Spur IP Context Application

```
Version:        1.1.0
Release Date:   20220801
```

Changelog

20220801 - Incorporation of Spur's v2 API data

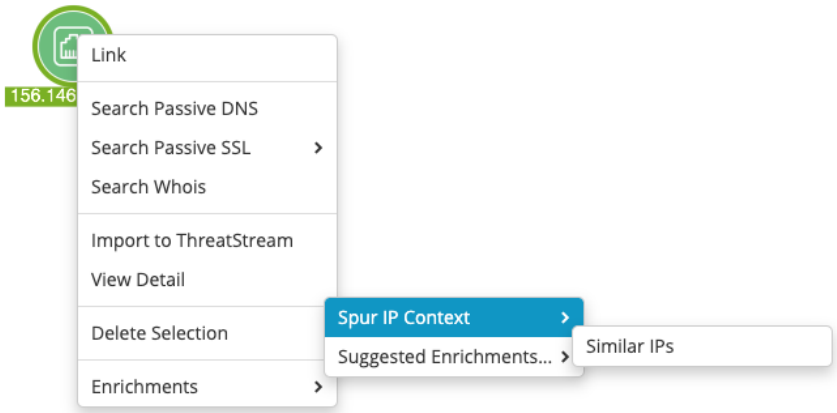
20210714 - Support for Python 3.x

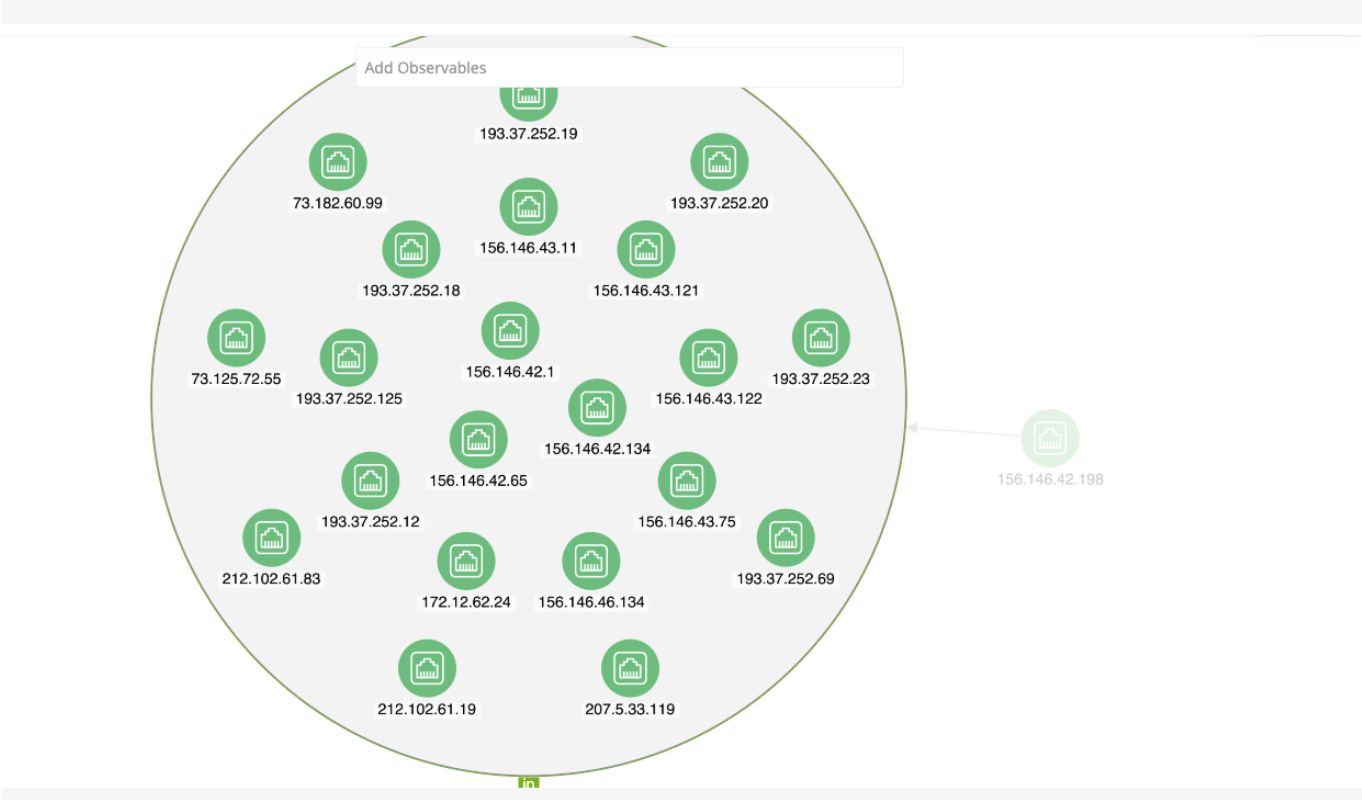
20200804 - Initial release of both Similar IPs Pivot and IP Context Enrichment

Description

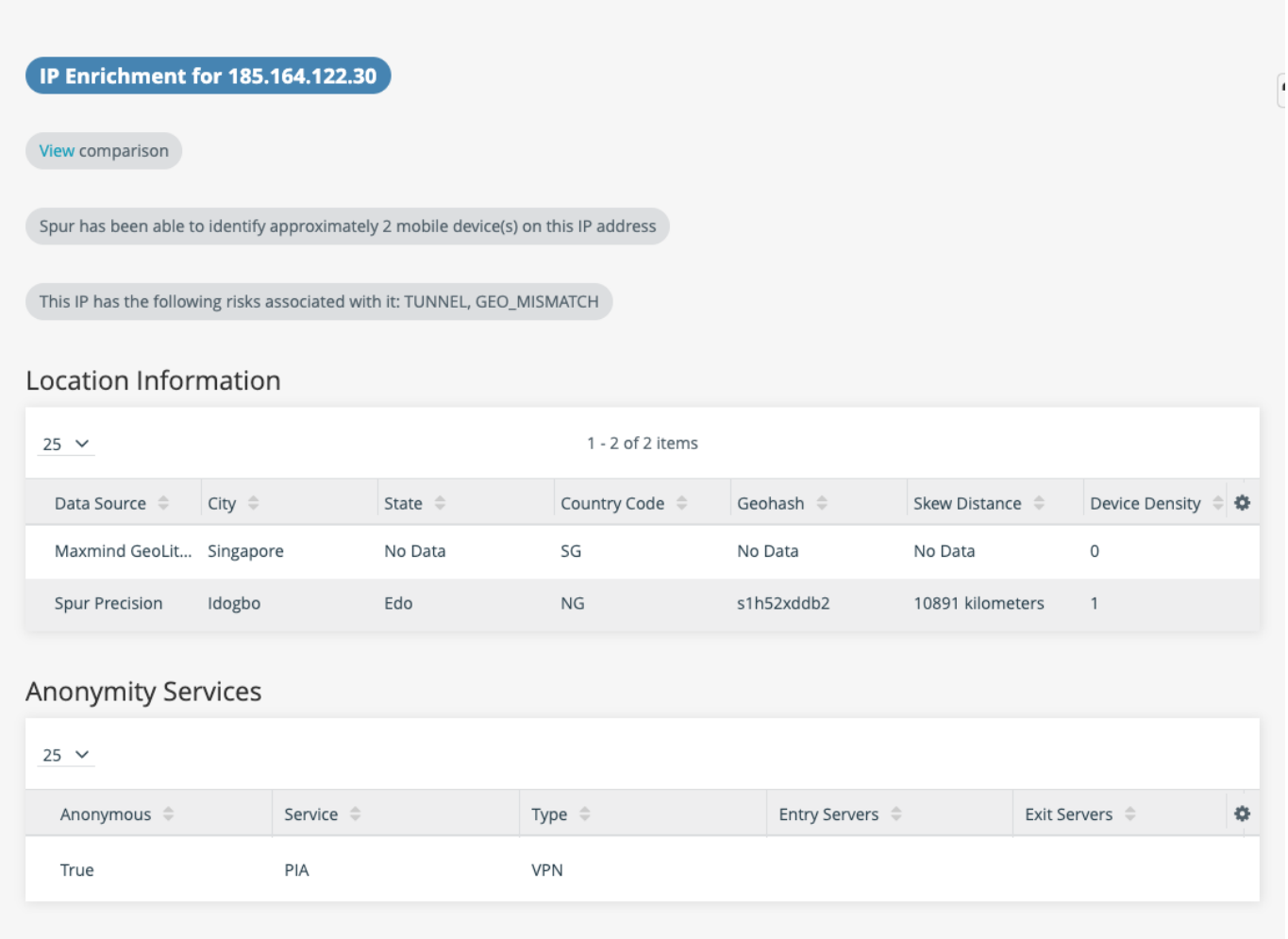
When activated, the Spur IP Context enrichment can provide high-fidelity contextual information on IP addresses. This data includes precision geolocation, SSIDs, anonymity network details, device count, device behaviors, and IPs that are likely similar.

You can leverage Spur's Similar IPs to enumerate infrastructure on the Explore pivoting tool after activation.





The Spur IP Context application also displays enrichment data on the observable details page for IP addresses. For example, the following displays the relevant contextual information for a Private Internet Access VPN. The `Location Information` shows that the IP address is geolocated to Singapore. However, Spur's precision geolocation has identified that the users are primarily in Nigeria. The skew shows the distance in kilometers from the user's location to the datacenter IP address. This discrepancy created the `GEO_MISMATCH` risk. The `Anonymity Services` table shows that `PIA` is active on this IP address.



To learn more about Spur, please visit spur.us

Transformations

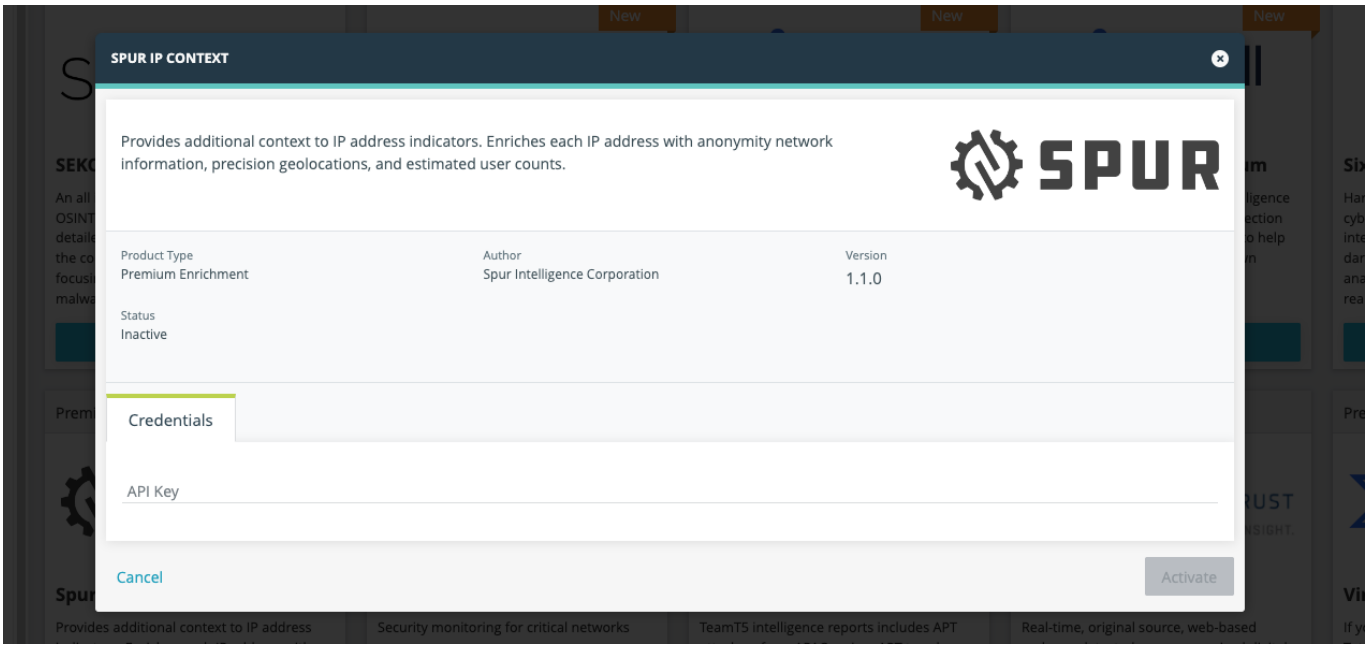
The Spur IP Context application enabled the following data transformations:

- `similarIPs`: Returns IP addresses that have a high confidence of being used by the same devices on the original IP address. For instance, if used on a Private Internet Access VPN exit point, one would be able to enumerate other exit points for PIA.

Setup

1. Log in to the ThreatStream user interface
2. In the top navigation bar, navigate to the APP Store
3. Click `Get Access` button in the `Spur IP Context` box
4. Click `I have credentials` and enter your Spur IP Context API token.

- If you need a token, visit https://spur.us/api and sign-up for an account. Your token will be available in the API portal.



5. Click activate

At this point, the application is active and ready to be used.

Support

For any questions regarding our integration or our data, please contact our support desk at support@spur.us