

# What's New – Custom Visualizations

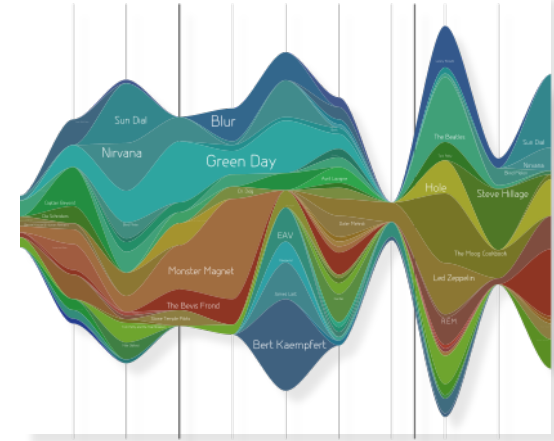
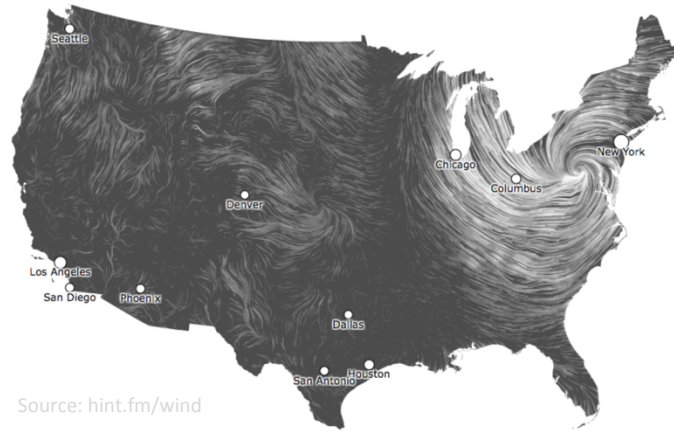
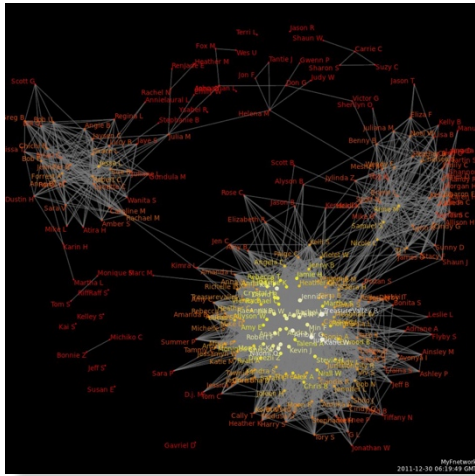
Michael Porath

Product Manager, Splunk

.conf2016

splunk >

# Visualizations For Each Use Case



# “There’s A Visualization For That”



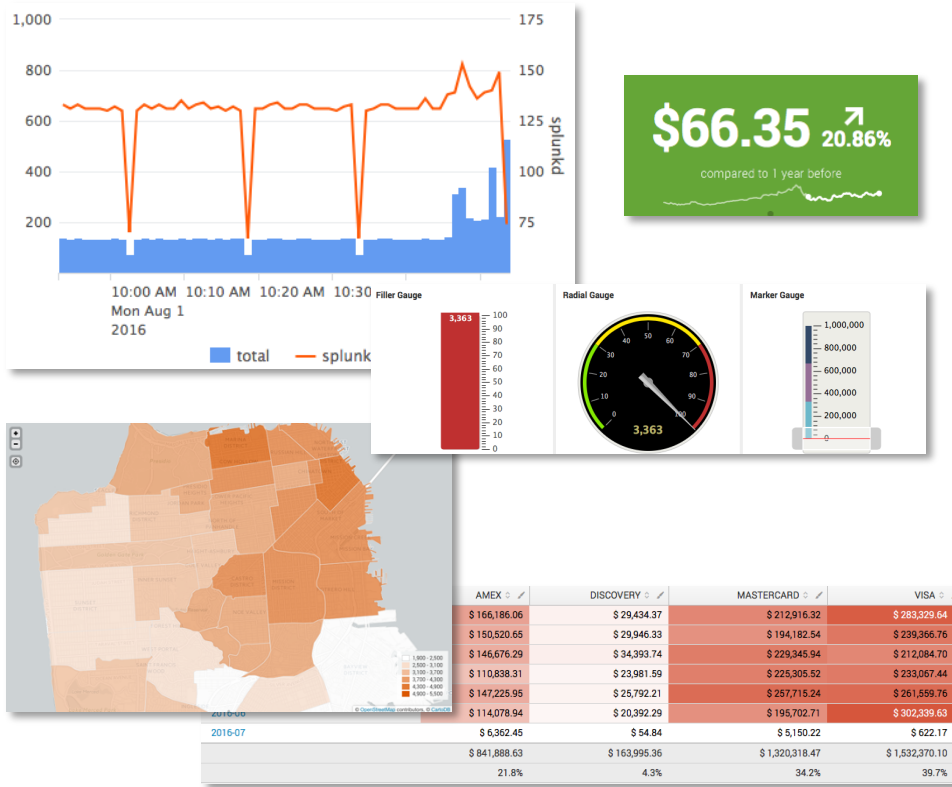
.conf2016

# 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.



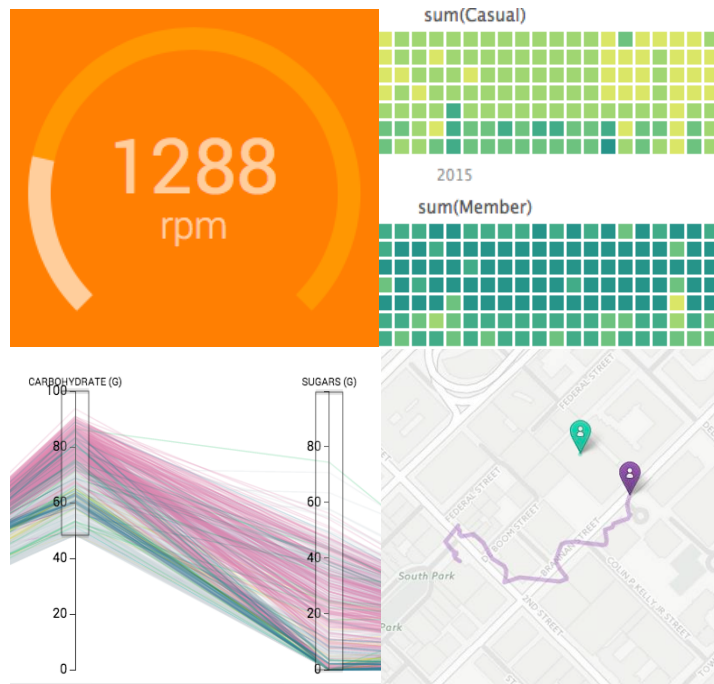
# Native Visualizations In Splunk



- 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 Visualizations FTW!

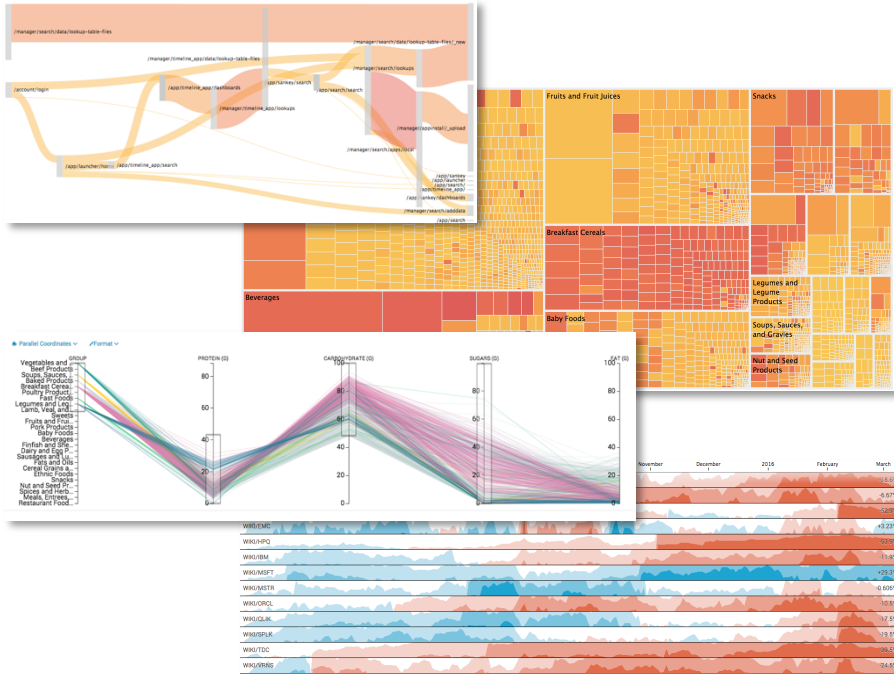
- Many use cases require a more specific visualization
- Specific custom appearance
- Represent data where native visualizations are not suitable
  - You can Splunk everything!
  - We won't be able to predict every possible use case



# 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



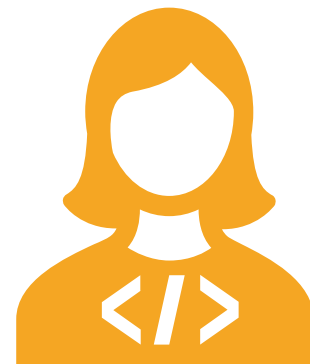
- Platform **extensibility** framework and API
- Targeted at internal and external **developers** with web development / JS skills and basic knowledge of the Splunk platform
- Developers can make use of any third party libraries (d3.js, three.js, highcharts.js, etc...) that run in the browser\*

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



# Custom Visualizations For Developers

- Works with any browser technology
- Can be a standalone app or part of a larger solution
- Standard APIs to define functionality (JS), styling (CSS) and configuration options declaratively (XML)



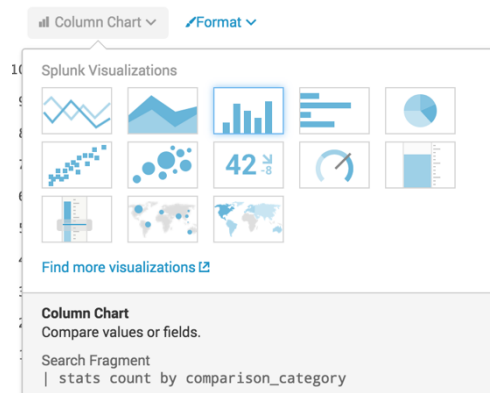
# Custom Visualizations For Developers

## 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)
```

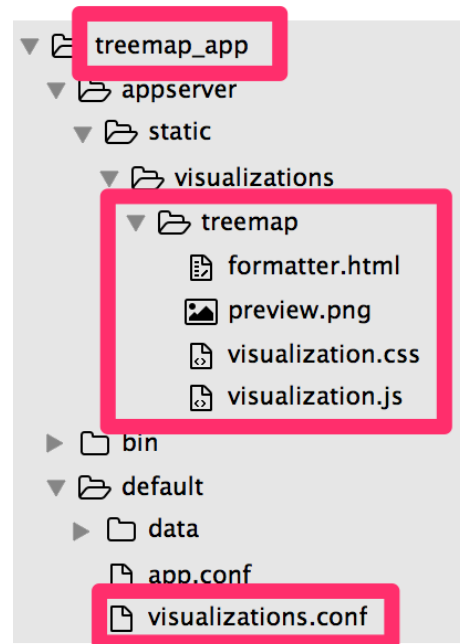
```
<label class="control-label">Show Change In</label>  
<div class="controls controls-block control-group controls-fill ">  
  <input type="radio" name="display.visualizations.custom.  
    horizon_chart_app.horizon_chart.show_change_in_percent" value="1">  
    <option value="1" selected>Percent</option>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



# Custom Visualizations

## How does it work?

- **Packaging**
  - Packaged as an app
  - One or many visualizations packaged in one app
  - Visualization can be part of a larger solution
- **Most important files**
  - Meta data: `visualization.conf`
  - Visualization Code: `visualization.js`
  - Styling: `visualization.css`
  - Format Editor specification: `formatter.html`



# 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 Admins

## Installation



Users can search for visualizations on Splunkbase and directly in the product

**Products Supported**

- Splunk Enterprise
- Splunk Cloud
- Splunk Light
- Hunk
- Splunk Enterprise Security

**> Splunk Version**

- 6.3
- 6.2
- 6.1
- 6.0
- 5.0

**Content Type**

- App
- Add-on

**App Contents**

- Inputs
- Alert Actions
- Visualizations**

## In-product

Browse More Apps

Find apps by keyword, technology...

CATEGORY

- Application Management
- IT Operations Management
- Security and Compliance
- Business Analytics
- Utilities
- Cool Stuff
- Internet of Things

CIM VERSION

- 4.3
- 4.2
- 4.1
- 4.0
- 3.0

SUPPORT TYPE

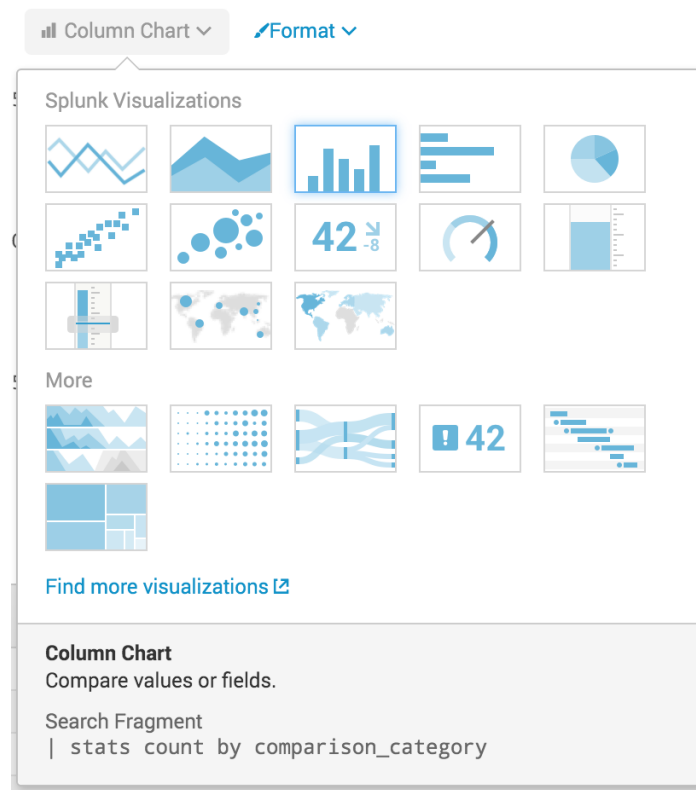
- Community
- Splunk
- Developer

APP CONTENT

- Inputs
- Alert Actions
- Visualizations**

# Custom Visualizations For Users

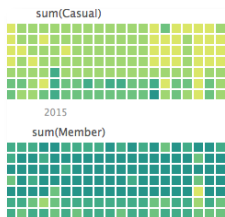
- Choose from potentially dozens of installed visualizations!
- Appears as a first-class citizen alongside native visualizations
  - Looks and works just like packaged native visualizations
- Customize functionality and appearance of the visualization without touching any code, straight from the UI



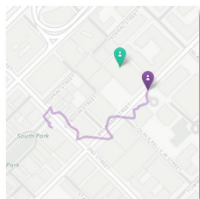
# New Splunk Visualizations



Punchcard



Calendar Heat Map



Location Tracker



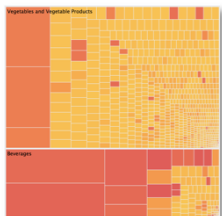
Sankey Diagram



Bullet Graph



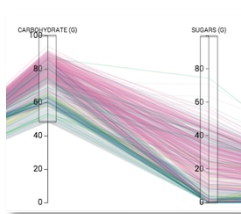
Timeline



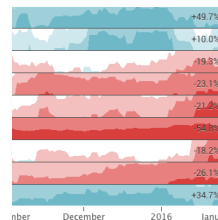
Treemap



Horseshoe Meter



Parallel Coordinates



Horizon Chart



Machine Learning Charts

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

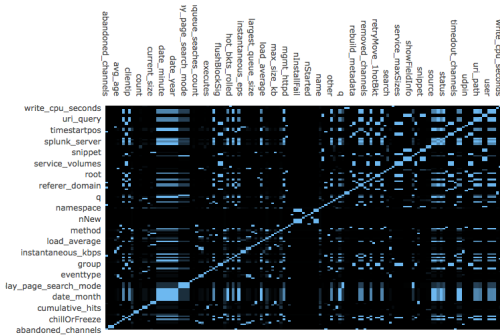
# Custom Visualizations – Demo



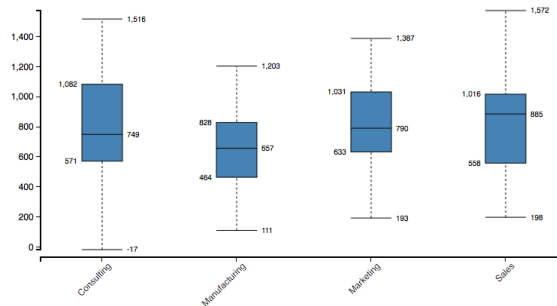
.conf2016



# New Partner/Community Visualizations



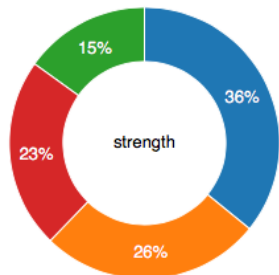
Heat Map



Box Plot

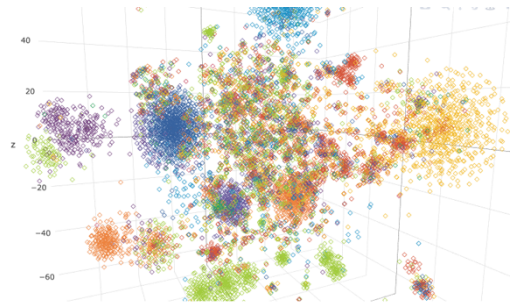


Wordcloud



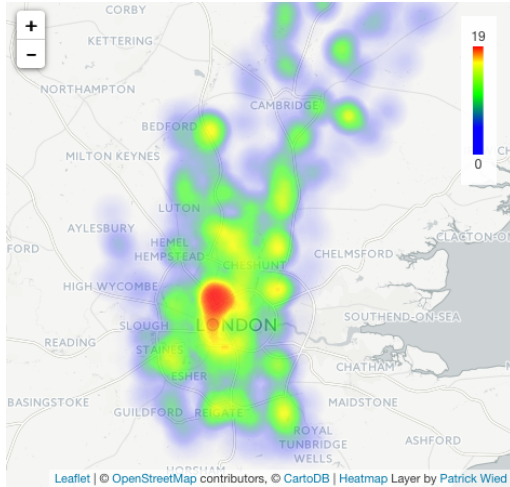
■ Hodor ■ Jon Snow ■ Tyrion Lannister ■ Eddard Stark

Donut Chart



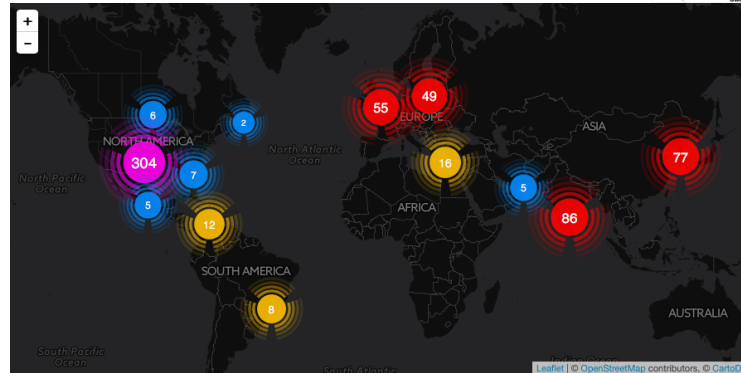
3D scatter plot

# New Partner/Community Visualizations



Geo Heatmap

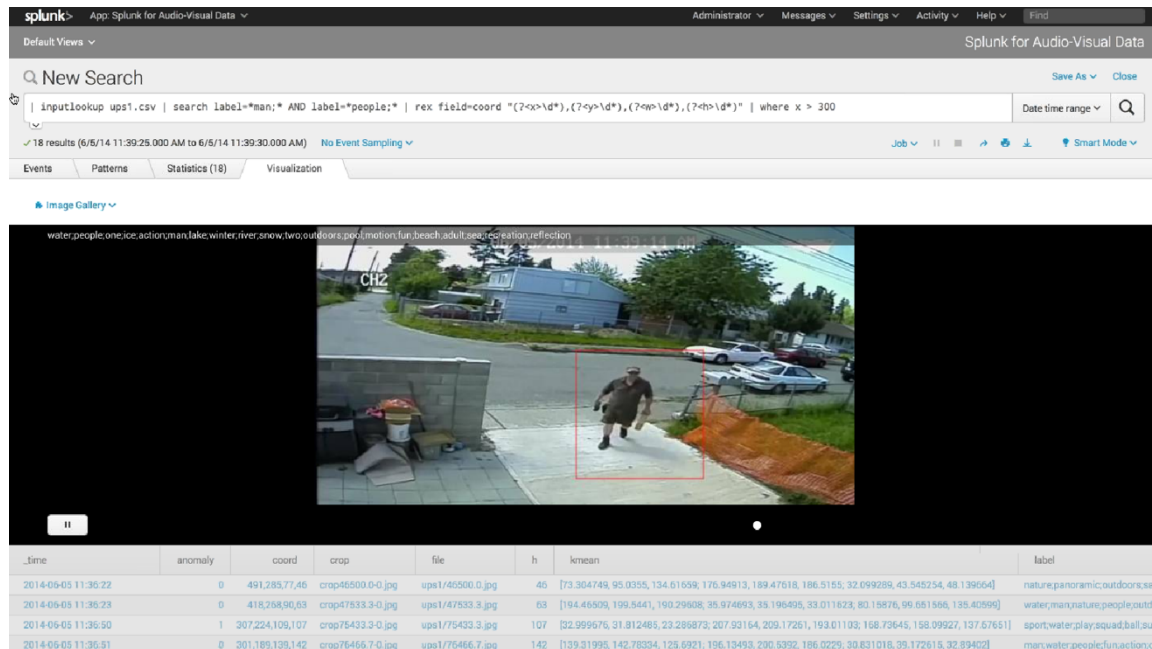
Custom Cluster Map



Clustered Single Value Map

# What's Possible Beyond That?

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



The screenshot shows the Splunk interface for the 'Splunk for Audio-Visual Data' app. A search query is entered: `inputlookup ups1.csv | search label=*man;* AND label=*people;* | rex field=coord "(?<math>x</math>)\d+(,)?(?<math>y</math>)\d+(,)?(?<math>z</math>)\d+(,)?(?<math>h</math>)\d+" | where x > 300`. The search results show 18 results from 6/5/14 11:39:25.000 AM to 6/5/14 11:39:30.000 AM. Below the search bar, there are tabs for 'Events', 'Patterns', 'Statistics (18)', and 'Visualization'. The 'Image Gallery' view is active, displaying a video player with a red bounding box around a person walking. Below the video player, a table lists the search results.

_time	anomaly	coord	crop	file	h	kmean	label
2014-06-05 11:36:22	0	491,285,77,46	crop46500 0-0 .jpg	ups1/46500_0.jpg	46	[73.304749, 95.0355, 134.61659, 176.94913, 189.47618, 186.5155, 32.059289, 43.545254, 48.139664]	nature;panoramic;outdoors;san
2014-06-05 11:36:23	0	418,268,90,63	crop47833 3-0 .jpg	ups1/47833_3.jpg	68	[164.46609, 199.5441, 190.29608, 35.974693, 35.196405, 33.011623, 80.18876, 99.681866, 135.40599]	water;man;nature;people;outdo
2014-06-05 11:36:30	1	307,224,109,107	crop75433 3-0 .jpg	ups1/75433_3.jpg	107	[32.959576, 31.812485, 23.288873, 207.93164, 209.17261, 193.01103, 166.72645, 158.09927, 137.67651]	sport;water;play;squad;ball;su
2014-06-05 11:36:31	0	301,189,139,142	crop76466 7-0 .jpg	ups1/76466_7.jpg	142	[139.31995, 142.78334, 125.6921, 196.13493, 200.5392, 186.0225, 30.831018, 39.172615, 32.83402]	man;water;people;fun;action;ou

# What Now?

Related breakout sessions and activities...

- “Building Splunk Visualizations with the New Custom Visualization API”  
– *session by Marshall Agnew*
- What’s New in Dashboards, Visualizations, and Alerting  
– *session by Michael Porath and Nick Filippi*



# THANK YOU

.conf2016

