Check the source IP of incoming web traffic

Check your cloud app for malicious web traffic using IP Intel

The code samples in this use case were created using the Pangea sample apps. If you want to follow along, check out the Pangea sample apps on GitHub:

- Golang
- Node.js
- Python
- Java

Create a token

Expand for details

Create a token so that you can access the IP Intel endpoints:

1. Go to the Pangea Console and click **IP Intel** in the left-hand navigation menu. The IP Intel Overview page will appear.
2. On the IP Intel Overview page, you'll see a notification asking you to set a service token. Click **Create new token** toward the bottom right side of your screen.
3. You'll be prompted to create a token. Enter a **Token name** and select an **Expiration Date**. You may also create a token for all Intel services, if you wish.
4. Once configured, the token is available in the Tokens section of the IP Intel Overview page.

Select your provider

Expand for details

Providers can be selected as default in the Pangea Console. Setting a provider as default in the Pangea Console means your API request calls will use this provider, unless another provider is specified as part of your API request.

To select a provider as default for an API:

1. Go to the Pangea Console
2. On the left-hand navigation menu, select **IP Intel**
3. Go to **Settings**
4. Click **Set as default** for your preferred provider

> **Tip**
>
> You can 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.

Configure your app for communication with the Pangea service

For your app to communicate with the Pangea service, you must set the following environment variables:

- `token`
- `domain`

All of these variables are created when you enable IP Intel and can be found in the **Overview** section under **IP Intel**.

Set environment variables

To set each variable in bash:

```
export PANGEA_DOMAIN="yourServiceDomain"
```

> **Note**
>
> Pangea services are cloud agnostic and deployed regionally, so service endpoints may vary.

```
export IP_INTEL_AUTH_TOKEN="yourAccessToken"
```

Send IP to IP Intel service

A `reputation` call from your app to the IP Intel service might look like this:

LANGUAGE


```python
import os

import pangea.exceptions as pe
from pangea.config import PangeaConfig
from pangea.services import IpIntel

token = os.getenv("PANGEA_IP_INTEL_TOKEN")
domain = os.getenv("PANGEA_DOMAIN")
config = PangeaConfig(domain=domain)
intel = IpIntel(token, config=config)


def main():

    try:
        response = ip.reputation(
            ip="93.231.182.110",
            provider="crowdstrike",
            verbose=True,
            raw=True,
        )
```

```
        print(f"Response: {response.result}")
    except pe.PangeaAPIException as e:
        print(f"Request Error: {e.response.summary}")
        for err in e.errors:
            print(f"\t{err.detail} \n")


if __name__ == "__main__":
    main()
```

IP Intel API sends a response

After your app submits an IP to the IP Intel service, you will receive the following JSON response:


```
{
  "request_id": "prq_z4ggu4wcfgga4a3iqx46boptczezgw44",
  "request_time": "2022-12-20T21:32:34.292491Z",
  "response_time": "2022-12-20T21:32:34.351665Z",
  "status": "Success",
  "summary": "IP was found",
  "result": {
    "data": {
      "category": ["Suspicious"],
      "score": 100,
      "verdict": "malicious"
    },
    "parameters": {
      "ip": "93.231.182.110",
      "verbose": true,
      "raw": true,
      "provider": "crowdstrike"
    },
    "raw_data": {
      "indicator": "93.231.182.110",
      "type": "ip_address",
      "deleted": false,
      "published": 1487468233,
      "updated": 1610003010,
      "malware_families": [],
      "kill_chains": [],
      "ip_address_types": [],
```

```
      "domain_types": [],
      "confidence": "unverified",
      "labels": [
        {
          "name": "ThreatType/Suspicious",
          "created_on": 1487468233,
          "last_valid_on": 1597406472
        }
      ],
      "threat_types": ["Suspicious"],
      "vulnerabilities": []
    }
  }
}
```


In this instance, the `verdict` returned as `malicious` . Additional raw data (from the provider specified in the API request) was returned, like:

- `raw_data`
- `parameters`
- `threat_types`
- `vulnerabilities`

These additional fields were returned because `raw` and `verbose` were set to `true` in the original API request.

Understand and review results

The API response sent by IP Intel includes various fields and values; however, the ones listed below give you the most information about the disposition of an IP. To learn about more response fields, visit the IP Intel API Reference.

Based on the IP Intel API response, it's evident that the IP you submitted is **Malicious.**

`verdict`	The verdict normalized categorization as interpreted by the data returned by the third party provider. There are four possible verdicts: • `Benign` - Confirmed as non-malicious • `Suspicious` - Associated with actions that are malicious • `Malicious` - Confirmed as malicious

	• `Unknown` - No data
`score`	The normalized score as interpreted by the data returned by the third party provider. Scores are associated with the verdict values listed above: • `0` = `Benign` • `1` - `99` = `Suspicious` • `100` = `Malicious` • `-1` = `Unknown`
`summary`	A summary of the various categories associated with an IP address, which help illustrate why an IP received a particular verdict.
`category`	Indicates the category associated with the IP address (e.g. Adware, Malware). This field may return more than one category and may, at times, not be populated.
`raw`	Raw data returned by the provider you specified in the API request. You can investigate the raw data if its meaningful to your use case or if you want to supply it to your users. You must set the `raw` field to `true` to receive this data.

Decide what to do with IP

You decide how to respond and/or communicate with your users once an IP's reputation becomes evident. Here are some suggestions:

- Block the IP
- Validate activity from a suspicious client IP using:
  - CAPTCHA
  - Email
  - Multi-factor Authentication (MFA)

In this use case, the IP will be blocked and no message will appear for the user to avoid giving them any hints that may help their potentially fraudulent intentions.