining to whether the IOC is used for tunnels and/or anonymization, as well as how the tunnel is typically used by threats.

```
GET https://api.spur.us/v2/context/{{ ip }}
```

Sample Response:

```
{
  "as": {
    "number": 30083,
    "organization": "AS-30083-GO-DADDY-COM-LLC"
  },
  "client": {
    "behaviors": ["TOR_PROXY_USER"],
    "concentration": {
      "city": "Weldon Spring",
      "country": "US",
      "density": 0.202,
      "geohash": "9yz",
      "skew": 45,
      "state": "Missouri"
    },
    "count": 14,
    "countries": 1,
    "proxies": ["LUMINATI_PROXY", "SHIFTER_PROXY"],
    "spread": 4941431,
    "types": ["MOBILE", "DESKTOP"]
  },
  "infrastructure": "DATACENTER",
  "ip": "148.72.164.186",
  "location": {
    "city": "St Louis",
    "country": "US",
    "state": "Missouri"
  },
  "risks": ["WEB_SCRAPING", "TUNNEL"],
  "services": ["IPSEC", "OPENVPN"],
  "tunnels": [
    {
      "anonymous": true,
      "entries": ["148.72.164.179"],
      "exits": ["148.72.164.177"],
      "operator": "NORD_VPN",
      "type": "VPN"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.as.number`	Indicator.Attribute	ASN	N/A	`30083`	N/A
`.as.organization`	Indicator.Attribute	AS Organization	N/A	`AS-30083-GO-DADDY-COM-LLC`	N/A
`.client.behaviors[]`	Indicator.Attribute	Client Behavior	N/A	`TOR_PROXY_USER`	N/A
`.client.concentration.city`	Indicator.Attribute	Client Concentration City	N/A	`Weldon Spring`	N/A
`.client.concentration.country`	Indicator.Attribute	Client Concentration Country Code	N/A	`US`	N/A
`.client.concentration.state`	Indicator.Attribute	Client Concentration State	N/A	`Missouri`	N/A
`.client.concentration.density`	Indicator.Attribute	Client Concentration Density	N/A	`0.202`	N/A
`.client.concentration.geohash`	Indicator.Attribute	Client Concentration Geohash	N/A	`9yz`	N/A
`.client.concentration.skew`	Indicator.Attribute	Client Concentration Skew	N/A	`45`	N/A
`.client.proxies[]`	Indicator.Attribute	Client Proxy	N/A	`SHIFTER_PROXY`	N/A
`.client.types[]`	Indicator.Attribute	Client Type	N/A	`DESKTOP`	N/A
`.infrastructure`	Indicator.Attribute	Infrastructure	N/A	`DATACENTER`	N/A
`.location.city`	Indicator.Attribute	City	N/A	`St Louis`	N/A
`.location.country`	Indicator.Attribute	Country Code	N/A	`US`	N/A
`.location.state`	Indicator.Attribute	State	N/A	`Missouri`	N/A
`.risks[]`	Indicator.Attribute	Risk	N/A	`WEB_SCRAPING`	N/A
`.services[]`	Indicator.Attribute	Service	N/A	`IPSEC`	N/A
`.tunnels[].operator`	Indicator.Attribute	Tunnel Operator	N/A	`NORD_VPN`	N/A
`.tunnels[].type`	Indicator.Attribute	Tunnel Type	N/A	`VPN`	N/A
`.tunnels[].entries[]`	Indicator.Value	IP Address	N/A	N/A	N/A
`.tunnels[].exits[]`	Indicator.Value	IP Address	N/A	N/A	N/A
`.tunnels[].anonymous`	Indicator.Attribute	Is Anonymized	N/A	`True`	N/A
N/A	Indicator.Attribute	Node Type	N/A	`Entry`	`Entry`if the IP is in `.tunnels[].entries[]`. `Exit` if the IP is in `.tunnels[].exits[]`

Change Log

- **Version 1.0.0**
    - Initial release