ThreatQuotient

Spur Enrichment Action 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

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	>= 5.14.0
ThreatQ TQO License Required	Yes
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 Enrichment 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 action can perform the following functions:

- **Spur Enrichment** - utilizes Spur's API to enrich an IP Address with context pertaining to whether the IOC is used for tunnels and/or anonymization.

The action is compatible with the following indicator types:

- IP Address
- IPv6 Address

The action returns enriched IP Address and IPv6 Address type indicators.

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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A Spur API Key.
- A data collection containing at least one of the following indicator types:
  - IP Address
  - IPv6 Address

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 zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip 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.

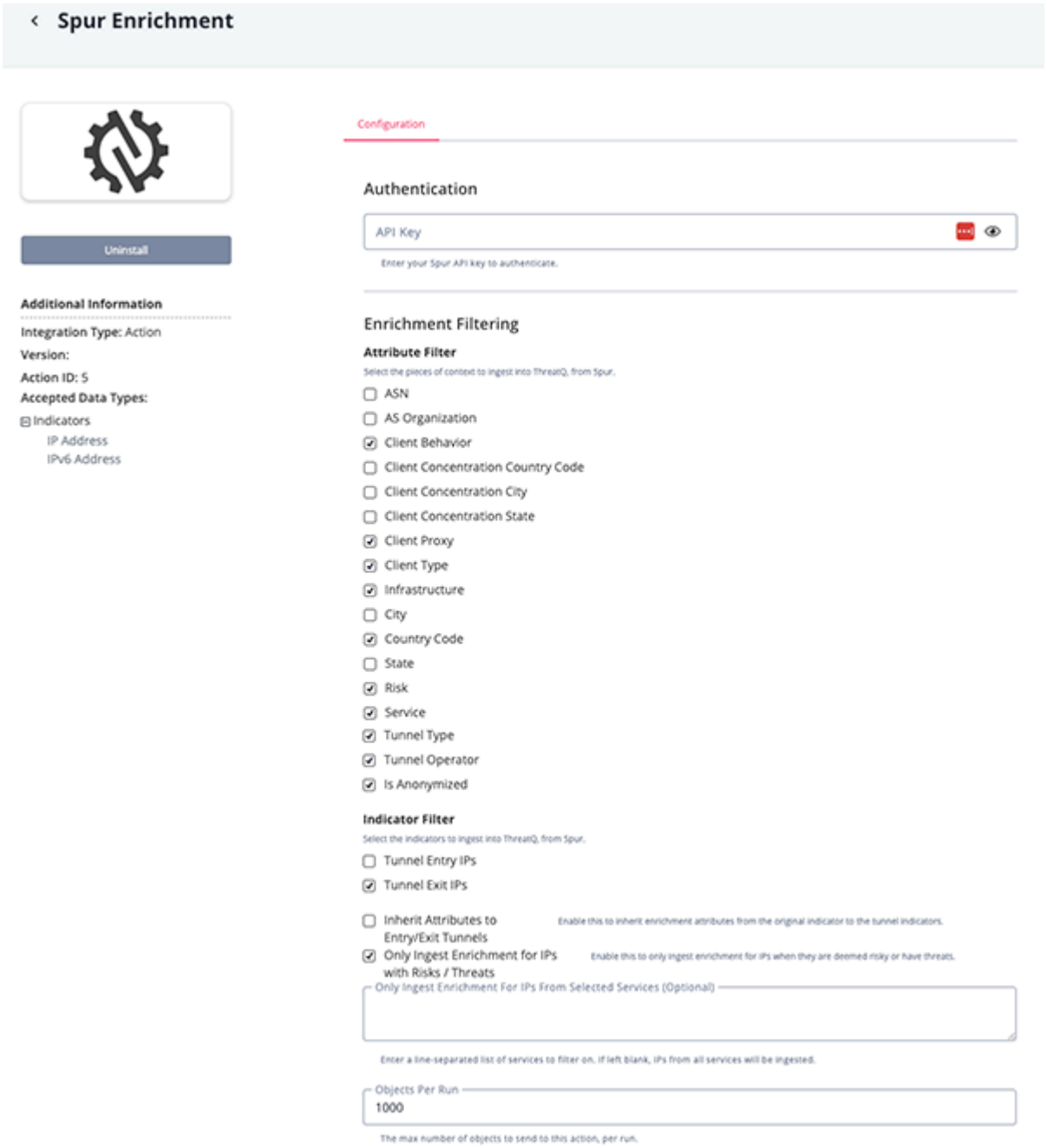
To configure the integration:

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	The API Key from the Spur Account
Attribute Filter	Select the pieces of context to ingest into ThreatQ, from Spur. Options include: ◦ ASN ◦ AS Organization ◦ Client Behavior (default) ◦ Client Concentration Country Code ◦ Client Concentration City ◦ Client Concentration State ◦ City ◦ Country Code ◦ State ◦ Risk (default) ◦ Service (default) ◦ Tunnel Type (default)

PARAMETER	DESCRIPTION
	◦ Client Proxy (default) ◦ Client Type (default) ◦ Infrastructure (default) ◦ Tunnel Operator (default) ◦ Is Anonymized (default)
Indicator Filter	Select the indicators to ingest into ThreatQ, from Spur. Options include: ◦ **Tunnel Entry IPs** ◦ **Tunnel Exit IPs** (default) ◦ **Inherit Attributes to Entry/Exit Tunnels** - Enable this to inherit enrichment attributes from the original indicator to the tunnel indicators. This parameter is disabled by default. ◦ **Only Ingest Enrichment for IPs with Risks / Threats** (default) - Enable this to only ingest enrichment for IPs when they are deemed risky or have threats.
Only Ingest Enrichment for IPs from Selected Services (Optional)	Enter a line-separated list of services to filter on. If left blank, IPs from all services will be ingested.
Objects Per Run	The max number of objects per run to send to this action. The default value is 1000.



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

Actions

The integration performs the following action:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Spur Enrichment	Fetches contextual information from the Spur API.	Indicator	IP Address, IPv6 Address

Spur Enrichment

The Spur Enrichment action will use 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.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[]`

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	2 minutes
Indicators	225
Indicator Attributes	782

Use Case Example

1. A Threat Analyst wants to identify when anonymized services (VPNs and Proxies) are contacting the network infrastructure and take action when the activity is a known threat.
2. The Threat Analyst creates a collection of Indicators that have the type IP Address or IPv6 Address.
3. The Threat Analyst adds the Spur Enrichment action to a Workflow.
4. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
5. The action will enrich the indicators with information that indicates if they are used by anonymization services.

Known Issues / Limitations

- When the action is run on a unnormalized IPv6 Address ,a new indicator with the normalized value will be created and enriched. The original indicator will not be enriched.

Change Log

- **Version 1.0.0**
  - Initial release