Getting started with ThreatPoint IP Reputation API

The ThreatPoint IP Reputation is a rest API that delivers IP intelligence based on IP data aggregation, exit node, proxy and VPN monitoring and consortium data.

Score and risk elements returned:

Item	Example	Description
Date/Time	-	Date IP first seen by ThreatPoint
IP Address	-	The IP passed to the API
Risk	High – Tor detected	IP assigned to a Tor Exit Node
Source	ThreatPoint	The source of the IP data
Country Code	US	ISO 2 character code
Country Name	United States	-
Last Update	Date/Time	The last time the IP address was seen by ThreatPoint
Latitude	35.1746101379395	-
Longitude	-94.6869888305664	-
Region Code	OK	-
Region Name	Oklahoma	-
Zip	74951	-

All requests submitted to the IP reputation API:

- Require an API key
- Use https://verify.threatpoint.co.uk/api/v1/resources/ip?ipaddress=<ipaddress> as the endpoint
- Accepts only valid IP v4 or IP v6 addresses as inputs
- Use X-Api-Key with the valid API key in the request header

Risk examples

The IP reputation risk level is a measure of the perceived risk in allowing access from that IP address. Of course IP reputation is subjective depending on the business vertical and use case. The table below shows the recommend decisions based on the risk levels delivered in the response.

Risk Level	Recommendation
High	Redirect or Block
Consider	Redirect
Low	Allow

IP Reputation API examples

curl example

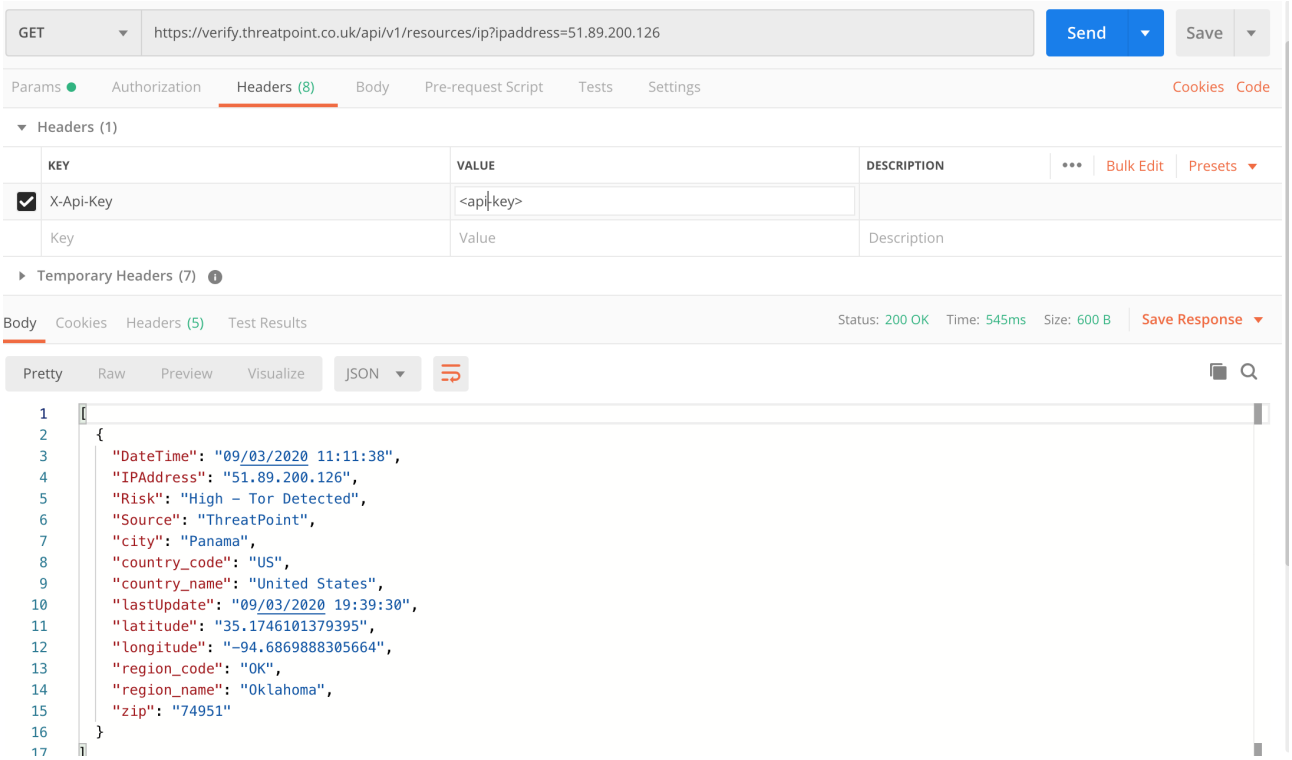
```
curl -i -H 'X-Api-Key:<api-key>' http://127.0.0.1:5000/api/v1/resources/ip?ipaddress=51.89.200.126
```

When you send the number the risk level and other elements are returned in the response:

curl results


```
{
  "DateTime": "09/03/2020 12:41:00",
  "IPAddress": "51.89.200.126",
  "Risk": "High - Tor Detected",
  "Source": "ThreatPoint",
  "city": "Panama",
  "country_code": "US",
  "country_name": "United States",
  "lastUpdate": "09/03/2020 19:35:56",
  "latitude": "35.1746101379395",
  "longitude": "-94.6869888305664",
  "region_code": "OK",
  "region_name": "Oklahoma",
  "zip": "74951"
}
```

Postman example



If something goes wrong the response will provide the reason.

Error for missing or invalid API key

```
{
  "message": "ERROR: Unauthorized"
}
```

Error for invalid IP address:

```
{
  "error": "Invalid IP V4/V6 provided"
}
```

Next Steps

Request an API key from ThreatPoint by emailing info@threatpoint.co.uk

Wordpress user? Download the ThreatPoint IP reputation plugin which utilises the IP reputation API.

https://wordpress.org/plugins/threatpoint-api/