

# Dashboard Wizardry: *Advanced Dashboard Interactivity*

Nicholas Filippi - Product Management, Splunk

Siegfried Puchbauer - Core Engineering, 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 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.

# Brought to You By...



**Siegfried Puchbauer**

- Lead Engineer, Dashboard Team
- Expert in Dashboards, Alerting, Javascript, and Bowler Hats



**Nicholas Filippi**

- Product Management, Splunk
- Responsible for Dashboards & Info Delivery

# You are Here Because...

- Interested in Building More Interactive Dashboards
- Don't Want to Use Custom Javascript or Stylesheets
  - (but familiar with Simple XML)

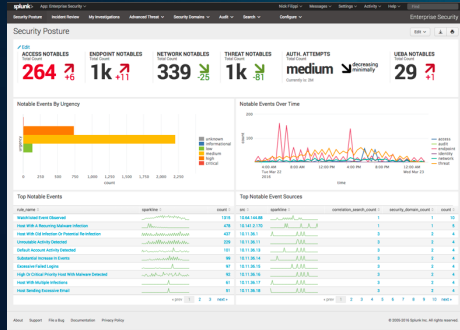


# Agenda

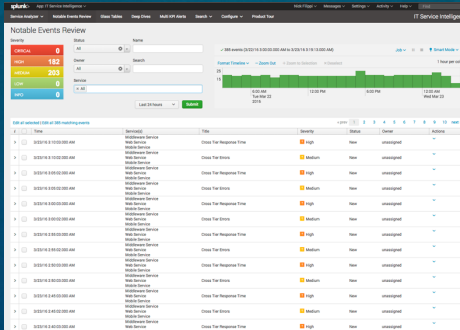
- Background
- Live Example
  - Tokens
  - Event Handlers
  - Show/Hide content
  - Search Events
- What's new in Splunk 6.5
- Wrap-Up

# What Is A Dashboard?

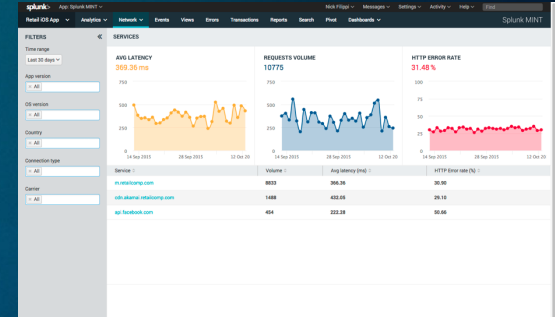
## Enterprise Security



## IT Service Intelligence



## MINT

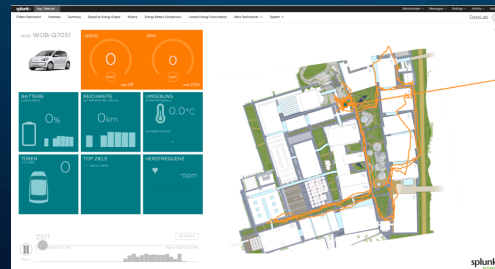


Premium Solutions

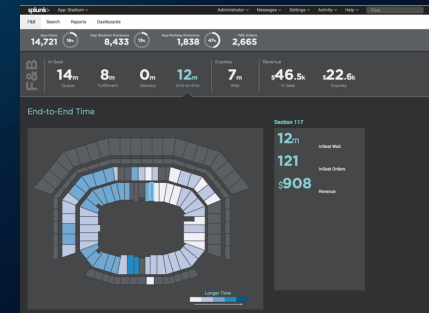
## Sample App



## eCars Project

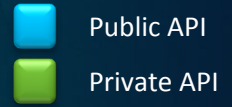


## Stadium Project



Internal Examples

# Dashboard Stack

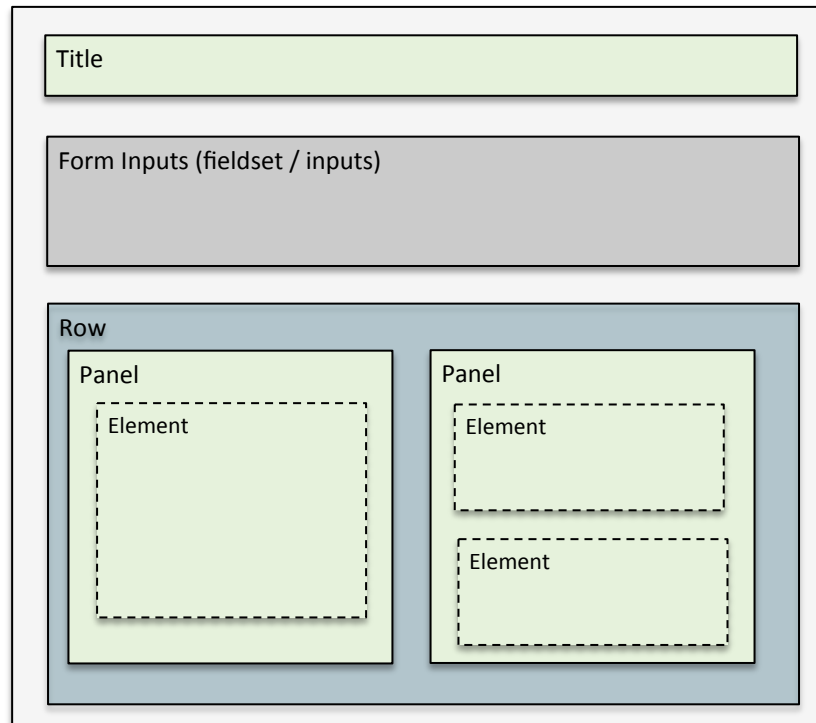


# Anatomy of a Dashboard

```
<form>
  <label>My Dashboard</label>

  <fieldset>
    <input>
      <!-- form inputs -->
    </input>
  </fieldset>

  <row>
    <panel>
      <chart>
        <!-- ... -->
      </chart>
      <table>
        <!-- ... -->
      </table>
    </panel>
  </row>
</form>
```



# Dashboard Fundamentals

Layout	Search Managers	Event Handlers	Form Inputs	Display Controls	Visualizations	Extensions
<ul style="list-style-type: none"><li>• row</li><li>• panel</li><li>• element</li></ul>	<ul style="list-style-type: none"><li>• search</li><li>• ref (report)</li><li>• base (Post-process)</li><li>• cache</li><li>• refresh**</li><li>• refreshType**</li></ul>	<ul style="list-style-type: none"><li>• input</li><li>• change</li><li>• search</li><li>• drilldown</li><li>• selection</li><li>• init**</li></ul>	<ul style="list-style-type: none"><li>• text</li><li>• radio</li><li>• dropdown</li><li>• checkbox</li><li>• multiselect</li><li>• link</li><li>• time</li></ul>	<ul style="list-style-type: none"><li>• depends</li><li>• rejects</li></ul>	<ul style="list-style-type: none"><li>• Events</li><li>• Table</li><li>• Line</li><li>• Area</li><li>• Column</li><li>• Bar</li><li>• Pie</li><li>• Scatter</li><li>• Bubble</li><li>• Single Value</li><li>• Radial Gauge</li><li>• Filler Gauge</li><li>• Marker Gauge</li><li>• Map</li><li>• Choropleth Map</li></ul>	<ul style="list-style-type: none"><li>• script (JS)</li><li>• stylesheet (CSS)</li><li>• dashboard.js</li><li>• dashboard.css</li></ul>

Token Management


\*\* New in Splunk Enterprise 6.5

# Let's Build Some Dashboards!

.conf2016



# The Data: Track Day

- Sonoma Raceways
  - 1 Day
  - 28 Splunkers
  - 30 Cars
  
- Data via  **carvoyant**  
Your Car. Your Data. Your API.
  - ODB II Dongle -> Cloud Service -> Modular Input
  - Location data & metrics (speed, rpm, etc)



# The Data: Track Day

The screenshot displays the Splunk interface for an application named 'Track Day'. The search query is `sourcetype=trackday_json`, which has returned 195,885 events. A timeline visualization at the top shows green bars representing data points over time. Below this, a table lists individual events. Two events are visible, both occurring on 7/18/15 at approximately 6:59 PM. Each event contains a JSON object with various vehicle and engine metrics.

i	Time	Event
>	7/18/15 6:59:59.000 PM	<pre>{ [-]   accountId: 2900   batteryVoltage: 13.418   dataSetId: 29971979   engineCoolantTemperature: 90   engineSpeed: 1197   fuelLevel: 58.03   heading: 168.36   ignitionStatus: RUNNING   lateralGForce: 0.68   latitude: 37.785328   longitude: -122.41623   longitudeGForce: -0.02   speed: 16   timestamp: 20150719T015959+0000   tripId: 1364164   vehicleDatumId: 194199587   vehicleId: 50678   verticalGForce: -2.0 }</pre> <p>Show as raw text</p> <p>host = nflippi-mbp.sv.splunk.com   source = /Users/nflippi/splunk/vvory/splunk/etc/apps/advanced_dashboards/data/track_day/json   sourcetype = trackday_json</p>
>	7/18/15 6:59:58.000 PM	<pre>{ [-]   accountId: 2900   batteryVoltage: 13.418   dataSetId: 29971977   engineCoolantTemperature: 90   engineSpeed: 1254   fuelLevel: 58.03   heading: 167.59   ignitionStatus: RUNNING   lateralGForce: 0.7   latitude: 37.78539   longitude: -122.416245   longitudeGForce: 0.03   speed: 17   timestamp: 20150719T015958+0000   tripId: 1364164   vehicleDatumId: 194199571   vehicleId: 50678   verticalGForce: -2.0 }</pre> <p>Show as raw text</p>

# Building Dashboards

## Part I

# Tokens

- Automatic data binding
- Variables – connecting components and interactions
- Use in UI or XML

`$buttercup$`

# Token Filters

- Insert altered/processed value
- Built-in
  - \$token|s\$ - search escape
  - \$token|u\$ - URL encode
  - \$token|h\$ - HTML escape
  - \$token|n\$ - No encoding (New in Splunk 6.5)
- Build your own (in Javascript)
  - \$token|myfilter\$

# Form Input Values and Token Namespaces

- Token Namespaces
  - **default** – current values of form input fields
  - **submitted** – submitted values of fields
  - **url** – submitted form.\* tokens persisted
- **\$form.mytoken\$**  
tokens contain raw form input
- **\$mytoken\$**  
after applying prefix, suffix, default value

Refer to namespaces:

**\$submitted:driver\$**

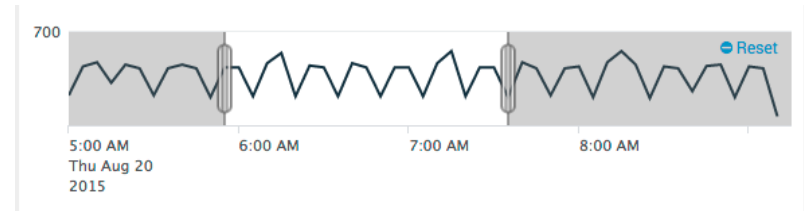
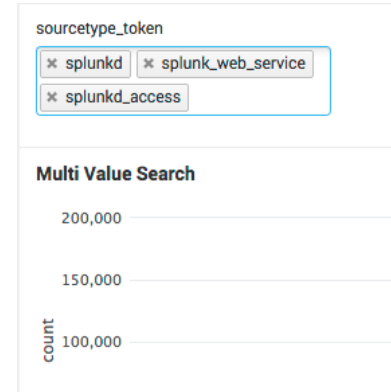


# Building Dashboards

## Part II

# Event Handlers

- Introduce behaviors based on event hooks
  - User initiated events, or search job events
- Types
  - Drilldown/condition – user clicks on a cell, or bar on a chart
  - input / change – user selects a value on a form input
  - selection – for line/column/area, user selects a window to zoom into
  - search – events come back from a search job (progress, done, error)
  - init – initial page load; use this to set page tokens
- Configure Behaviors
  - Set tokens
  - Unset tokens
  - Link to another page or search
  - Evaluate new tokens



# Show and Hide Content

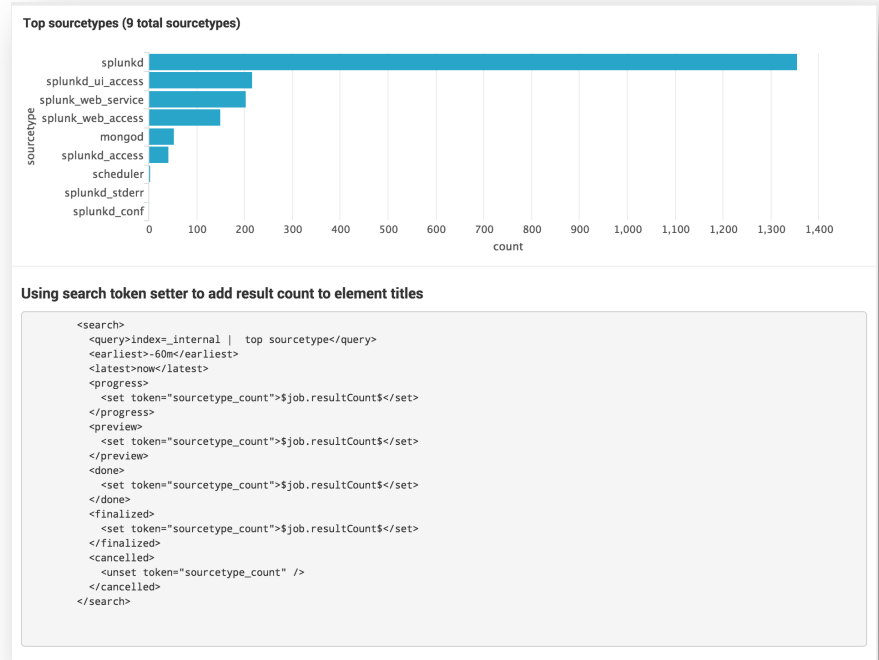
- Control whether you hide or show a given object based on existence of a token
  - Contextual (in-page) Drilldown
  - Cascading Form Inputs
- Applies to element, row, panel, input objects
- Type
  - `<table depends="$show_table$">`
    - Hide by default, show when token(s) exist
  - `<table rejects="$hide_table$">`
    - Show by default, hide when token(s) exist

# Building Dashboards

## Part III

# Search & Result Token Setter

- Advanced Dashboard Logic
- Key Benefits
  - Include result count in title
  - Null search swapper (hide if search returns no results)
  - Custom HTML element driven by search object
- Run search object anywhere on the page
- Set tokens within search based on
  - Search metadata (string, earliest/latest)
  - Job metadata (result count, run time)
  - 1<sup>st</sup> result
- Eval-based condition/value support



# Wrap-Up



.conf2016



# What's New in 6.5

- Search Refresh & RefreshDisplay
- Initial Page Load Controls
  - <init> event
  - Global environment variables
- Token Filters
  - For "No Encoding", use \$token|n\$

# Dashboard Refresh

*optimizing the view experience for continuous monitoring of insights*

- Continuous dashboard monitoring
  - Run refresh searches in the background, then configure how you want the results to surface to the UI
  - Seamlessly transition new results to the page
  - Pseudo real-time behavior
- Technical Details
  - Configurable refresh indicator
    - (“none” | “progress bar” | “preview and progress bar”)
  - Configurable refresh interval/delay schedule
  - UI editor support (no XML editing needed)
  - Refresh supported within search manager

Dashboard Refresh

Enable dashboard elements to auto-refresh, optimizing the view experience for continuous monitoring of insights

Preview Progress Bar None

refresh.display="preview" (Pre-Ivory Behavior) refresh.display="progressbar" refresh.display="none"

262,500 1,423,375 1,423,375

Preview Progress Bar None

refresh.display="preview" (Pre-Ivory Behavior) refresh.display="progressbar" refresh.display="none"

count

30,000 20,000 10,000

12:00 PM 8:00 PM 4:00 AM

Mon Jul 18 2016 Tue Jul 19 2016

\_time

Enhanced Dashboard Refresh

The behavior of a real-time dashboard, now powered by historical searches. Introducing the enhanced dashboard to optimize for the given view experience. The net result, create dashboards that can more effectively be used for overhead display in an operations center.

Key features:

- Configurable Refresh Indicator - Choose the desired refresh behavior (Preview, Progress Bar, None)
- Moved Refresh Control to Search Manager - This enables users to setup refresh even for global searches
- Configurable Refresh Schedule Type - Choose between interval-based or delay-based refresh times (delay is supported)
- UI Controls Support - Configuring refresh time and behavior is fully supported in the UI search editor for each search
- Differentiate Refresh Search from Initial/Form-driven - Configurable behavior only applies to refresh search

Sample XML with the new refresh controls:

```
<chart>
  <!-- Set the refresh time and type (delay || interval) directly in the search object -->
  <search>
    <query>index=_internal | timestats count</query>
    <earliest>=7d</earliest>
  </search>
  <refresh interval="1m" type="delay"/>
</chart>
```

omnie13000@en-US:~/app/refresh-test

Edit Search

Title refresh.display="progressbar"

Search String index=\_internal | stats count

Run Search

Time Range Last 7 days

Auto Refresh Delay 30 seconds

Refresh Indicator Progress bar

None  
Background Search with No Progress Bar

Progress bar  
Background Search with Progress Bar

Preview and progress bar  
Preview Events with Progress Bar

Cancel

# Initial Page Load Controls

- Global Variables For Use Throughout the Page

- \$env:app\$
- \$env:user\$
- \$env:user\_realname\$
- \$env:user\_email\$
- \$env:locale\$
- \$env:page\$
- \$env:product\$
- \$env:version\$
- \$env:instance\_type\$
- \$env:deployment\_type\$

```
<dashboard>
  <label>Network Monitoring</label>
  <init>
    <set token="application">Exchange</set>
    <eval token="now">strftime(now(), "%m/%d/%y %H:%M:%S")</eval>
  </init>
  ...
</dashboard>
```

- <init> Event

- Set global page variables
- Use condition logic against global variables

# More Information

- Splunk 6.x Dashboard Examples

<https://splunkbase.splunk.com/app/1603/>

- Documentation

<http://docs.splunk.com/Documentation/Splunk/6.5.0/Viz/PanelreferenceforSimplifiedXML>

# More Information

- Demo Code

<https://github.com/splunk/advanced-dashboards-conf15>

- Splunk 6.x Dashboard Examples

<https://splunkbase.splunk.com/app/1603/>

- Documentation

<http://docs.splunk.com/.../6.3.0/Viz/OverviewofSimplifiedXML>

# Splunk 6.x Dashboard Examples App

- Recipe Book for Dashboards
- Updated on Every Release
- Examples
  - Basic
  - Chart
  - Table
  - Single Value
  - Map
  - Search Types
  - Form Input
  - Drilldown
  - Layout
  - Custom Visualizations
  - Token Customization
- Tools

The screenshot shows the Splunkbase page for the 'Splunk 6.x Dashboard Examples' app. The page features a dark header with the Splunkbase logo and navigation links for 'CATEGORIES', 'TECHNOLOGIES', and 'FOR DEVELOPERS'. A search bar is located in the top right corner. Below the header, the app title 'Splunk 6.x Dashboard Examples' is prominently displayed next to a green 'DOWNLOAD' button. A blue bar below the title contains 'ADMINISTRATOR TOOLS' and links to 'Manage App', 'View App', and 'View Analytics'. The main content area includes a description of the app, a rating section with 35 ratings and 4.5/5 stars, and a list of related apps under the heading 'VERSION 5.0.1'. A 'RELEASE NOTES' section is also visible, detailing updates and bug fixes. The footer contains a 'Sitemap' and various legal and support links.



# Come Visit – “Ask the Dashboard Expert”

@Dashboard Clinic

- For assistance with troublesome dashboards
- For migration tips
- To brag about something cool you built
- To ask questions
- Or, just to say hi!

# THANK YOU

.conf2016

