IP reputation

Review the basics of making API calls to IP Intel

Use the /reputation endpoint to make an API call and return IP address details. You can create an API request to retrieve as little or as many details as you need.

Note

For more information, visit the interactive IP Intel API Reference.

Look up the reputation score of an IP

Allows you to retrieve the IP score (normalized by Pangea) for a specific IP. Based on that score (which will fall under one of these categories: benign, suspicious, malicious, or unknown), you can determine actions your application should take.

Use Case: Check the client IP of unauthenticated activities like file uploads, newsletter subscriptions, and account sign ups.

Example: To retrieve only the IP score (normalized by Pangea), create your API request using the only required body parameter: `ip` . Your API Request might look like the example below:

POST /v1/reputation cURL

```
curl -sSLX POST 'https://ip-intel.aws.us.pangea.cloud/v1/reputation' \
-H 'Authorization: Bearer <your_token>' \
-H 'Content-Type: application/json' \
-d '{"ip":"93.231.182.110"}'
```

Retrieve a detailed intelligence report for an IP

Allows you to receive a report containing provider data intelligence in your API response (in addition to the IP score).

Use Case: This capability is very similar to the capability above (Look up reputation score of an IP). However, a comprehensive report, full of rich data, can help you analyze and pinpoint larger trends.

Example: To receive a report containing provider data intelligence in your API response (in addition to the IP score), set `raw` and `verbose` to `true` in your API request. And make sure you've set a `provider` as default in the Pangea Console.

```
POST  /v1/reputation                                                                cURL

curl -sSLX POST 'https://ip-intel.aws.pangea.cloud/v1/reputation' \
-H 'Authorization: Bearer <your_token>' \
-H 'Content-Type: application/json' \
-d '{"provider":"crowdstrike","ip":"93.231.182.110","verbose":true,"raw":true}'
```

Tip

You can also select a provider and override the default provider by specifying their name in the `provider` field when making an API request to the `reputation` endpoint. This is helpful if your default provider returns a verdict of `Unknown` and you want a second opinion from another provider.

Geolocate an IP

Allows you take an IP address and determine the geographic location from which it came.

Use case: Send the client IPs of your users to the geolocate endpoint to understand where they are coming from. Use this information to pre-populate forms with country information or even default to specific language if your application has that capability. Further, this could be used to understand and record activity to a specific country in something like Secure Audit Log.

Example: To retrieve the location of an IP, create your API request using the only required body parameter: `ip` and call the /geolocate endpoint. You can request additional data in your API response by setting `raw` and `verbose` to `true` in your API request. However, this additional raw data is not reflected in the example below.

```
POST  /v1/geolocate                                                                 cURL
```

```
curl -sSLX POST 'https://ip-intel.aws.pangea.cloud/v1/geolocate' \
-H 'Authorization: Bearer <your_token>' \
-H 'Content-Type: application/json' \
-d '{"ip":"93.231.182.110"}'
```

Check if an IP is from VPN

Allows you to take an IP and determine whether it is coming from a known VPN service

Use case: In some cases, you application's content may not be permitted in certain countries. Often times, users will try to get around this by using a VPN so they can appear to be located in a permissable country. Use this endpoint to submit a client IP and understand if it belongs to a commercial VPN service. If so, determine whether or not you want to allow this activity to continue.

Example: To check if an IP is being hosted on a VPN service, create your API request using the only required parameter: `ip` and call the /vpn endpoint. You can request additional data in your API response by setting `raw` and `verbose` to `true` in your API request. However, this additional raw data is not reflected in the example below.

POST /v1/vpn cURL

```
curl -sSLX POST 'https://ip-intel.aws.pangea.cloud/v1/vpn' \
-H 'Authorization: Bearer <your_token>' \
-H 'Content-Type: application/json' \
-d '{"ip":"1.46.128.165"}'
```

Check if an IP is from a proxy

Allows you take an IP and determine if it is coming from a proxy server

Use Case: In some cases, you application's content may not be permitted in certain countries or regions. Often times, users will try to get around this by using a proxy server so they can appear to be located in a permissable country/region. Use this endpoint to submit a client IP and understand if it belongs to a known proxy. If so, determine whether or not you want to allow this activity to continue.

Example: To check if an IP is coming from a proxy server, create your API request using the only required parameter: `ip` and call the /proxy endpoint. You can request additional data in your API response by setting `raw` and `verbose` to `true` in your API request. However, this additional raw data is not reflected in the example below.

```
POST  /v1/proxy                                                              cURL

curl -sSLX POST 'https://ip-intel.aws.pangea.cloud/v1/proxy' \
-H 'Authorization: Bearer <your_token>' \
-H 'Content-Type: application/json' \
-d '{"ip":"34.201.32.172"}'
```

Look up domain for an IP

To determine the domain associated with an IP, create your API request using the only required parameter: `ip` and call the /domain endpoint. You can request additional data in your API response by setting `raw` and `verbose` to `true` in your API request. However, this additional raw data is not reflected in the example below.

```
POST  /v1/domain                                                             cURL

curl -sSLX POST 'https://ip-intel.aws.pangea.cloud/v1/domain' \
-H 'Authorization: Bearer <your_token>' \
-H 'Content-Type: application/json' \
-d '{"ip":"24.235.114.61"}'
```

Was this article helpful? 👍 Yes 👎 No Contact us