Dashboard Wizardry:
Advanced Dashboard Interactivity

Nicholas Filippi - Product Management, Splunk

Siegfried Puchbauer - Core Engineering, 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)

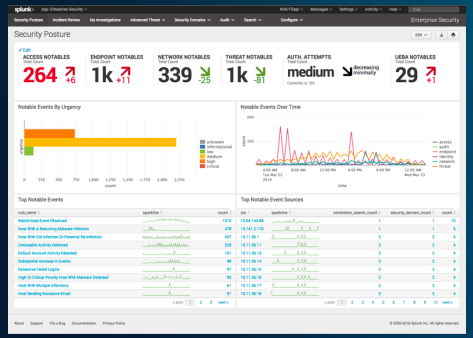
Agenda

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

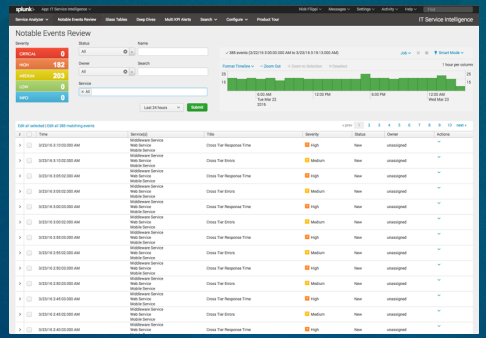
What Is A Dashboard?

Premium Solutions

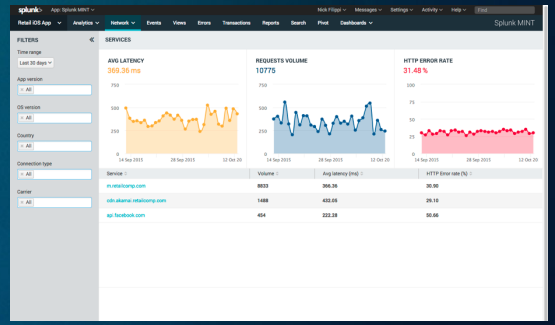
Enterprise Security



IT Service Intelligence

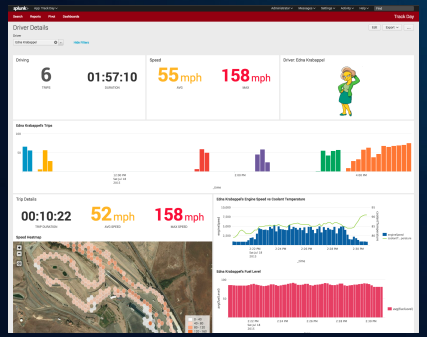


MINT

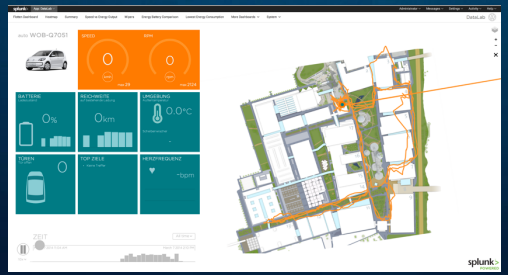


Internal Examples

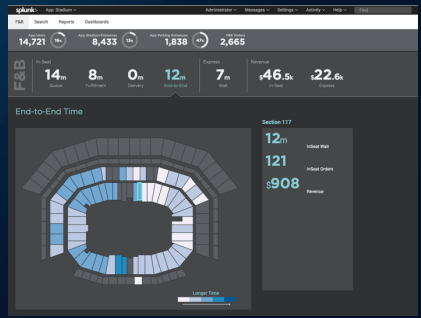
Sample App



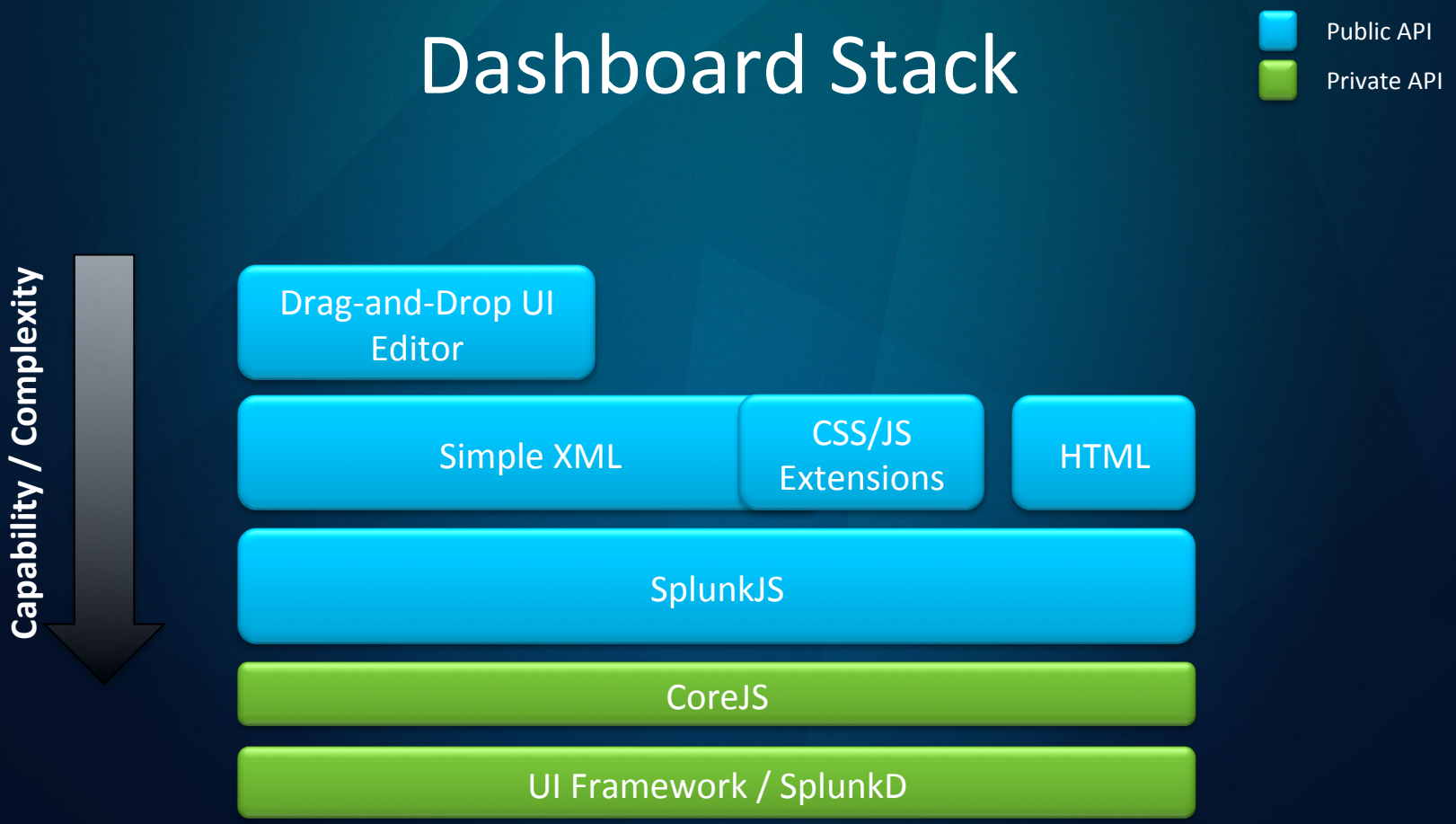
eCars Project



Stadium Project



Dashboard Stack

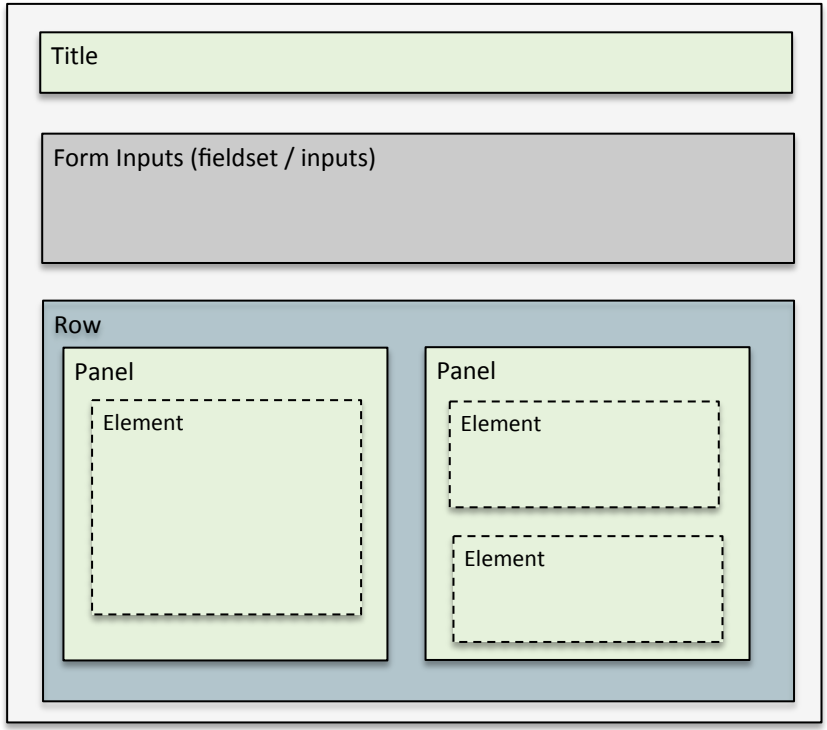


Anatomy of a Dashboard

```
<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
• row • panel • element	• search • ref (report) • base (Post-process) • cache • refresh** • refreshType**	• input • change • search • drilldown • selection • init**	• text • radio • dropdown • checkbox • multiselect • link • time	• depends • rejects	• Events • Table • Line • Area • Column • Bar • Pie • Scatter • Bubble • Single Value • Radial Gauge • Filler Gauge • Marker Gauge • Map • Choropleth Map	• script (JS) • stylesheet (CSS) • dashboard.js • dashboard.css

Token Management

** New in Splunk Enterprise 6.5

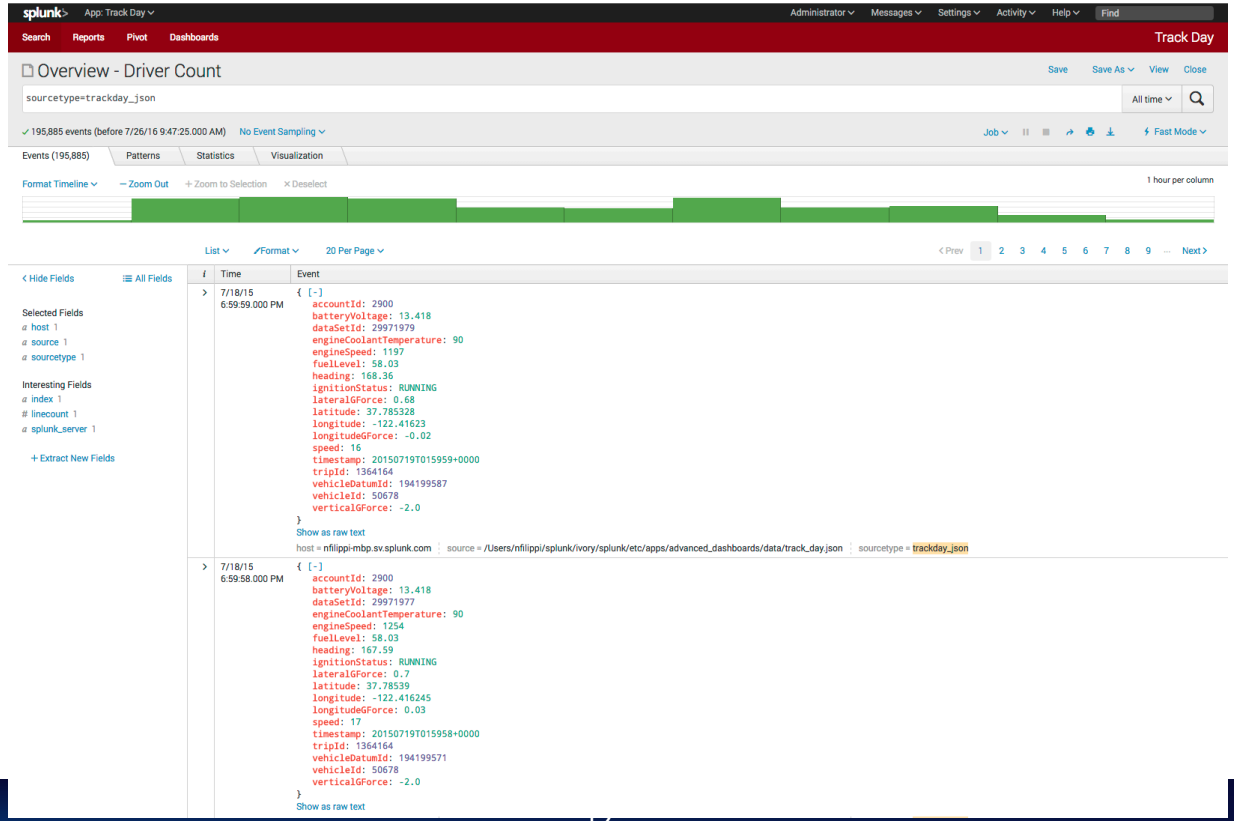
Let’s Build Some Dashboards!

The Data: Track Day

- Sonoma Raceways
  - 1 Day
  - 28 Splunkers
  - 30 Cars

- Data via carvoyant
  - ODB II Dongle -> Cloud Service -> Modular Input
  - Location data & metrics (speed, rpm, etc)

The Data: Track Day



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

Refer to namespaces:

```
$submitted:driver$
```

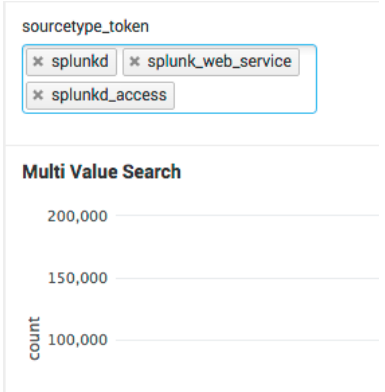
- `$form.mytoken$`
  tokens contain raw form input
- `$mytoken$`
  after applying prefix, suffix, default value

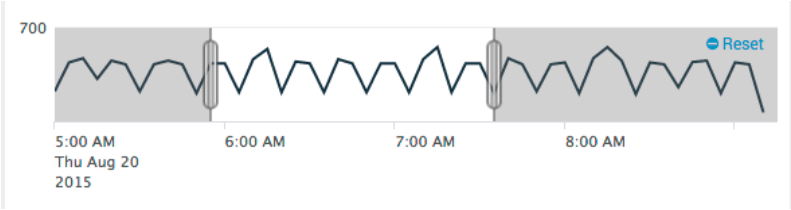
Building Dashboards

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

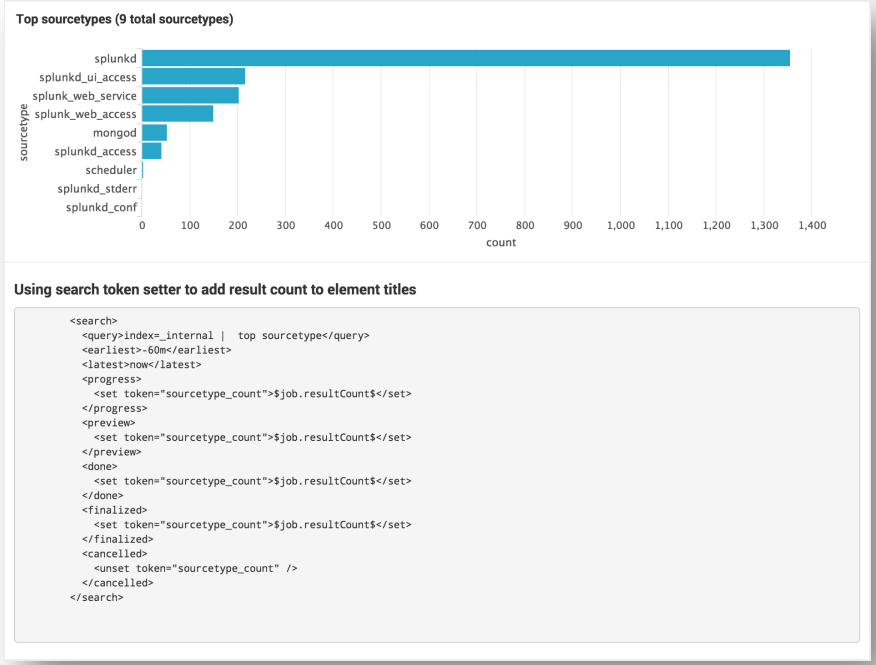
- Control whether you hide or show a given object based on existence of a token
  - Contextual (in-page) Drilldown
  - Cascading Form Inputs
- Applies to element, row, panel, input objects
- Type
  - `<table depends="$show_table$">`
    - Hide by default, show when token(s) exist
  - `<table rejects="$hide_table$">`
    - 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)
  - 1st result
- Eval-based condition/value support



Wrap-Up

What's New in 6.5

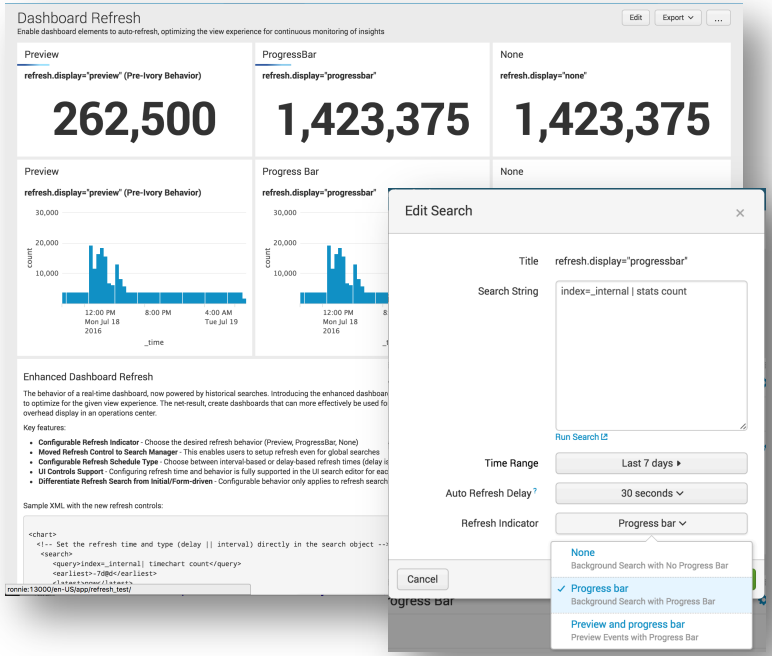
- Search Refresh & RefreshDisplay
- Initial Page Load Controls
  - <init> event
  - Global environment variables
- Token Filters
  - For "No Encoding", use $token|n$

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



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

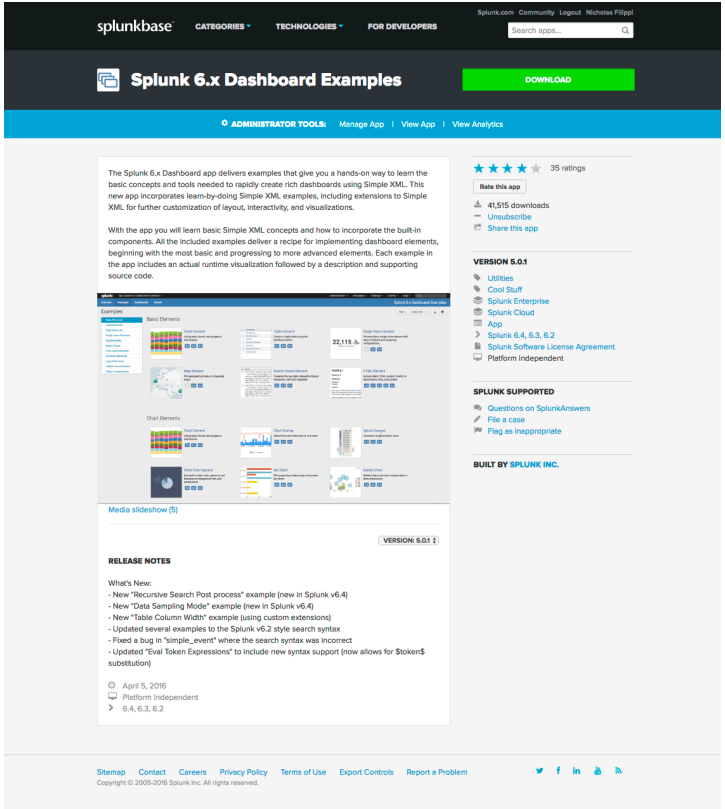
  https://splunkbase.splunk.com/app/1603/

- 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



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

splunk>