

# Let's Customize Those Visualizations

Michael Porath

Product Manager, Splunk

.conf2016

splunk>

# Disclaimer

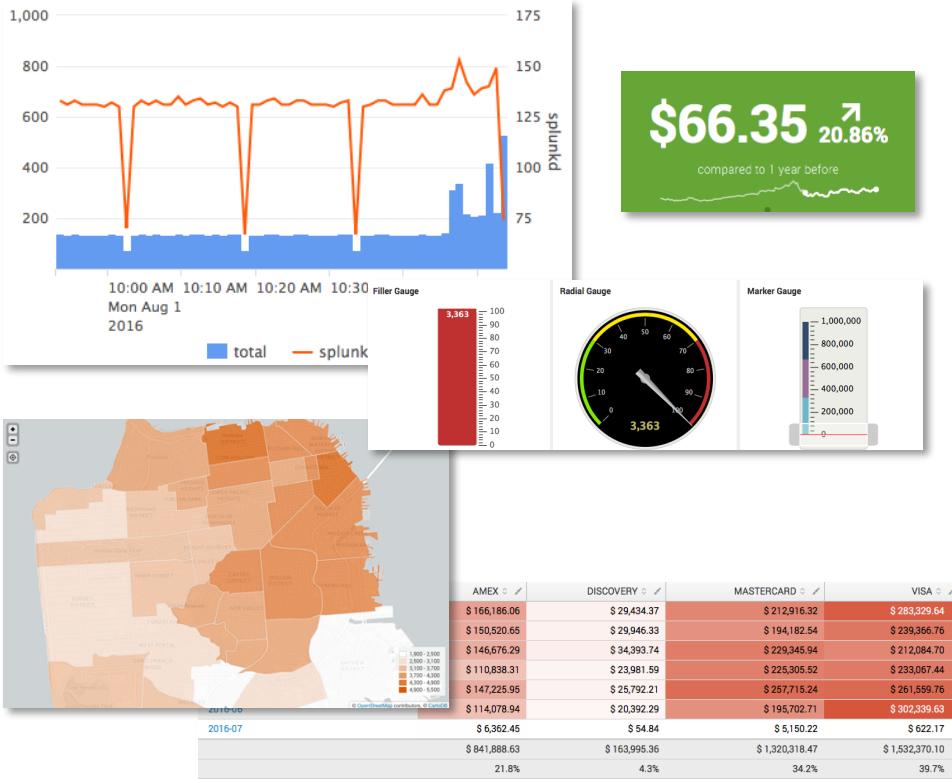
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results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

# “There’s A Visualization For That”

.conf2016

splunk>

# Native Visualizations in Splunk

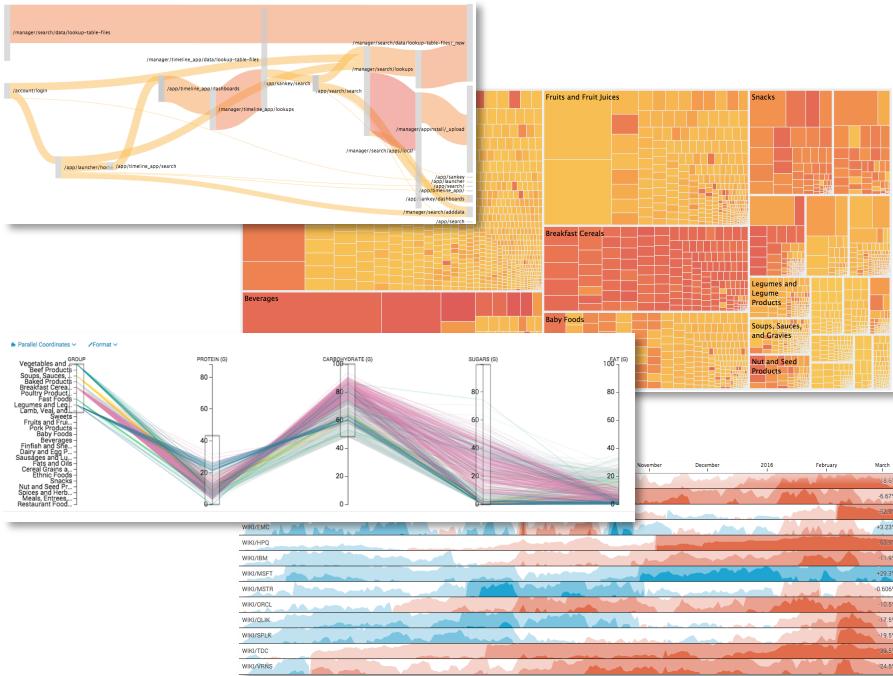


- Native charts and maps
  - Bar / Line / Area charts
  - Bubble / Scatter plots
  - Gauges
  - Maps
  - Single Value Displays
  - Tables
- Generalized to fit use cases across many different areas
- Can be customized to some extent to cover specific use cases

# Custom Visualization, the “old” way

- Custom <html> dashboard panels
- Requires changing app source code
- Only way to re-use across apps is to copy source to another app
- Non-trivial SimpleXML to make it work
- Much native functionality didn't work out of the box
  - Panel height
  - Resize events
  - Customization by end-users

# Custom Visualizations



- Platform **extensibility** framework and API
- Targeted at internal and external **developers** with web development / JS skills and basic knowledge of the Splunk platform
- Developers can make use of any third party libraries (d3.js, three.js, highcharts.js, etc...) that run in the browser\*

\* with minor adjustments, and if third party license permits such use

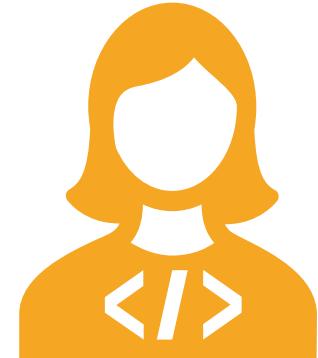
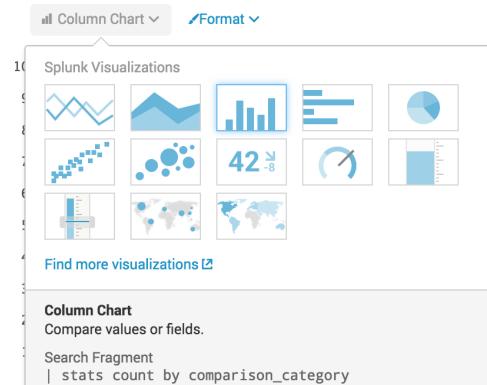
# Custom Visualizations for Developers

## Framework

- Javascript API that receives search results
- Declarative (HTML) API to expose format controls
- Visualizations picked up automatically to be shown in visualization picker
- All other aspects (permission, layering, app management etc) that apply to other knowledge objects

```
updateView: function(data, config)
```

```
<label class="control-label">Show Change In</label>
<div class="controls controls-block control-group controls-fill ">
  <splunk-radio-input name="display.visualizations.custom.
    horizon_chart_app.horizon_chart.show_change_in_percent" value="1">
    <option value="1" selected>Percent</option>
    <option value="0">Absolute Value</option>
  </splunk-radio-input>
</div>
```



# Custom Visualizations for Admins

- **Packaged as an app!**
- Installed like any other app
- No more copy/paste of code across apps
- Same permissioning / layering model
- Installed visualizations are automatically picked up by any other app if permissions are set that way



tools by Dolly Vu from the Noun Project

# Custom Visualizations for Users

- Choose from potentially dozens of installed visualizations!
- Appears as a first-class citizen alongside native visualizations
  - Looks and works just like packaged native visualizations
- Customize functionality and appearance of the visualization without touching any code, straight from the UI

The screenshot shows the Splunk user interface for selecting a visualization. At the top, there are dropdown menus for 'Column Chart' and 'Format'. Below this is a grid of 'Splunk Visualizations' including various chart types like line, bar, and pie charts, as well as more complex visualizations like scatter plots and world maps. A 'More' section below the grid shows additional visualization options. At the bottom, a detailed description of the selected 'Column Chart' is provided, along with a search fragment for generating the visualization.

Column Chart

Format

Splunk Visualizations

More

Find more visualizations ↗

Column Chart

Compare values or fields.

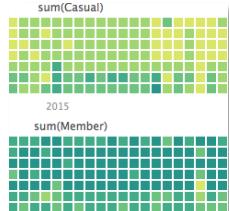
Search Fragment

| stats count by comparison\_category

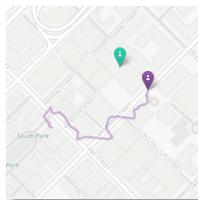
# New Splunk Visualizations



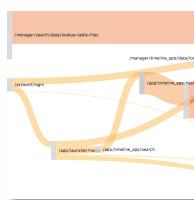
Punchcard



Calendar  
Heat Map



Location  
Tracker



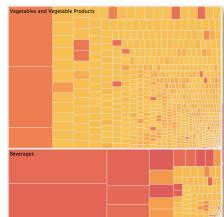
Sankey  
Diagram



Bullet Graph



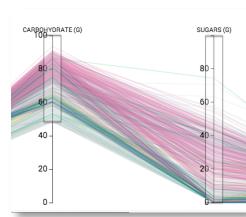
Timeline



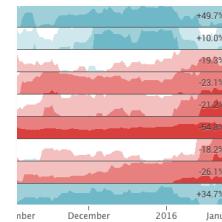
Treemap



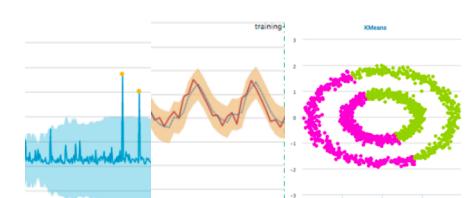
Horseshoe  
Meter



Parallel  
Coordinates



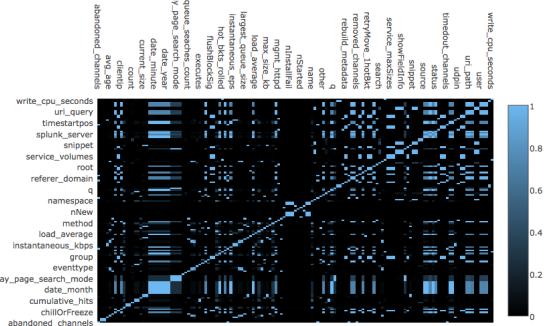
Horizon  
Chart



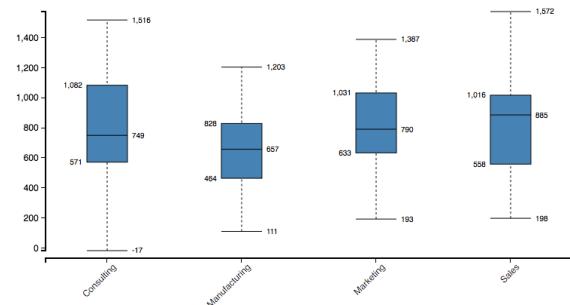
Machine Learning  
Charts

*Multiple use cases across IT, security, IoT, and business analytics*

# New Partner / Community Visualizations



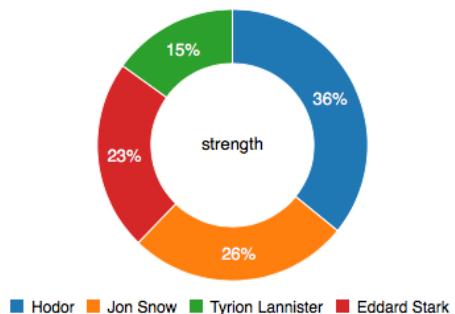
Heat Map



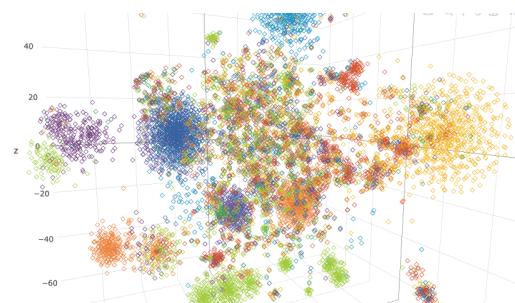
Box Plot



Wordcloud

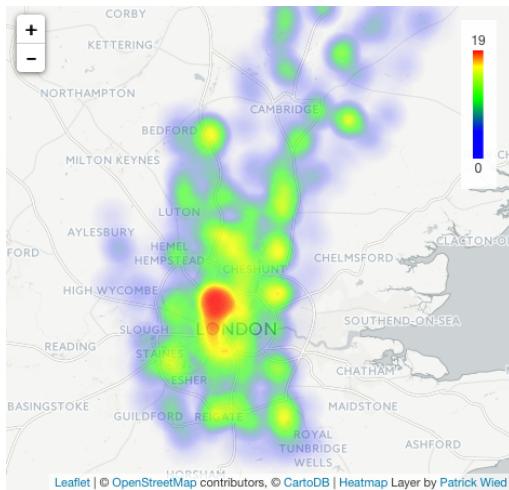


Donut Chart

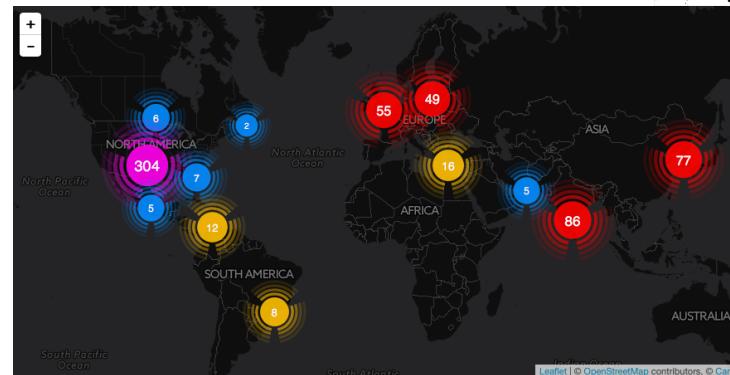


3D scatter plot

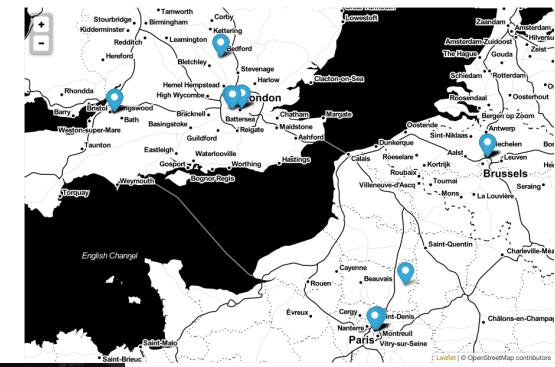
# New Partner / Community Visualizations



Geo Heatmap



Custom Cluster Map



Clustered Single Value Map

# What's possible beyond that?

- Anything that works in the browser
- Video
- Interactivity
- WebGL

Splunk > App: Splunk for Audio-Visual Data

Administrator Messages Settings Activity Help Find

New Search

| inputlookup ups1.csv | search label=\*man;\* AND label=\*people;\* | rex field=coord "(?<x>\d\*),(?<y>\d\*),(?<q>\d\*),(?<h>\d\*)" | where x > 300

18 results (6/5/14 11:39:25.000 AM to 6/5/14 11:39:30.000 AM) No Event Sampling Date time range Save As Close

Events Patterns Statistics (18) Visualization

Image Gallery

water,people,one,ice,action;man,lake,winter,river,snow,two,outdoors,pool,motion;fun,beach,adult,sea,receration,reflection

CH2

Verification whether we can use this still pending

1

_time	anomaly	coord	crop	file	h	kmean	label
2014-05-05 11:36:22	0	491,285,77,46	crop46500.0-0.jpg	ups1/46500.0.jpg	46	[73.304749, 95.0355, 134.61659, 176.94813, 189.47618, 186.5155, 32.099289, 43.545254, 48.139656]	nature,panoramic,outdoors,san
2014-05-05 11:36:23	0	418,288,90,63	crop47833.0.jpg	ups1/47833.0.jpg	63	[194.466809, 199.8441, 190.29608, 35.974693, 35.196499, 33.011823, 80.18876, 99.651566, 135.40599]	water,man;nature,people,outdo
2014-05-05 11:36:50	1	307,224,109,107	crop75433.0.jpg	ups1/75433.0.jpg	107	[32.999676, 31.812485, 23.286873, 207.93164, 209.17261, 193.01103, 168.73645, 158.09927, 137.67651]	sport,water,play,squad,ball,su
2014-05-05 11:36:51	0	301,189,139,142	crop76466.7-0.jpg	ups1/76466.7.jpg	142	[139.31995, 142.78334, 125.6921, 196.13493, 200.5392, 186.0229, 30.631018, 39.172615, 32.89402]	man;water,people,fun,action,ou

# THANK YOU

.conf2016

splunk®