Location of remote workers

You might need to know where your remote workers are located when doing the following:

- Securing a work-from-home organization

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security analyst
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Authentication data, normalized to the Authentication data Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

Example

Your workforce is fully remote. To ensure network security, you want to report on where your remote workers are located.

To optimize the search shown below, you should specify a time range.

1. Run the following search:

   | tstats count(Authentication.user) FROM datamodel=Authentication WHERE (index=main OR index=firewall) BY Authentication.action Authentication.src
   | rename Authentication.* AS *
   | eval src = if(src=="216.113.183.230","142.252.17.31", if(src=="64.147.162.160","71.193.0.238",if(src=="216.129.122.242","162.245.239.68", src)))
   | iplocation src
   | where len(Country)>0 AND len(City)>0
   | geostats count BY action

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
**Splunk Search**  
| tstats count(Authentication.user) FROM datamodel=Authentication WHERE (index=main OR index=firewall) BY Authentication.action Authentication.src | **Explanation**  
| | Search the main and firewall indexes for authentication actions and group the results by action and source. Set `prestats` to true so the results can be sent to a chart.  
| rename Authentication.* AS * | Rename the field as shown for readability.  
| eval src = if(src=="216.113.183.230","142.252.17.31",if(src=="64.147.162.160","71.193.0.238",if(src=="216.129.122.242","162.245.239.68",src)))) | Convert the IP addresses for the matches shown; otherwise, return the source IP address from the dataset.  
| iplocation src | Extract location information from the IP addresses.  
| where len(Country)>0 AND len(City)>0 | Filter results to those where the values in the country and city fields are greater than one character.  
| geostats count BY action | Create a map that shows a count of authentication events.  

**Result**

This search produces a map of your users' locations and statistics about how many logins come in from each location. Correlate this information with the results of other searches to determine what is normal or anomalous activity on your network.