Paint By Number: What's New in Visualization

Michael Porath

Product Manager, Splunk

Geoffrey Hendrey

Architect, Splunk

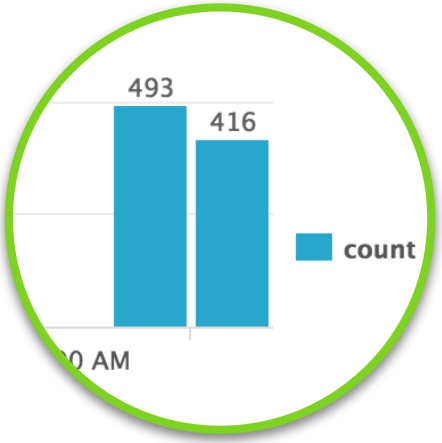
splunk>

Disclaimer

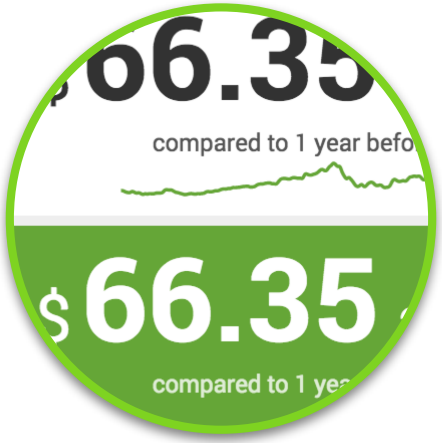
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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.

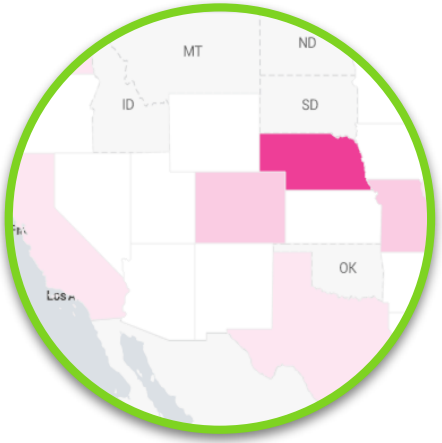
You Asked — We Listened



Improvements
towards
Better Data Analysis



Improved
Dashboard
Visualizations



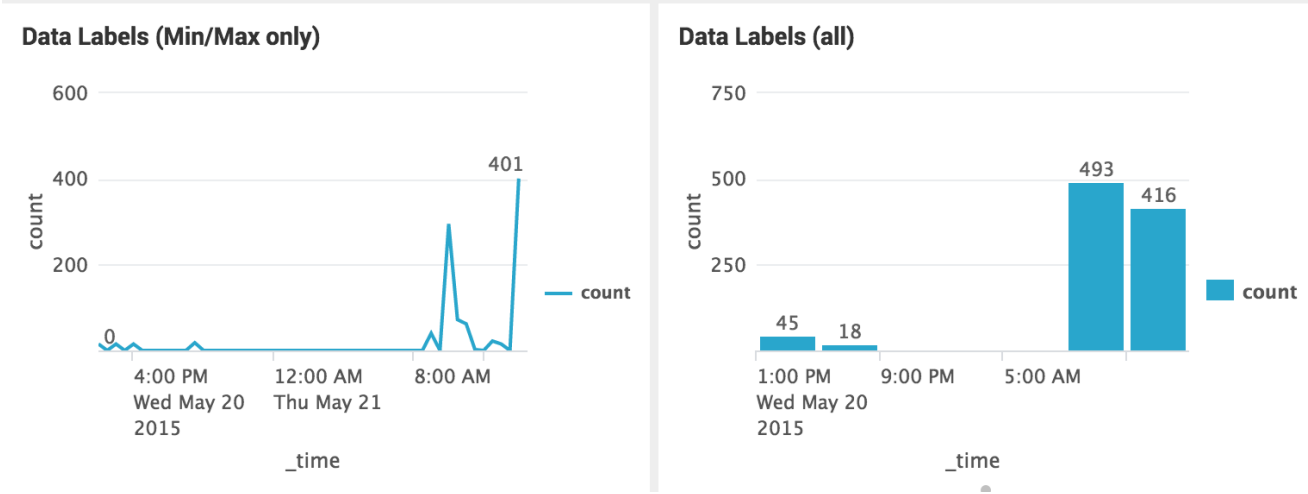
New Geo
Visualization Type

Visualization Improvements

splunk>

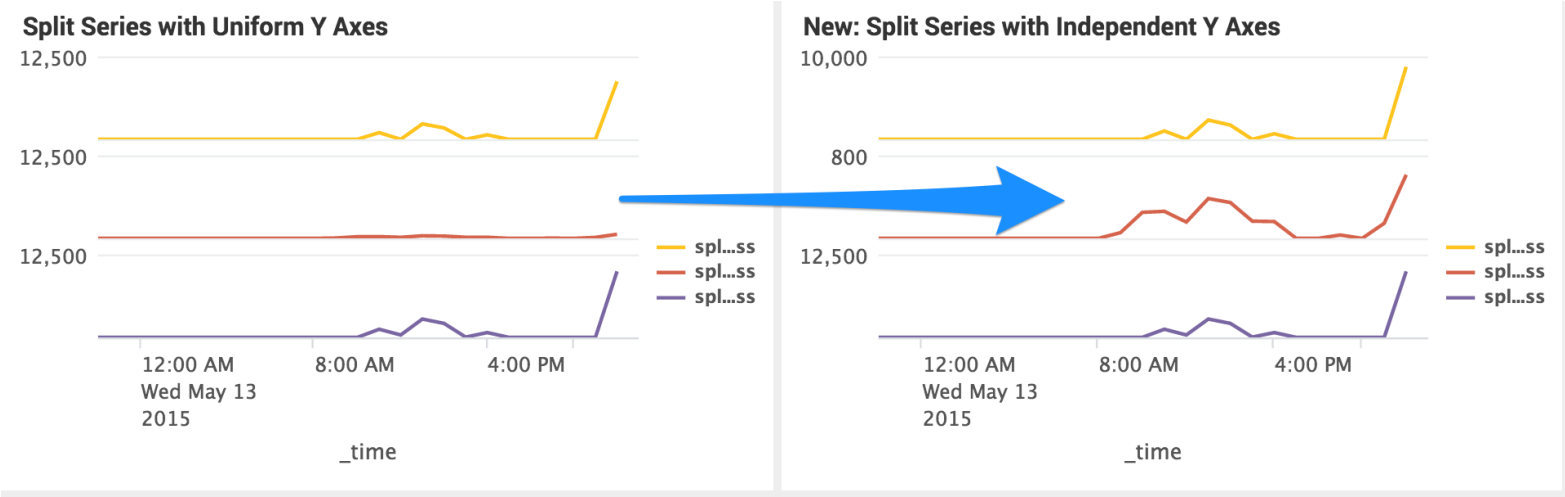
Data Labels

- Labels individual data points
- Min/Max points only, or all points



Independent Axes

- Split Series can now have their independent Y Axes
- Helps compare spikes and trends across series



Single Value Visualization

splunk>

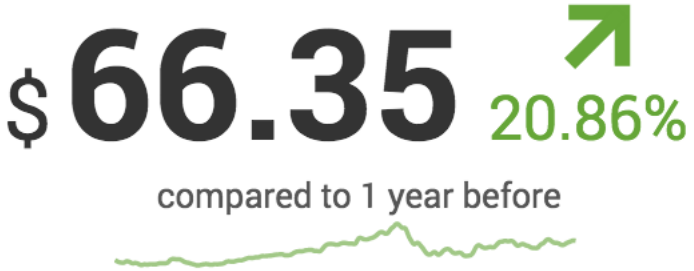
Dashboards are Far Away

Single Value

Completely Redesigned

Existing

New



Single Value

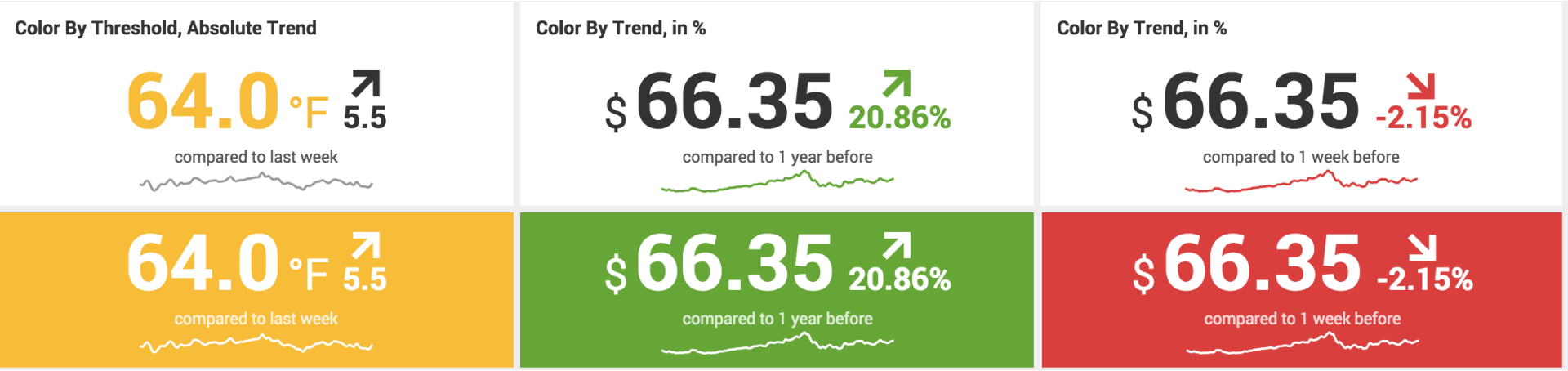
Small Space, High Information Density


```
… | timechart max(value) span=1w
```

No JS coding / CSS styling necessary!

Single Value

Color Modes



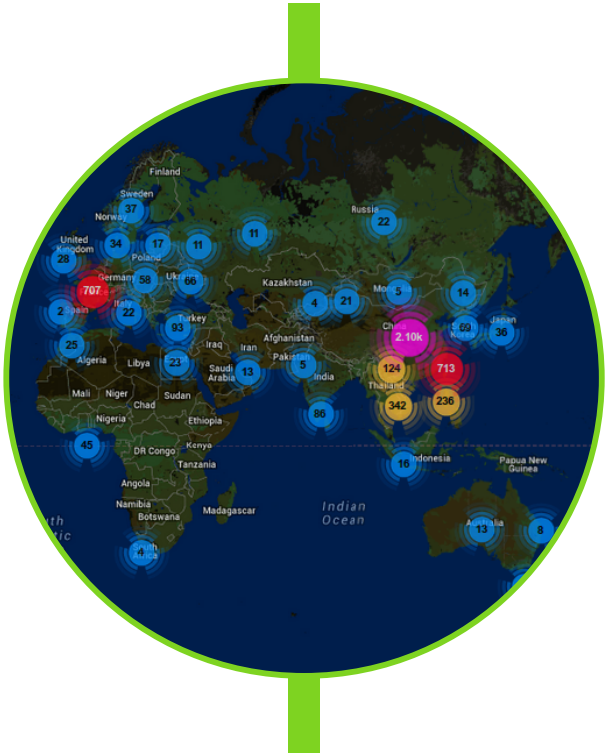
Value Range Map,
custom thresholds

Trend up/down,
Can be inversed

Geospatial Analysis And Visualization

splunk>

Maps in Splunk

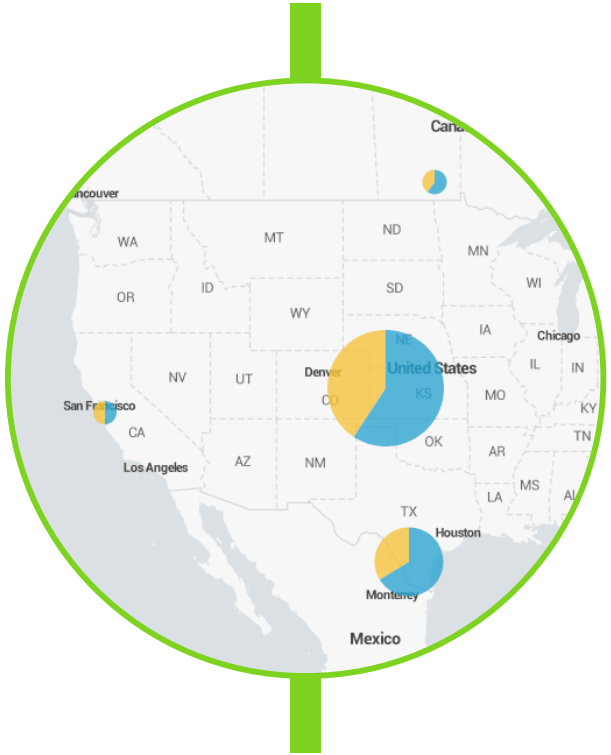


Pre Splunk Enterprise 6.0

Community Supported Apps

E.g. Google Maps add-on

Maps in Splunk



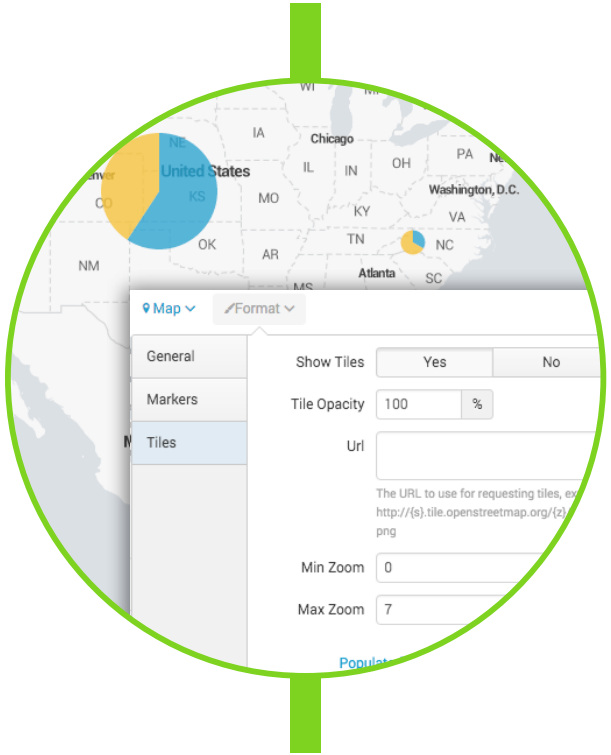
Splunk Enterprise 6.0

Cluster Maps

Splunk Tiles

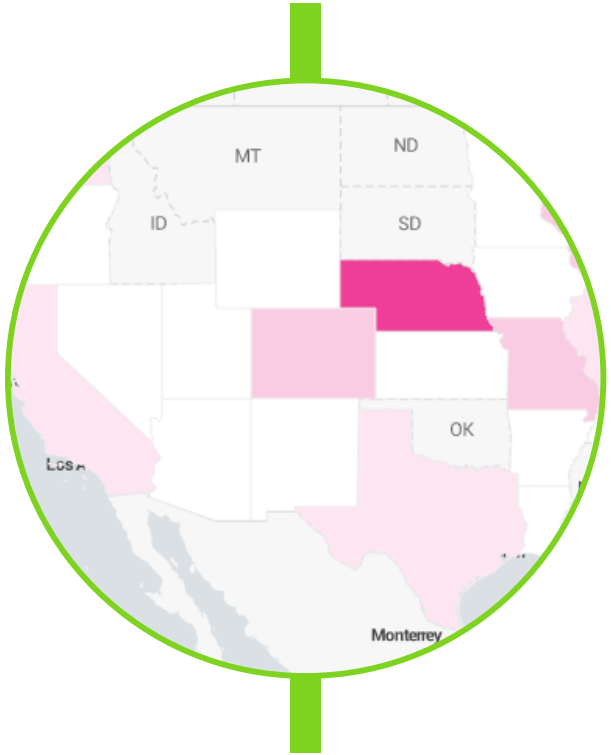
| geostats

Maps in Splunk



Splunk Enterprise 6.1
UI integration
Format Editor

Maps in Splunk

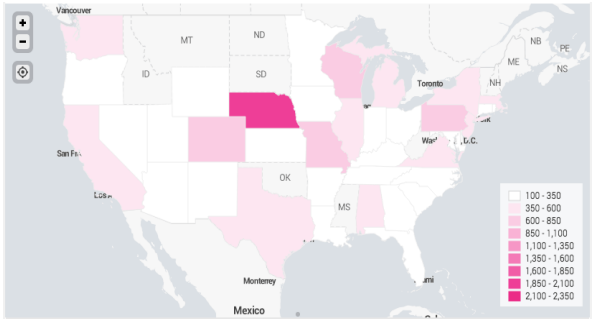


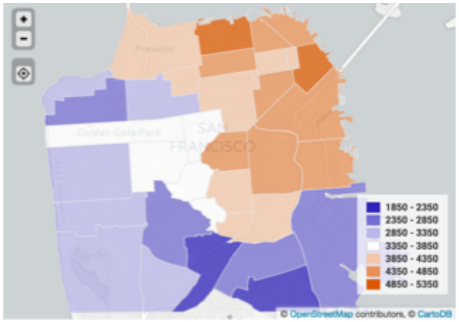
Splunk Enterprise 6.3

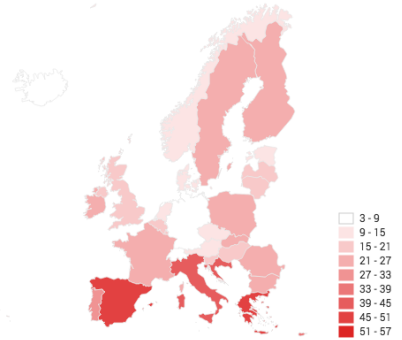
?

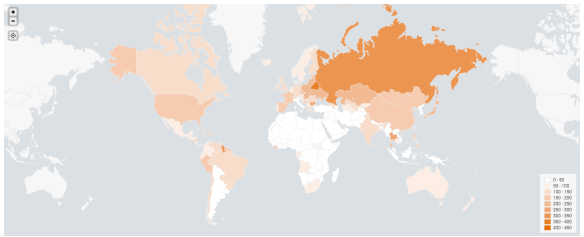
Choropleth Maps

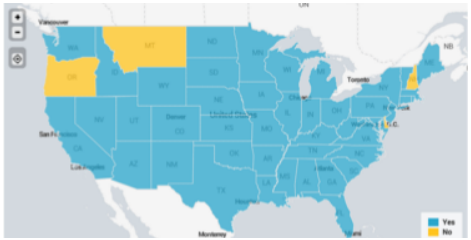
Newest member of the visualization family in 6.3









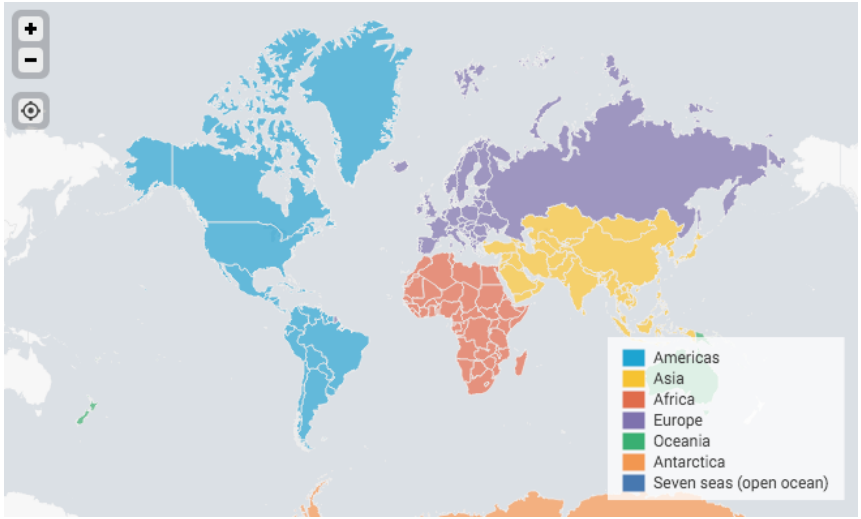


What is a Choropleth?

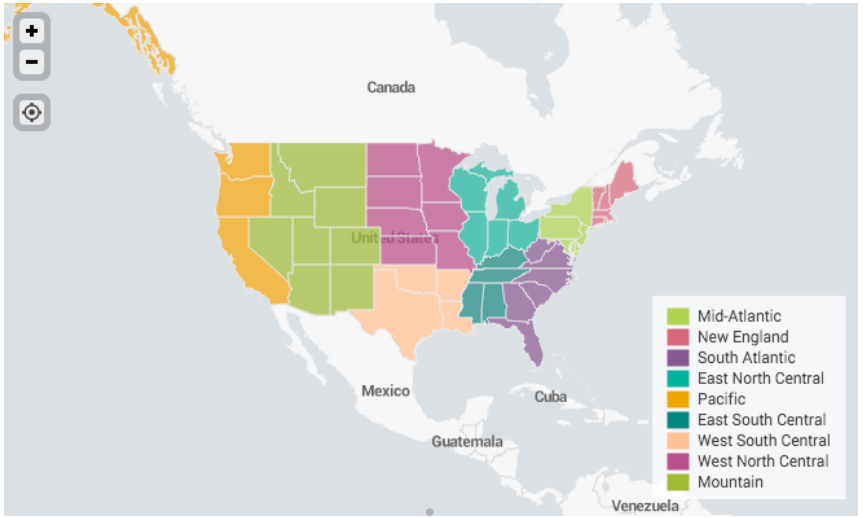
- ***Choropleth*** **-** from Greek: “a multitude of regions”
- A thematic map with areas shaded in proportion to the measurement of a variable
- Visualizes how a measurement varies by geographic region

Built-in, Ready to Use

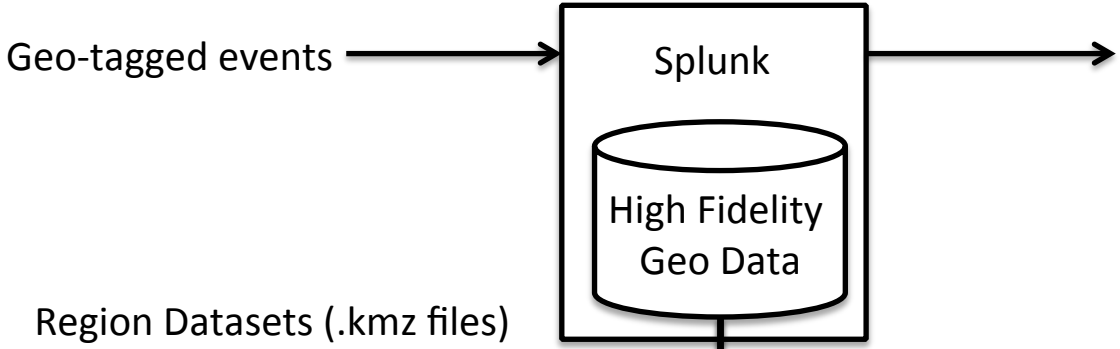
Countries of the world

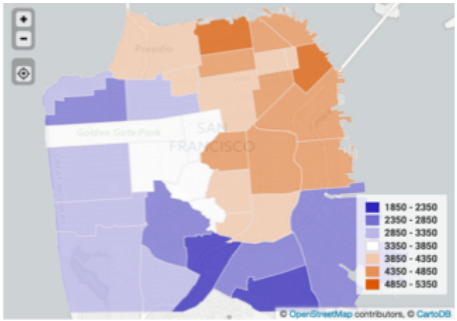


50 States of US + DC



Use Publically Available Region-data





NOAA

Current Severe Weather Zones

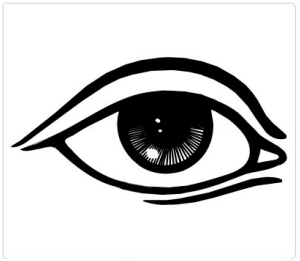
United States™ Census Bureau

State, county, city, congressional boundaries

Neighborhoods, building footprints

Match Events to Complex Shapes in Real-time

- Which polygon contains `37.7792523,-122.4194366`?
- A human eye can easily answer this
- For software the “Point in polygon” problem is harder



- Every event must be checked against every polygon

Relevant SPL Commands

`lookup`	Use the **`lookup`** command to match a polygon to a latitude and longitude coordinate
`stats`	Use **`stats`** commands to create per-polygon aggregates
`geom`	Use **`geom`** command to render polygons on a map

Geospatial Lookup

1. Lookup features (= polygons)

lat	lon	amount
37.7833	**-122.4167**	**46.00**
36.9719	-122.0264	89.25
36.1215	-115.1739	52.50

```
lookup geo_us_states
    latitude as lat
    longitude as lon
```

lat	lon	amount	featureId
37.7833	**-122.4167**	**46.00**	California
37.7814	-122.0264	89.25	California
36.1215	-115.1739	52.50	Nevada

The **name** of the surrounding polygon is attached to your event in the `featureId` field

Geospatial Lookup

2. Aggregate across features

lat	lon	amount	featureId
37.7833	**-122.4167**	**46.00**	California
37.7814	-122.0264	89.25	California
36.1215	-115.1739	52.50	Nevada

```
stats sum(amount)
  as amountTotal
    by featureId
```

featureId	amountTotal
California	135.25
Nevada	52.50

Geospatial Lookup

3. Visualize on a map

featureId	amountTotal
California	135.25
Nevada	52.50

```
geom geo_us_states
```

End-to-End Example

```
…
| lookup geo_us_states
    latitude as lat
    longitude as lon
| stats count by featureId
| geom geo_us_states
```

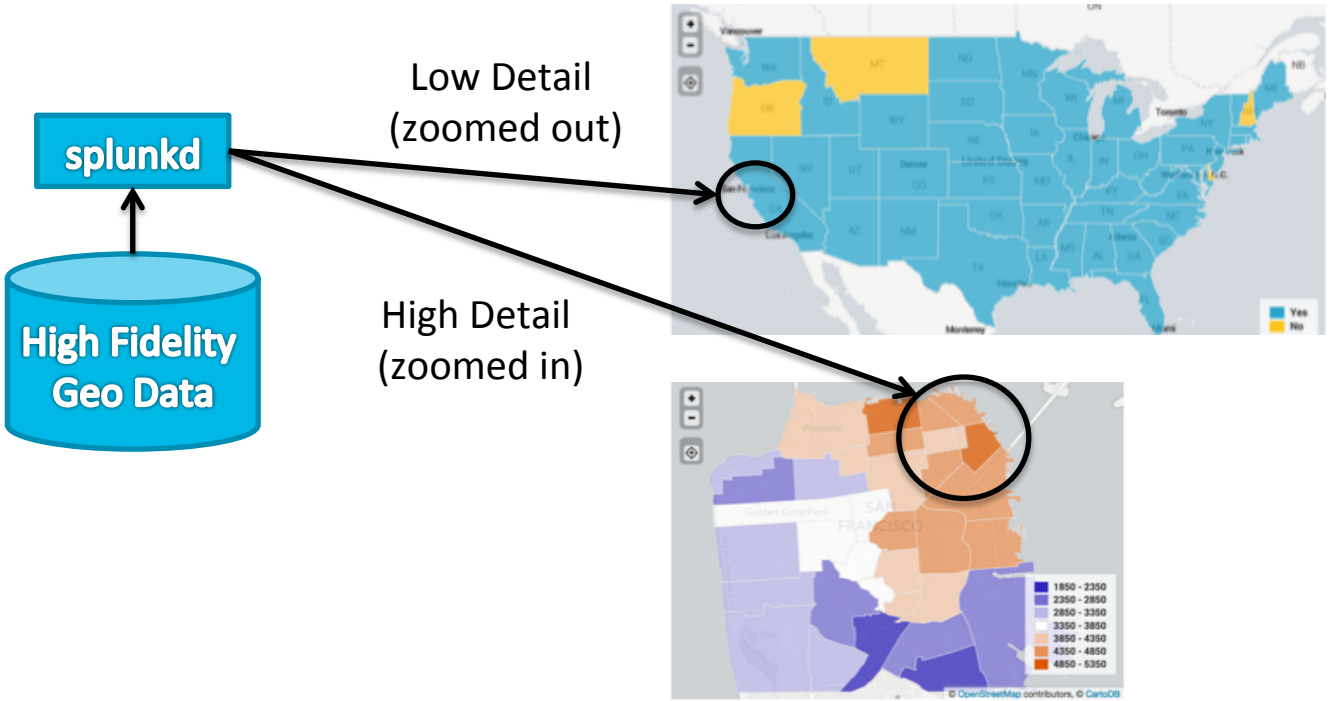
1. Lookup features (= polygons)

2. Aggregate across features

3. Visualize on a map

Rendering Polygons

Always as much detail as needed, never more



Demo

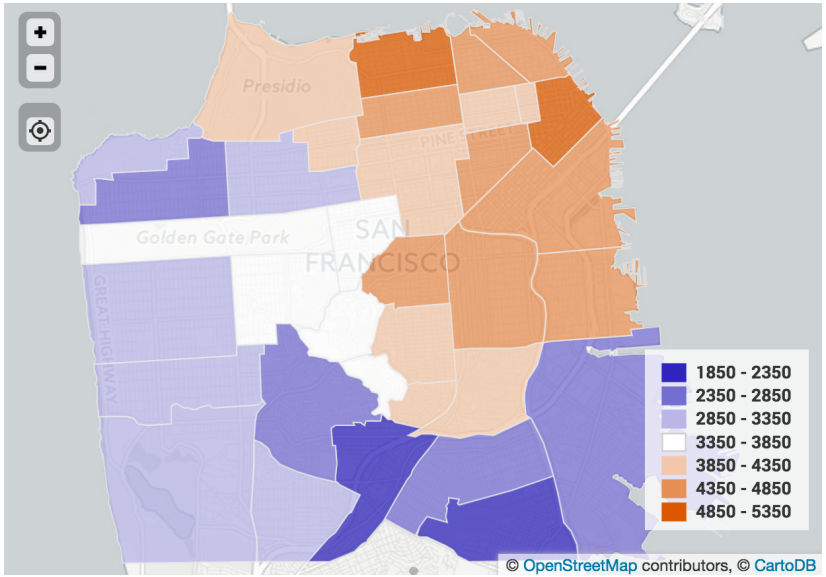
splunk>

Review: Creating a Geospatial Lookup Index

- Pick a KMZ (zipped KML) containing polygons
- Optional: Use Google Earth to view/verify the boundaries
- Setup lookup via UI / in the cloud
  - Upload .kmz file via lookup UI
  - Setup lookup definition with lookup type “Geospatial”
- Setup lookup manually
  - Move .kmz to `lookup` directory
  - Set `external_type=geo` in `transforms.conf`
- Splunk creates an efficient geo-index replicated across indexers

Choropleth Maps

Use Cases



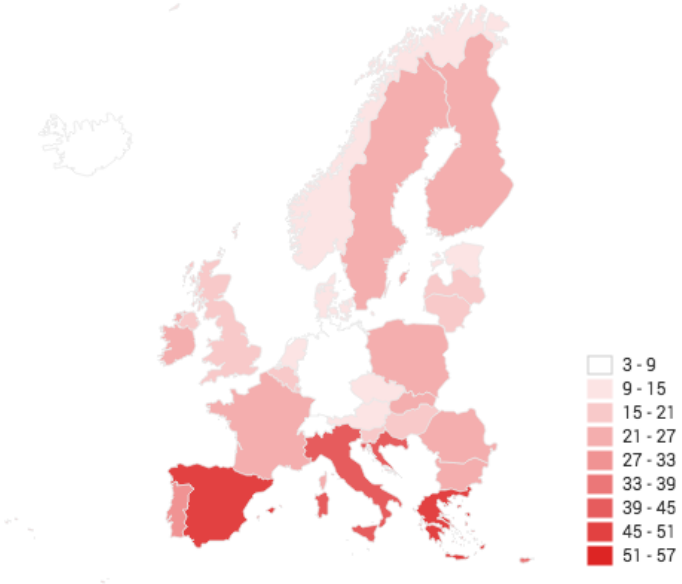
Supports any KMZ file with Polygons

Examples:

- Sales Regions
- Campus Maps
- Districts
- ZIP codes
- Census Tracts
- Geofencing areas

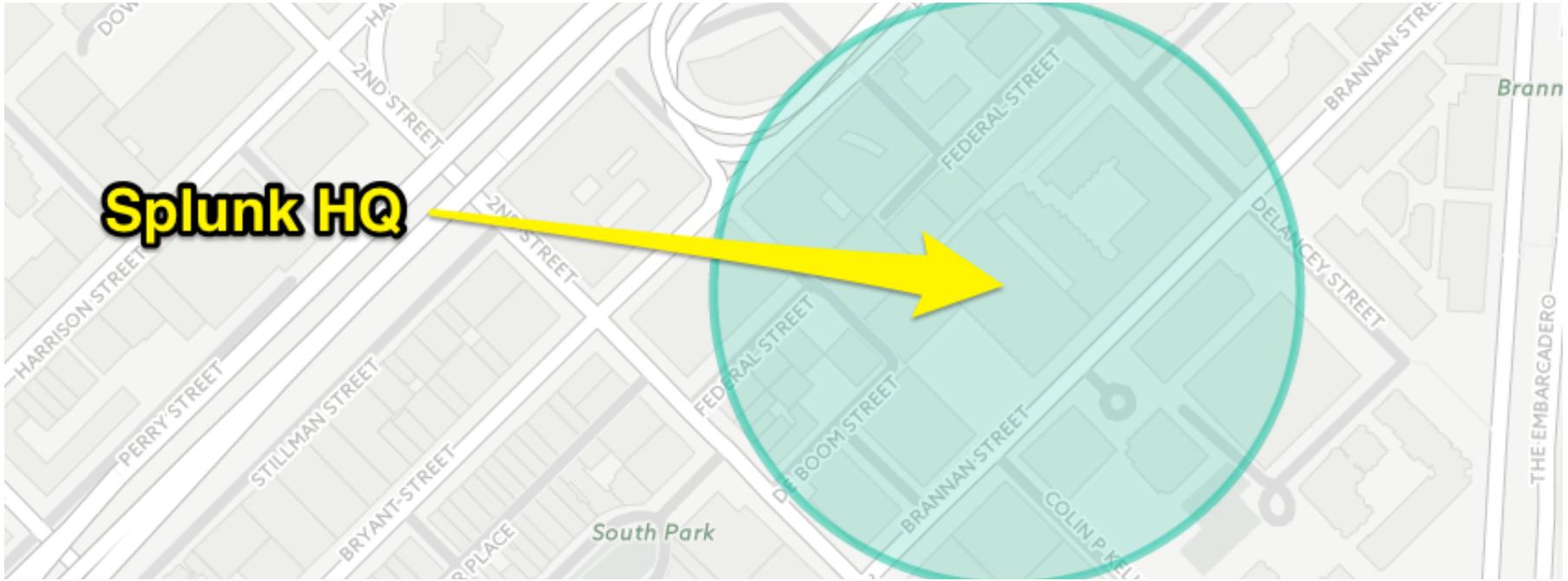
Use Cases

Geospatial Analytics



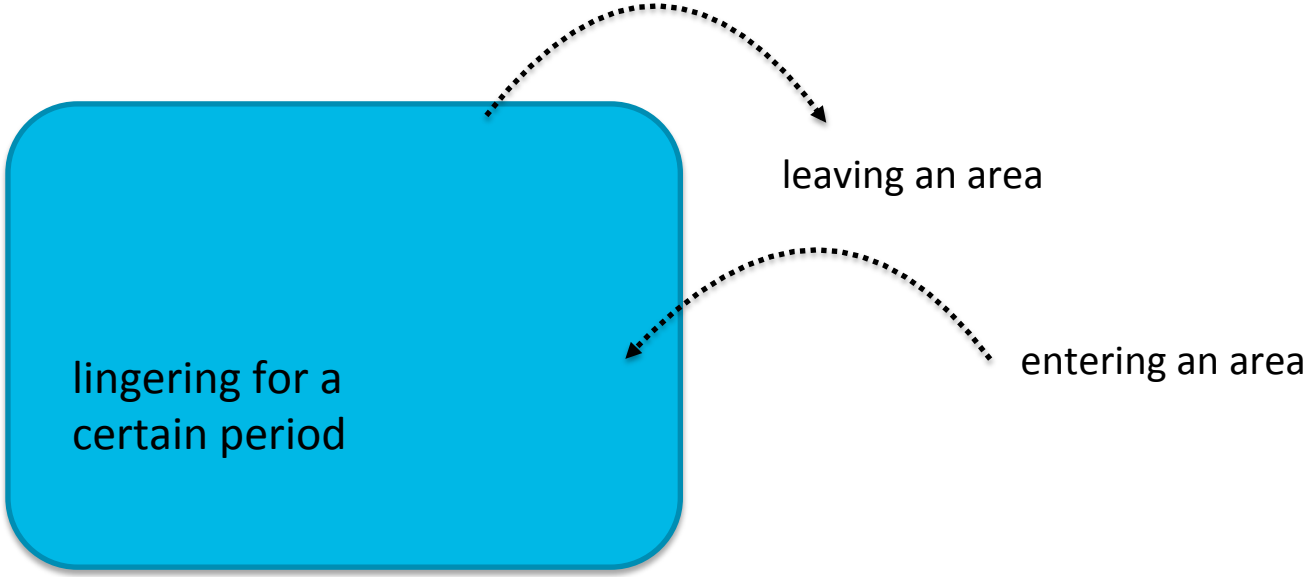
Use Cases

Geofencing



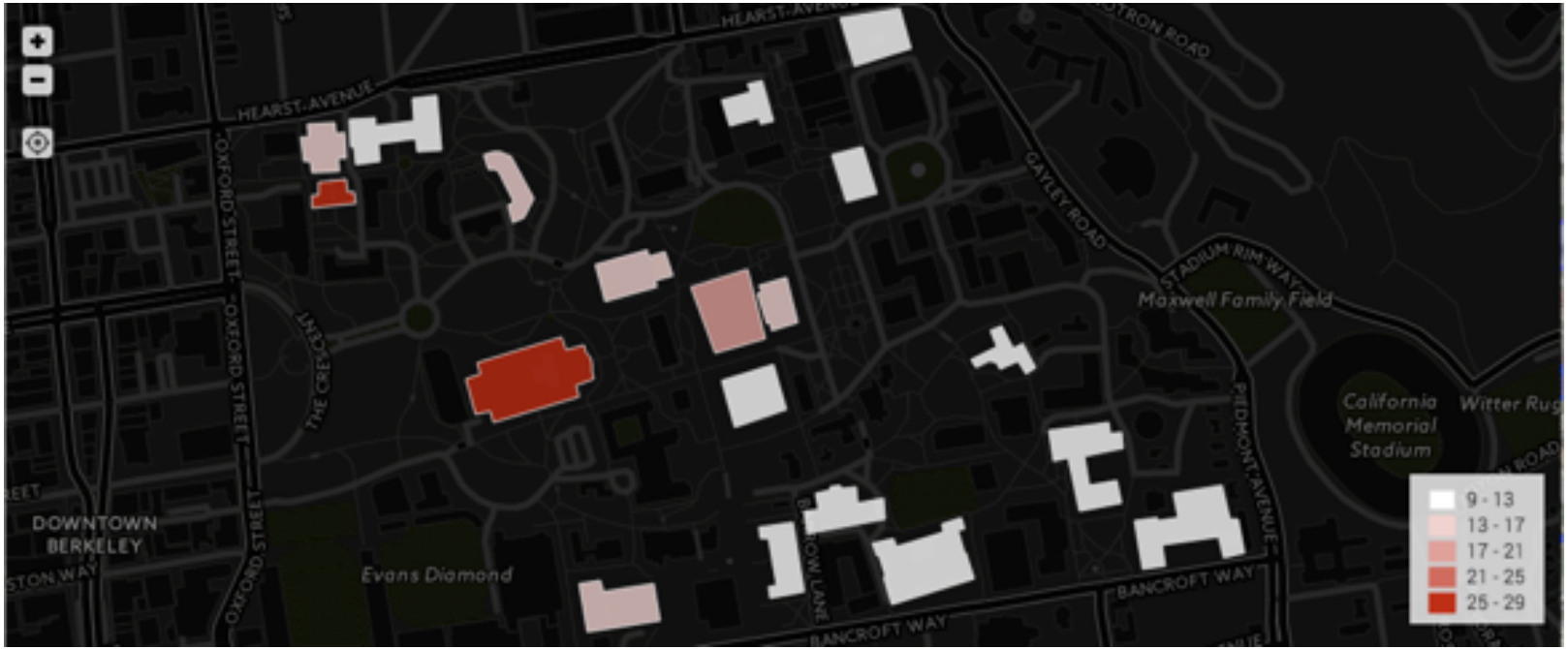
Use Cases

Geofencing



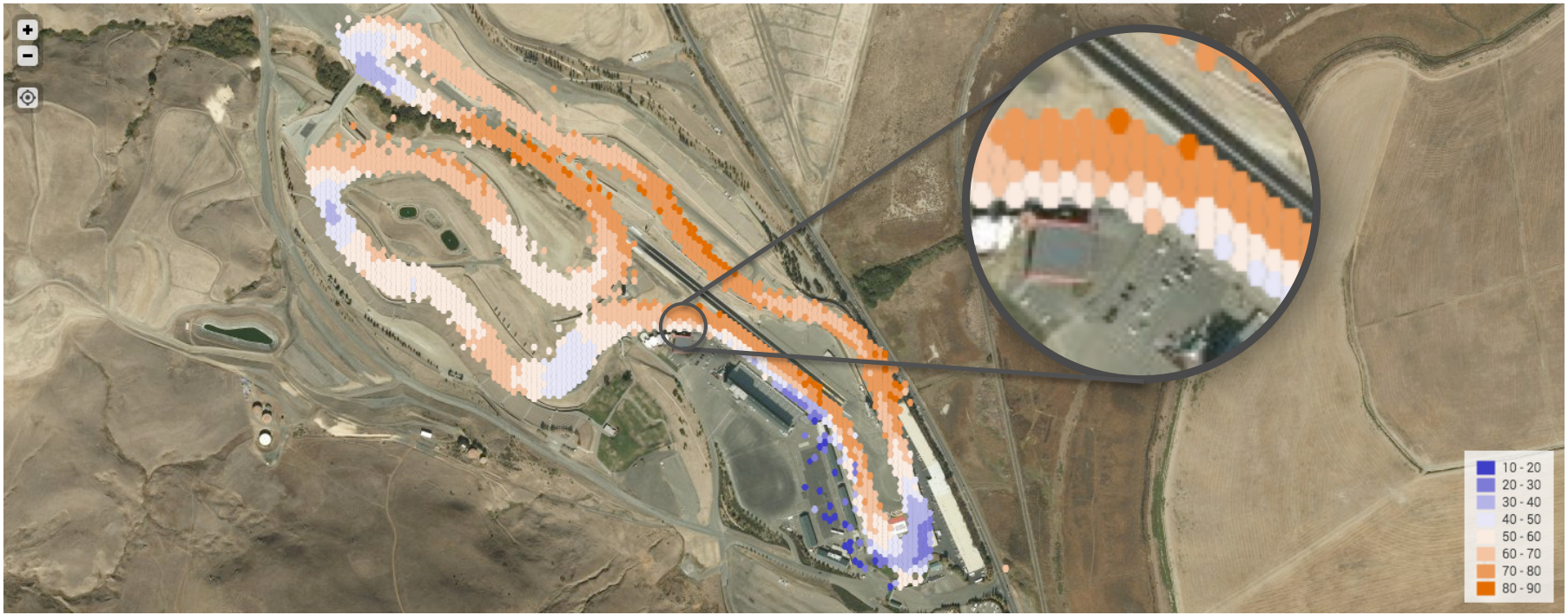
Use Cases

Campus Map: E.g. Show badge access



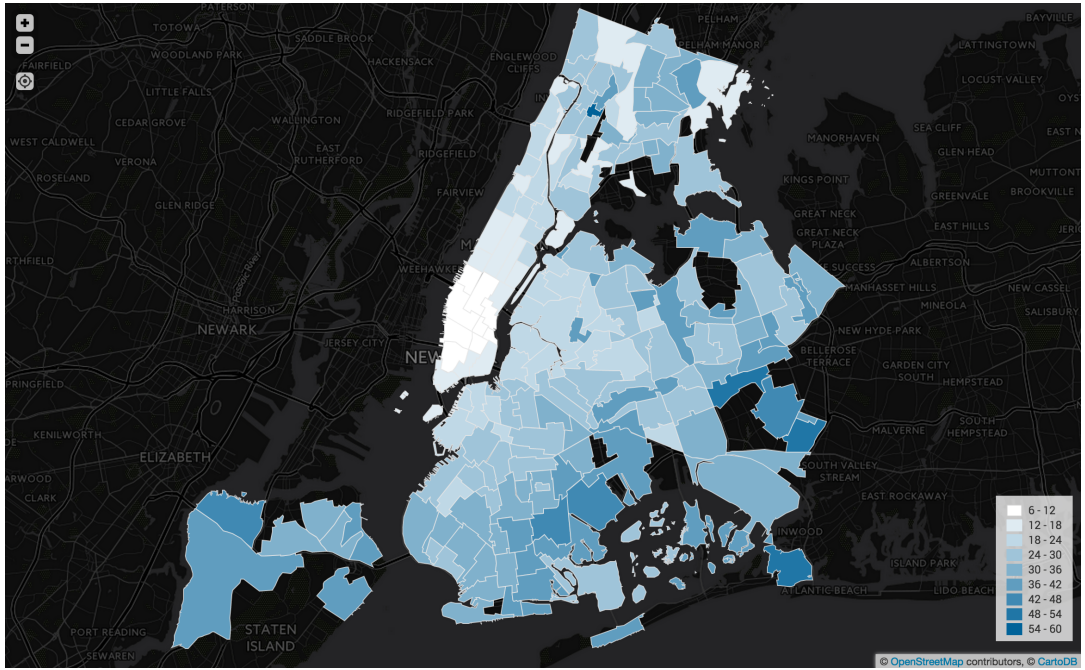
Use Cases

Hexagonal grid: Fine grained heat map



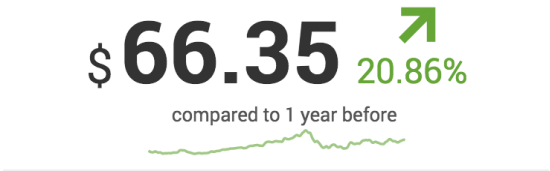
Examples Custom Polygons

New York neighborhoods: average taxi ride duration



Summary

Single Value redesigned for Dashboards

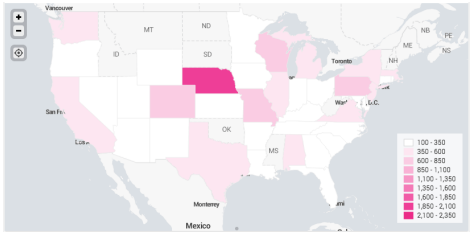


Geospatial Lookup based on custom boundaries

`36.104643, -115.165080`

Las Vegas?
MGM Convention Center?
United States?

High fidelity Choropleth maps based on custom shapes



THANK YOU

splunk>