Getting Started with Maps

Robb Bittner

Michael Porath

Product Managers, Splunk

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Intro

- **Robb Bittner**
- Product Manager: Splunk Light
- Map Geek

- **Michael Porath**
- Product Manager: Visualization and Analysis
- Visualization Nerd

A Splunk instance walks into a bar…

Format Timeline ∨ — Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

List ∨ Format ∨ 20 Per Page ∨ < Prev 1 2 3 4 5 6 7 8 9 10 Next >

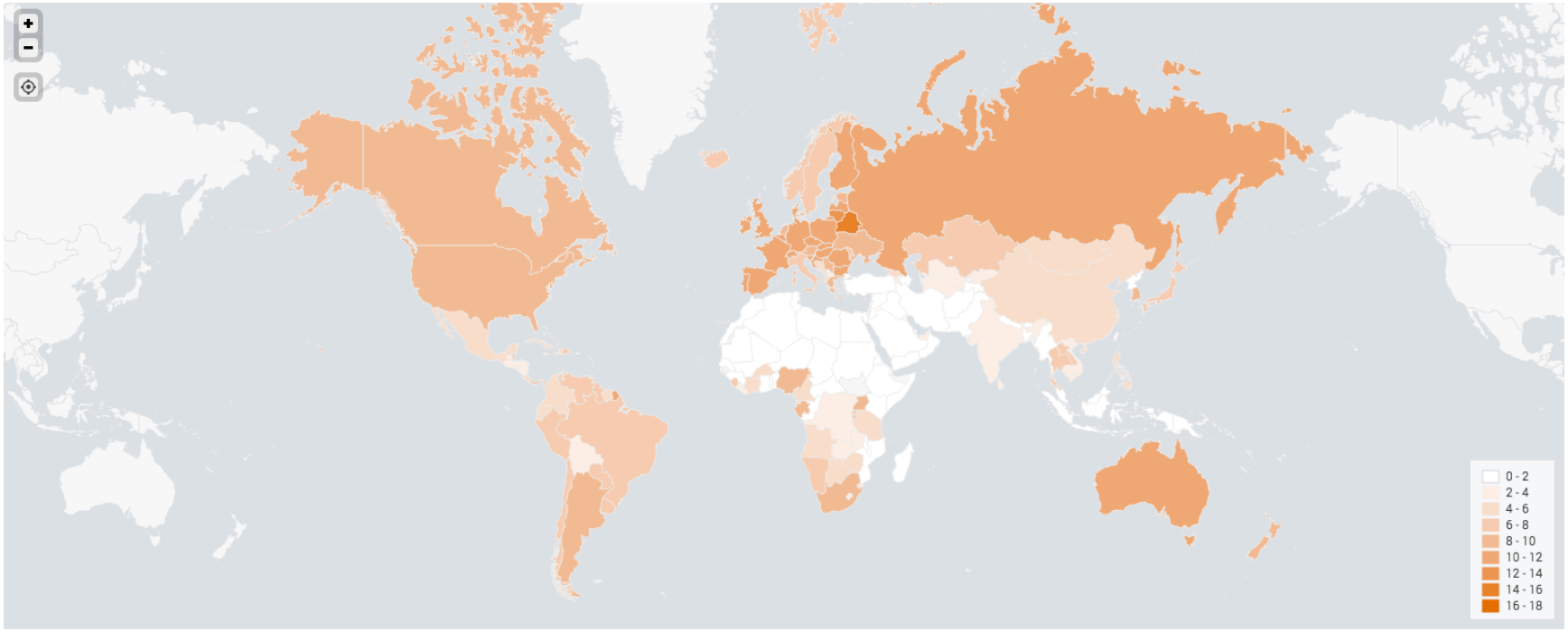
< Hide Fields All Fields

Selected Fields
a host 1
a source 1
a sourcetype 1

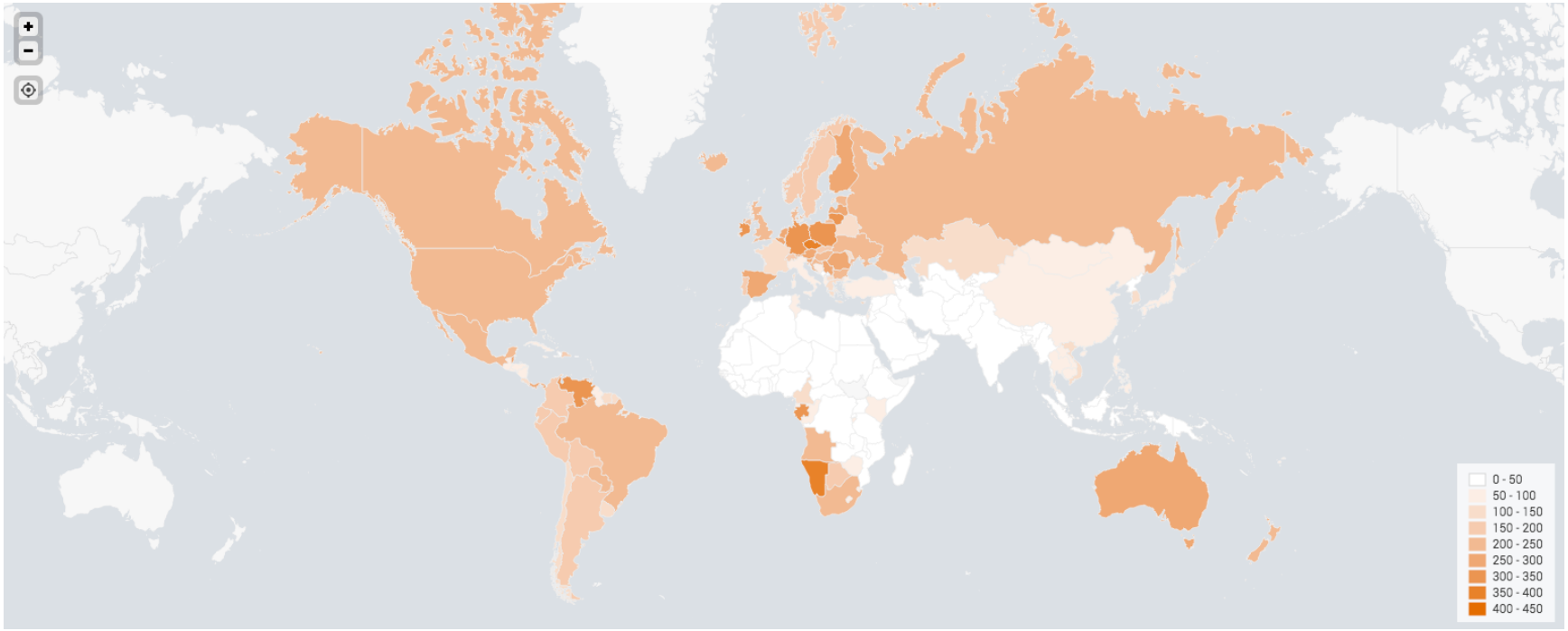
Interesting Fields
beer_servings 100+
a country 100+
a index 1
linecount 1
a punct 12
spirit_servings 100+
a splunk_server 1

i	Time	Event
>	9/8/15 3:28:28.000 PM	9/8/15 0:00,Zimbabwe,64,18,4,4.7 host = rbittner-mbpr.sv.splunk.com source = Drinking.csv sourcetype = csv
>	9/8/15 3:28:28.000 PM	9/8/15 0:00,Zambia,32,19,4,2.5 host = rbittner-mbpr.sv.splunk.com source = Drinking.csv sourcetype = csv
>	9/8/15 3:28:28.000 PM	9/8/15 0:00,Yemen,6,0,0,0.1 host = rbittner-mbpr.sv.splunk.com source = Drinking.csv sourcetype = csv
>	9/8/15 3:28:28.000 PM	9/8/15 0:00,Vietnam,111,2,1,2 host = rbittner-mbpr.sv.splunk.com source = Drinking.csv sourcetype = csv
>	9/8/15 3:28:28.000 PM	9/8/15 0:00,Venezuela,333,100,3,7.7 host = rbittner-mbpr.sv.splunk.com source = Drinking.csv sourcetype = csv
>	9/8/15 3:28:28.000 PM	9/8/15 0:00,Vanuatu,21,18,11,0.9 host = rbittner-mbpr.sv.splunk.com source = Drinking.csv sourcetype = csv
>	9/8/15	9/8/15 0:00,Uzbekistan,25,101,8,2.4

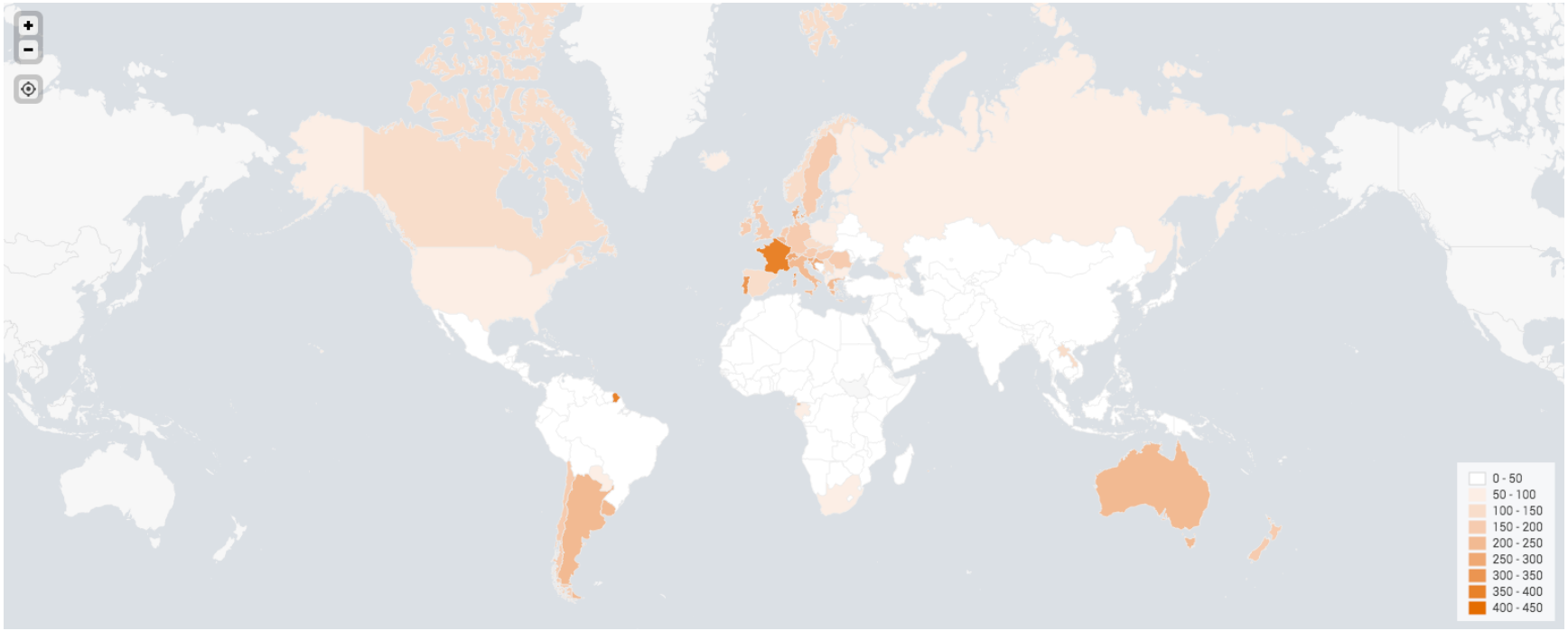
Liters of pure alcohol per capita



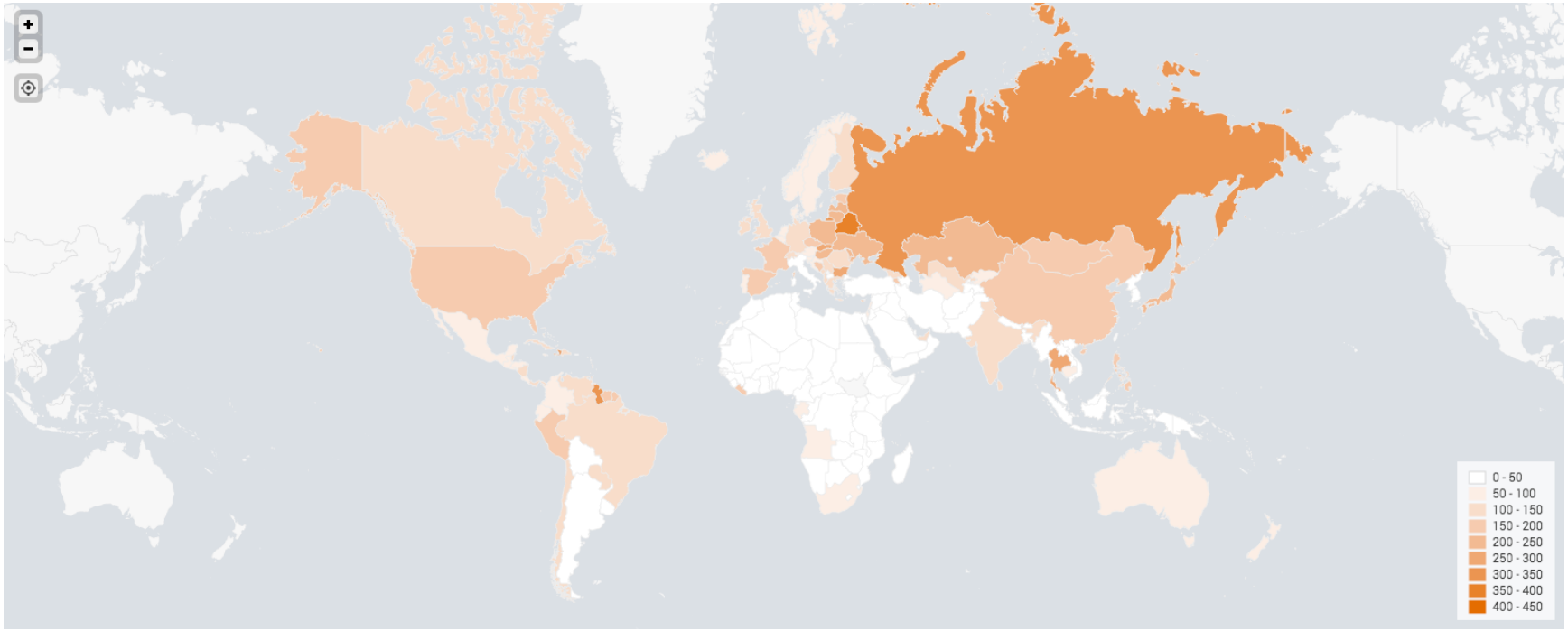
of Beer Servings per year



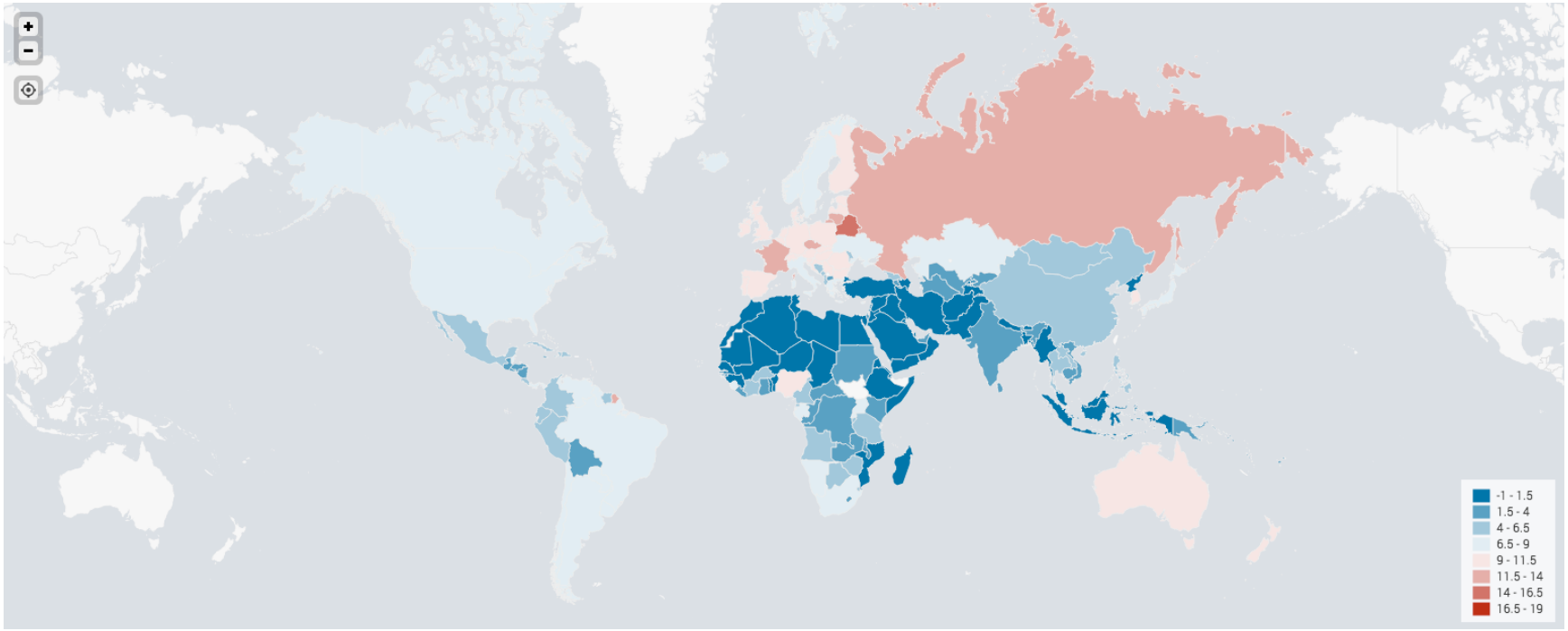
of Wine Servings per year



of Spirit Servings per year

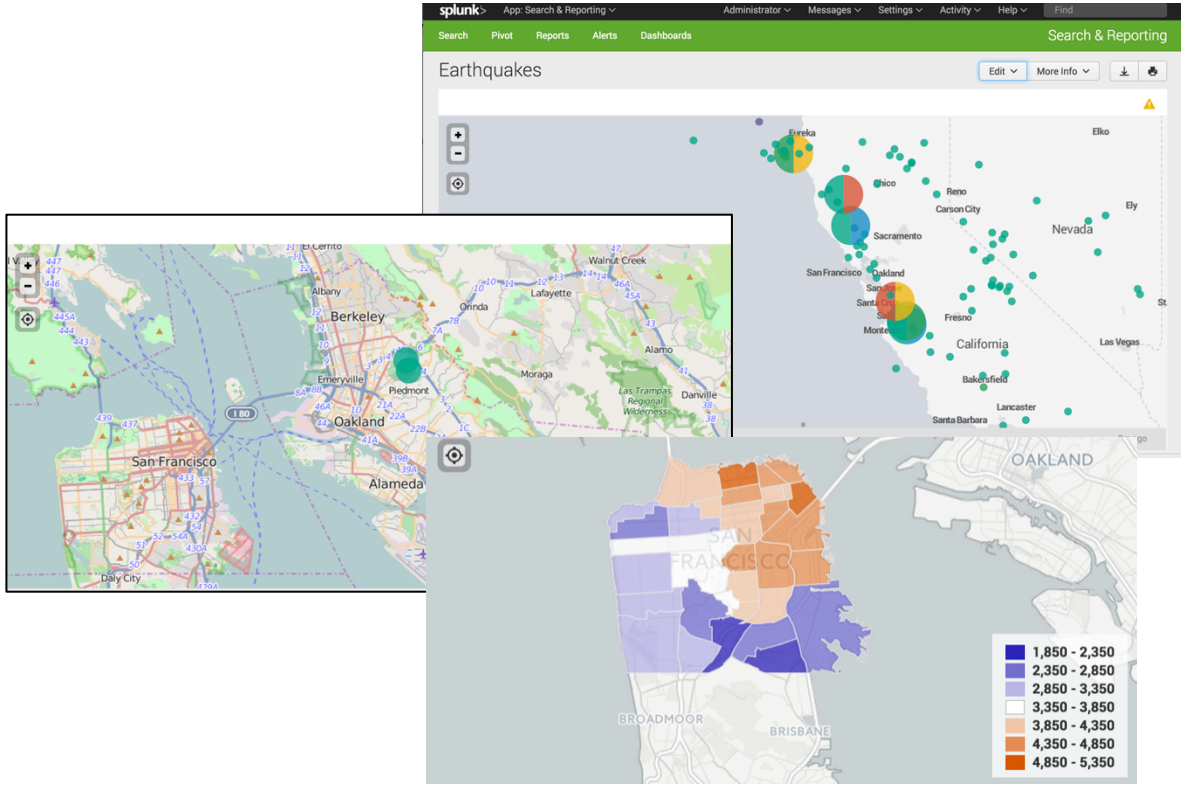


More or less than recommended?

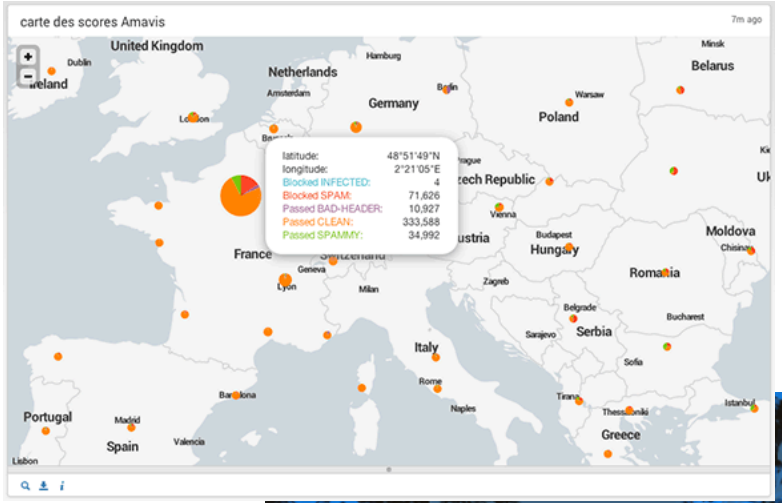


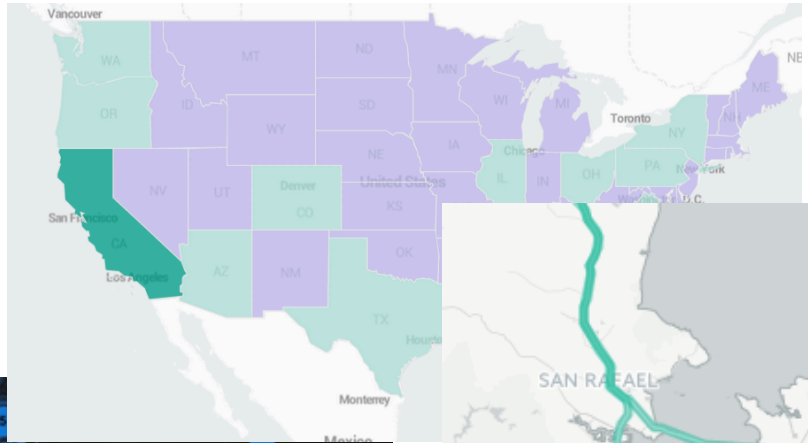
Mapping is easy (really)

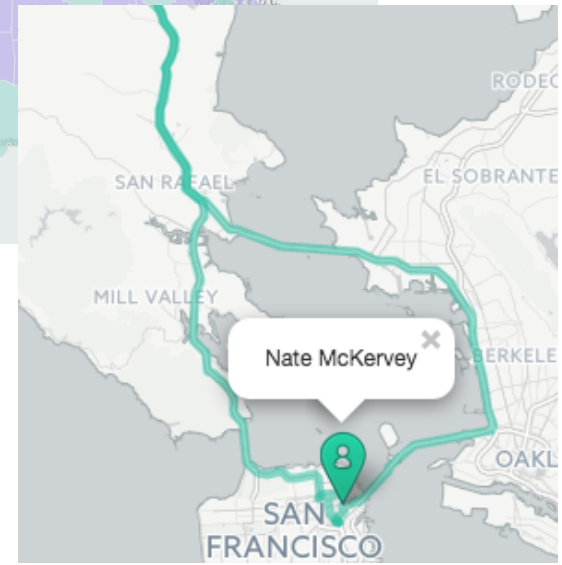
- **DEMO**
- Marker Map
  - Existing Lat/Lon
  - Generated Lat/Lon
- Choropleth
  - Lookup based
  - Aggregation based
- Styling



Mapping Gallery







Elements of Mapping

splunk>

Elements of mapping

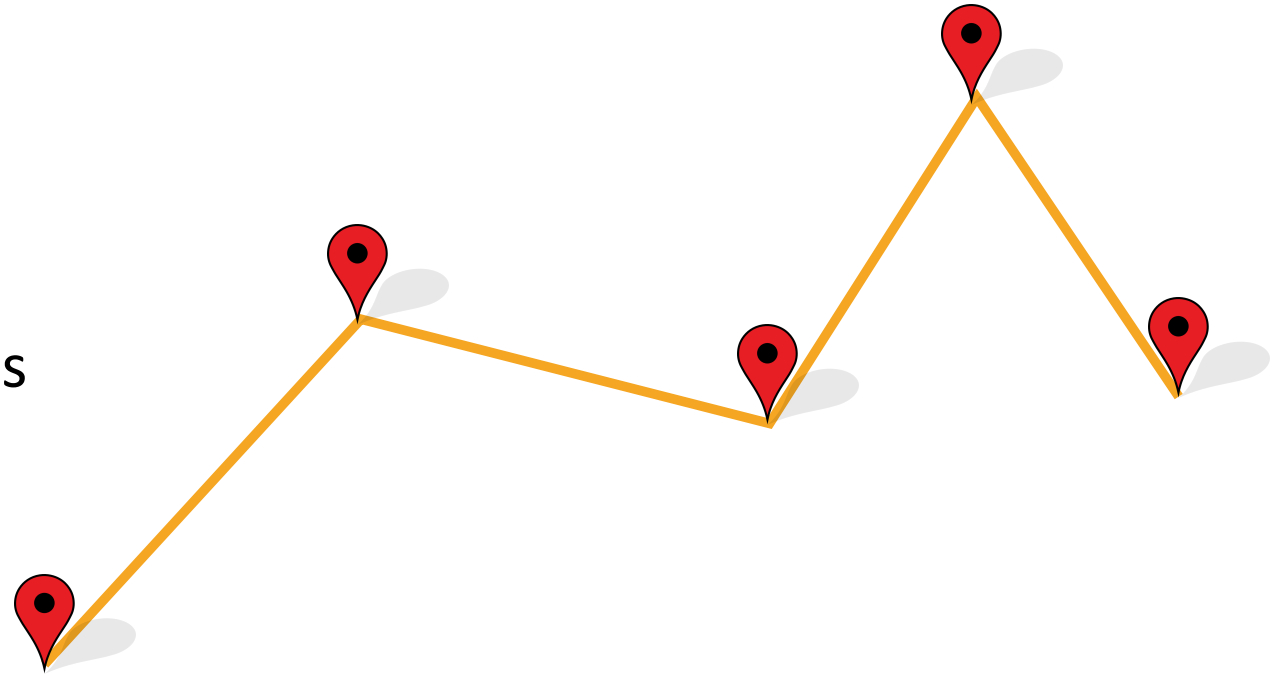
Point

Las Vegas
Longitude: 36.1215° N
Latitude: 115.1739° W

Elements of mapping

Lines

Path
Sequence in Time
Crossing boundaries



Elements of mapping

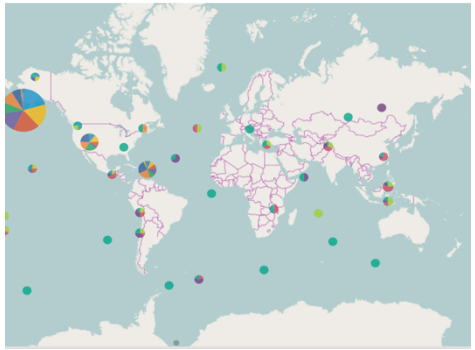
Polygons

Inside/Outside
Entering/Leaving
Lingering
Summarize

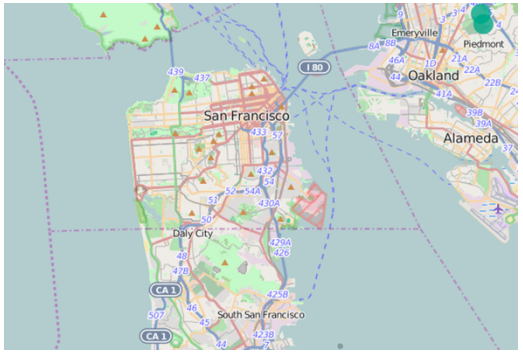
Elements of mapping

Zoom level

1 = World



10 = City



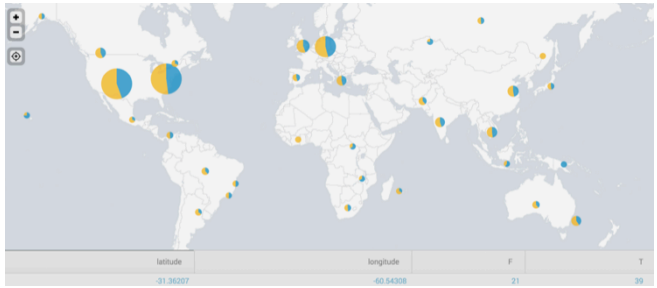
19 = House

Mapping in Splunk

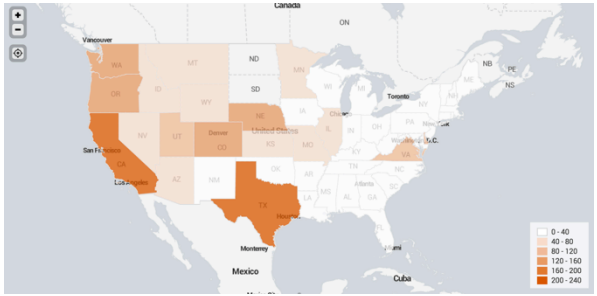
splunk>

What you need to build a map?

Marker Map



Choropleth Map

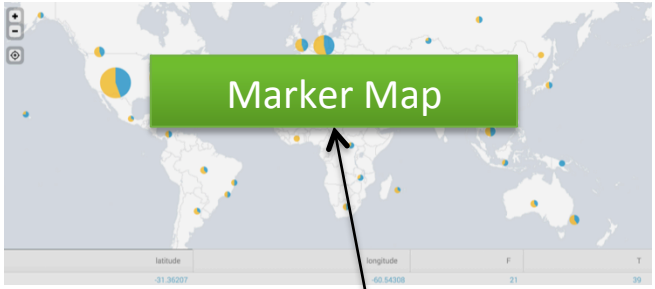


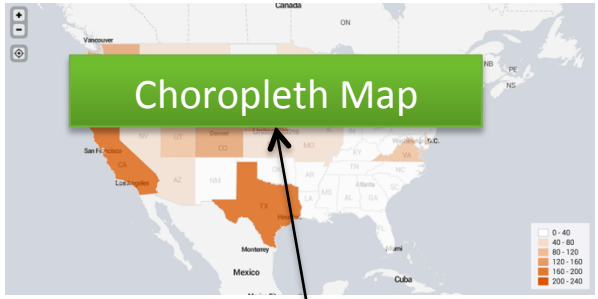
Event that contains latitude and longitude

or

Country / State / Polygon name

Making Data Mappable





Lat/Lon

Polygon

Street Address

ZIP+4

IP Address

Cell Tower

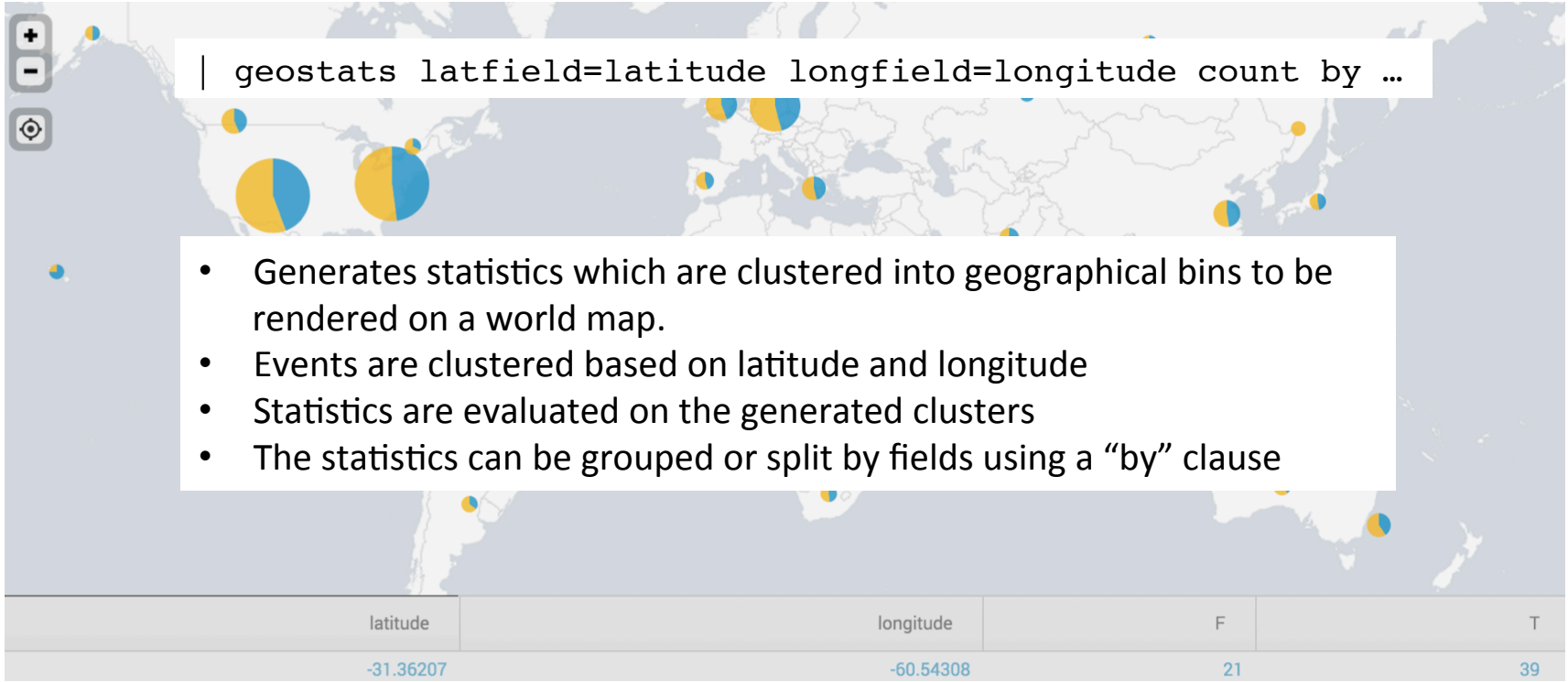
GPS

FIPS

Name

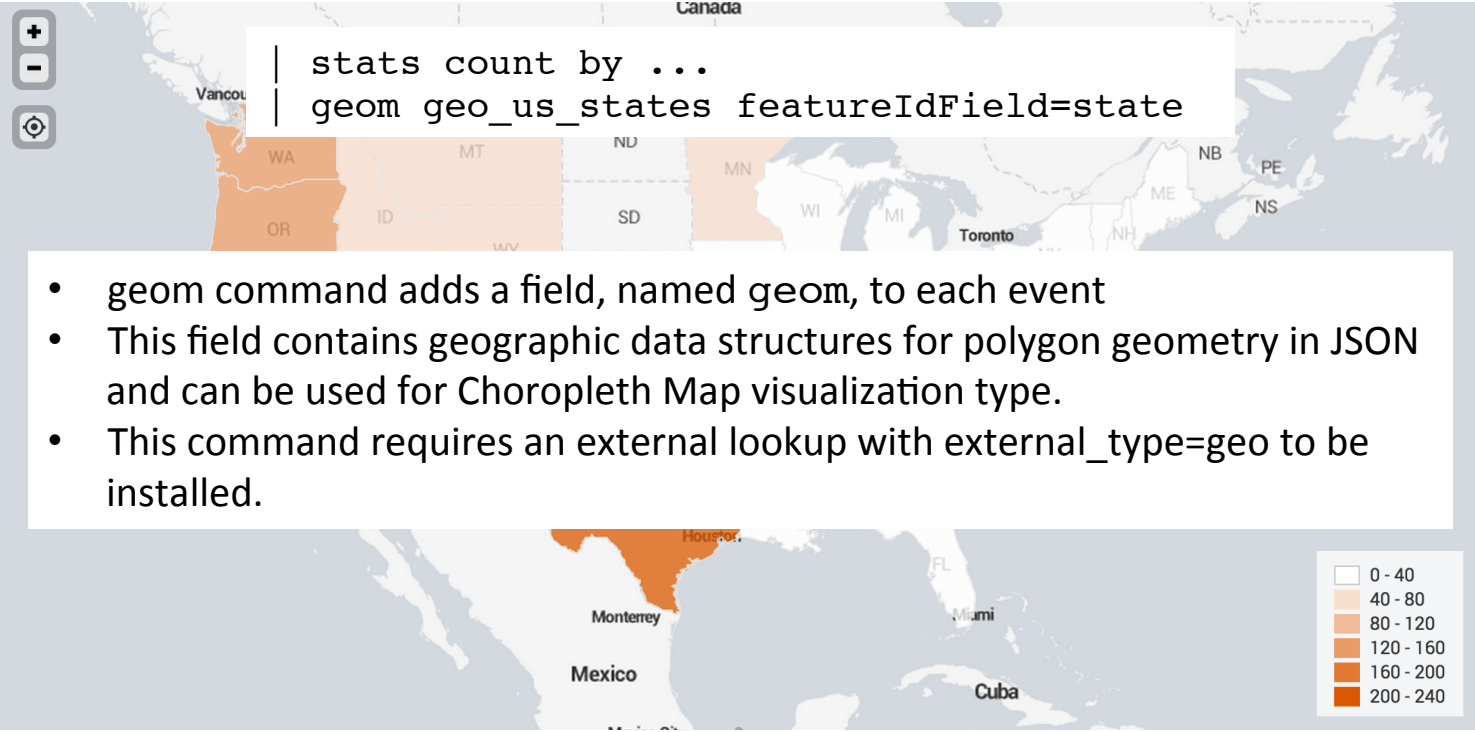
Code

Aggregation: Clusters



- Generates statistics which are clustered into geographical bins to be rendered on a world map.
- Events are clustered based on latitude and longitude
- Statistics are evaluated on the generated clusters
- The statistics can be grouped or split by fields using a “by” clause

Aggregation: Polygons



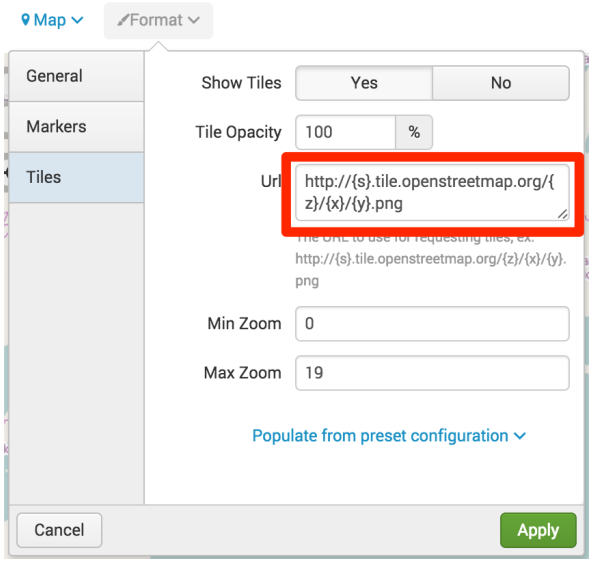
- geom command adds a field, named `geom`, to each event
- This field contains geographic data structures for polygon geometry in JSON and can be used for Choropleth Map visualization type.
- This command requires an external lookup with external_type=geo to be installed.

Tiles

Splunk Tiles
Packaged with every Splunk version
Offline usage OK
Zoom Levels 1-7
Muted Colors. Perfect for Data Overlays.

Open Street Map
Packaged with every Splunk version
Only online
Zoom Levels 1-19

Tiles: Alternatives



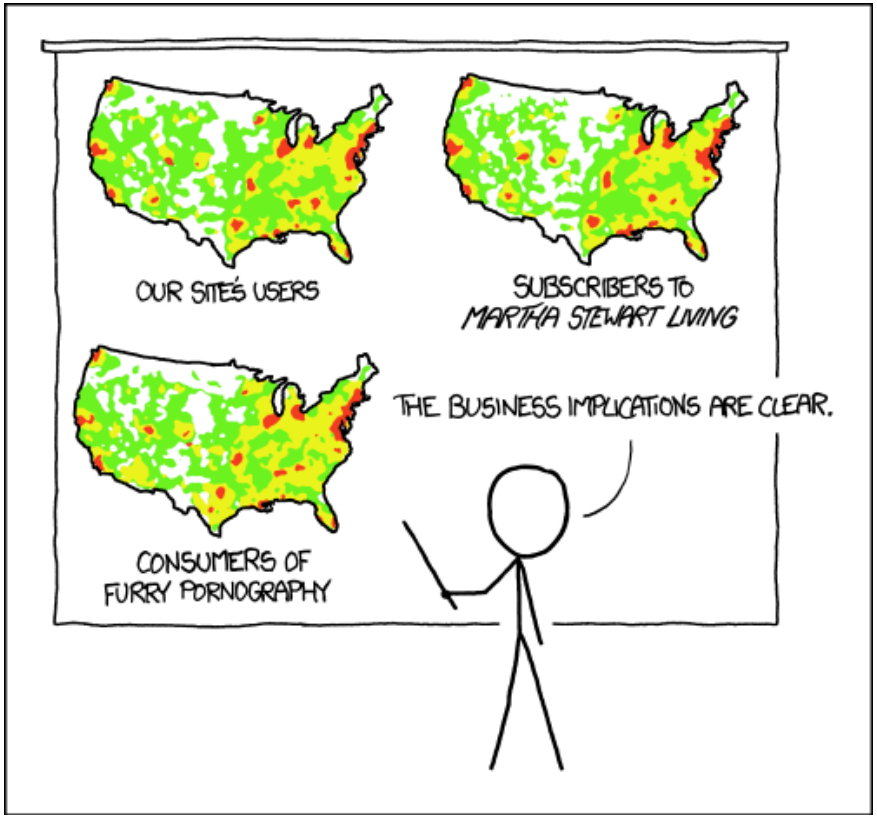
List of tile providers
http://leaflet-extras.github.io/leaflet-providers/preview/


PAY
ATTENTION

Interpretation

Is this really only Germany?

Normalize



PET PEEVE #208:
GEOGRAPHIC PROFILE MAPS WHICH ARE BASICALLY JUST POPULATION MAPS

Source: xkcd.com

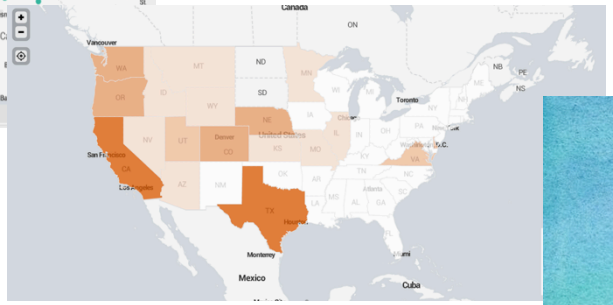
If possible, normalize!

- By population / user density
- By percent of a baseline
- Compared to a previous point in time

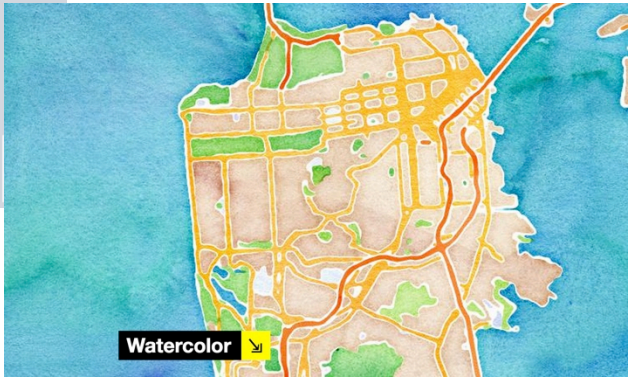
Recap!

Mapping is easy and useful

New: Choropleth Maps



Use Custom Tiles



Q&A

splunk>

Wrap up

- Coming up in this room
  Paint by Number: New Visualizations in Splunk 6.3

- Resources:
  - **Tile providers:** http://leaflet-extras.github.io/leaflet-providers/preview/
  - **Marker Maps Docs:** http://docs.splunk.com/Documentation/Splunk/6.3.0/SearchReference/Geostats
  - **Choropleth Docs:** http://docs.splunk.com/Documentation/Splunk/6.3.0/Viz/Choroplethmaps

THANK YOU

splunk>