Go From Dashboards to Applications With Ease

SplunkJS and Splunk Python for Non-Developers

David Veuve | Splunk Security Practice
Dave Herrald | Splunk Security Practice

Forward-Looking Statements

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.

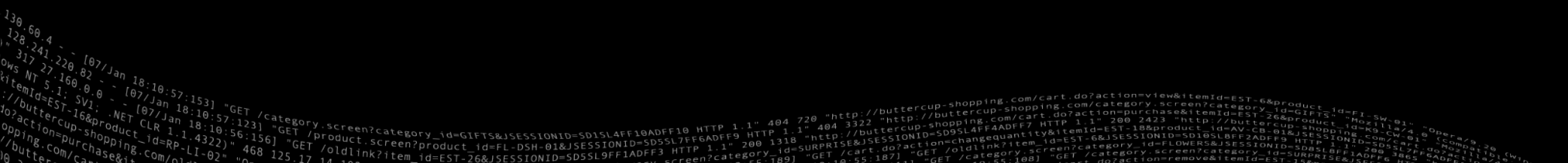
splunk> .conf18

Agenda

- Introductions – Who Are We, Who Are You?
- The App
- The Meat
  - Running a Search from SplunkJS (Veuve)
  - Tokens for adequate interactivity (Herrald) (Or other content.. Maybe a simple python something?)
  - Modal Dialogs (Veuve)
  - … (Herrald)
  - Our Top 5 Techniques for Making an App Great (Both)

What Is This Talk About?

- We have built a lot on top of Splunk
- We don't know what we're doing
- We've suffered
- We don't want you to suffer
- We put all our lessons learned in an app, and this talk accompanies the app



Introductions

Who Are We?

David Veuve

- He wrote the 5th most installed Splunk App: Splunk Security Essentials
- He also wrote the cult classic Splunk App: Search Activity
- He's presented 8 talks, 11 times to more than 2800 Splunkers @ .confs
- He just hit his 10 year anniversary of using Splunk

Dave Herrald

- More than 8,000 people have used his BOTS Scoring app
- He's built the most secure Splunk app on record
- He's presented at X SANS events and is super good at Security
- Splunk won't stop giving him awards for being awesome at Splunk

Why Are We Here? Because We Believe

- We believe that Splunk is an awesome development tool
- We believe that Splunk dev documentation is for people smarter than us
- We believe in maintaining state
- We believe in a great application experience
- We believe in being friends with people who understand UX design

- But above all…
- We believe in Copy-Paste Code Samples

Who Are You?

You're A Dashboard/Search Wizard

- You want to make better things
- You've probably copy-pasted code
- Maybe you've even written some code yourself!
- You're scrappy and want to impress people

You're a Software Engineer

- You know how to code
- You know how to read docs
- You want to save yourself a *ton* of energy with a quick start

Goal

- You should understand the essentials of doing Splunk Development with SplunkJS and Python
- You should understand how to leverage the app we are providing
- You should feel comfortable that you'll be able to do great things

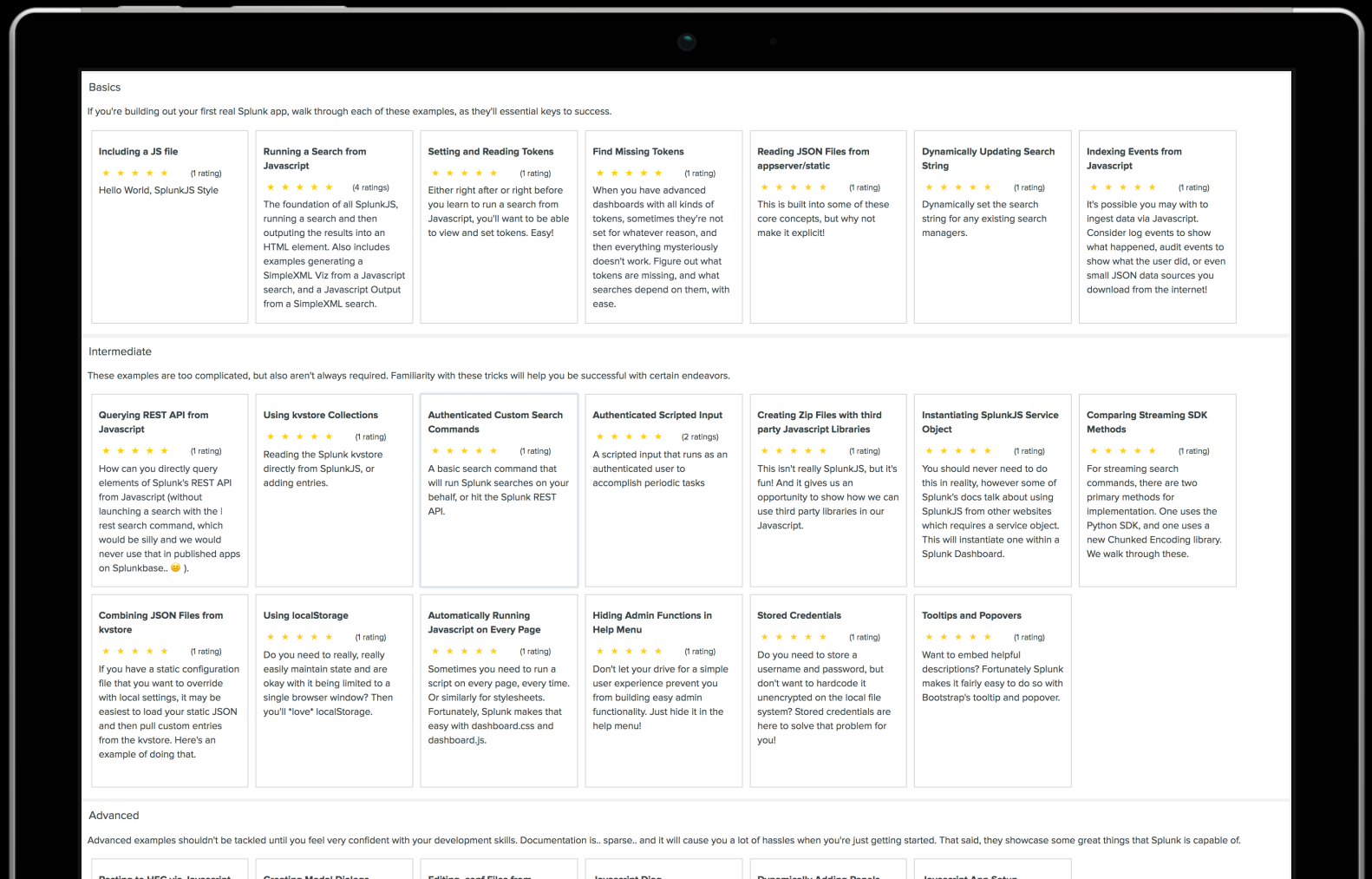
The App

Get The App

https://splunkbase.splunk.com/app/4104/

splunk> .conf18

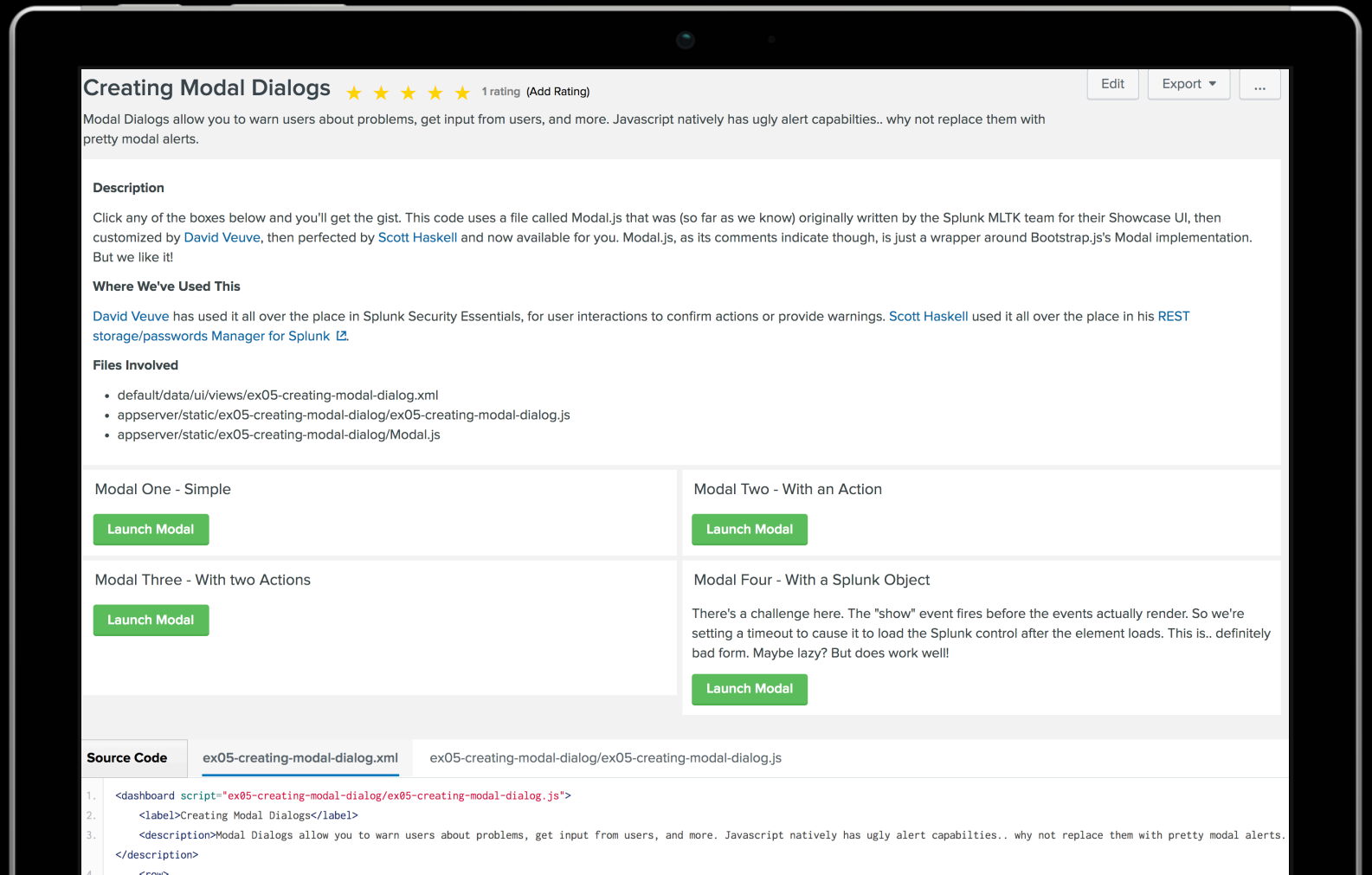
30+ Examples



- Guidance
- Basic
- Intermediate
- Advanced

splunk> .conf18

In Each Example...



- The JS / CSS
- Description
- Where we've used it
- Doc links
- Rating
- Working examples you can interact with
- (A few) detailed "how would you learn this" guides

splunk> .conf18

What's In The App?

As of this slide being built… conf is still weeks away!

Guidance

- Setting Up Your Development Environment
- Powerful Third Party and jQuery Plug-ins
- Splunk Style Guildelines (and Icons and such)
- Logging and Debugging

Basic

- Running JS
- Running a Search from SplunkJS
- Setting and Reading Tokens
- Find Missing Tokens
- Reading JSON Files from appserver/static
- Dynamically Updating Search String
- Indexing Events from Javascript
- Automatically running Javascript on Every Page

Intermediate

- Querying REST API from Javascript
- Using kvstore Collections
- Authenticated Custom Search Commands
- Authenticated Scripted Input
- Creating Zip Files with Third Party Javascript Libraries
- Instantiating SplunkJS Service Objects
- Comparing Streaming SDK Methods
- Combining JSON files with kvstore
- Using localStorage
- Hiding Admin Functions in Help Menu
- Stored Credentials
- Tooltips and Popovers

Advanced

- Posting to HEC via Javascript
- Creating Modal Dialogs
- Editing .conf Files from Javascript
- Javascript Diag
- Dynamically Adding Panels
- Javascript App Setup

splunk> .conf18

Running A Search from SplunkJS

Code Example

First The Basics - SplunkJS

splunk> .conf18

Require.js

- Require.js allows you to import modules – the equivalent of:
  - Perl: use HTTP::Simple;
  - Python: import json
  - Etc
- You take the code that you would normally write, and you just stick it in a require function:

```
require(["jquery", "splunkjs/ready!"], // run once view loaded
        function($, Ready) {
            $("body").append("<p>Hello World!</p>");
        }
       )
```

Search Manager

- Search Managers let you .. Manage searches. Run, edit, etc.

```
require(["splunkjs/mvc/searchmanager"], function(SearchManager) {

    // New Search
    var sm = new SearchManager({ [...]},
      { tokens: true, tokenNamespace: "submitted" });

    // Load Search
    var other_sm = splunkjs.mvc.Components.getInstance("search2")

    // Delete Search
    splunkjs.mvc.Components.revokeInstance("search2")

    // Test if Search Exists
    typeof splunkjs.mvc.Components.getInstance("search2") == "object"

})
```

splunk> .conf18

There Are Many Useful Classes

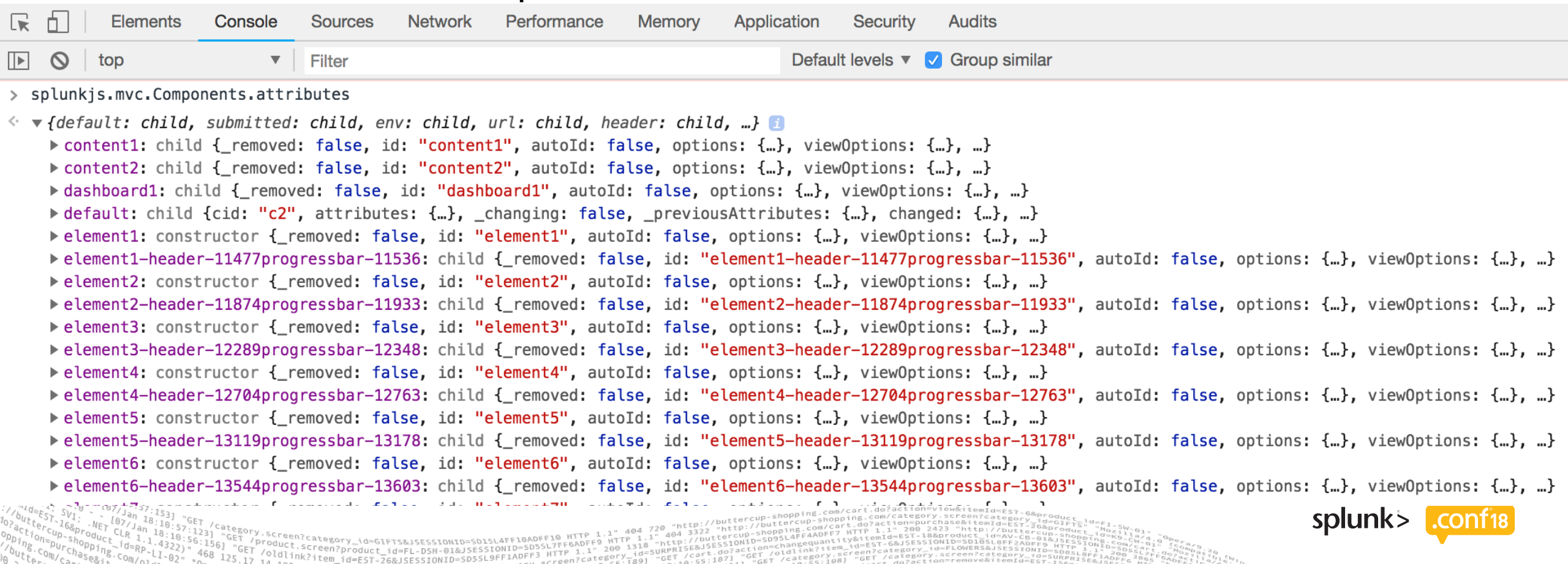
Here are a list of classes, and how the typical name they're loaded with

- "jquery" -> $
- "underscore -> _
- "splunkjs/mvc/dropdownview" -> DropdownView
- "splunkjs/mvc/textinputview" -> TextInputView
- "splunkjs/mvc/chartview" -> ChartView
- "splunkjs/mvc/tableview" -> TableView
- "bootstrap.tooltip" -> N/A (put it at the end, no object required)

- How to discover these? Easiest – put the element on an SimpleXML Dashboard and convert to HTML

Discovering Objects

- Every instantiated object is stored in: splunkjs.mvc.Components.attributes
- Find this in the Javascript Console:



splunk> .conf18

Loading Custom JavaScript

- Add a script tag to your dashboard tag:

```
<dashboard script="myscript.js">
   [...]
</dashboard>
```

- myscript.js will automatically load from: $SPLUNK_HOME/etc/apps/myApp/appserver/static/myscript.js
  - Any other resources you need can also be stored in that folder, or in subfolders.
- You can verify the file is there by going to: http://mySplunk:8000/static/app/myApp/myscript.js
  - .. Which adds language automatically: http://mySplunk:8000/en-US/static/app/myApp/myscript.js

Okay, enough with the basics
Let's run a search!

splunk> .conf18

Demo Plan

- If you're reading this slide, you're looking at the PDF copy. That means you're missing out!
- What are you missing out on? Well, a 4 minute demo. And in that demo I will do a:
  - Quick SA-jsforall App Demo
  - Create a new Simple XML Dashboard with an HTML element and an empty div
  - Add a Script Tag
  - Create a new Javascript file
  - Copy-paste the code example from ex01 that will output the first event
  - Save, debug refresh and _bump
  - (Discuss how you don't have to do that)
  - (Discuss how splunkd sometimes doesn't _bump on app updates because splunkd can be obnoxious)

Herrald Example 1 (Tokens? Python Basics?)

Code Example

splunk> .conf18

Creating Modal Dialogs

Code Example

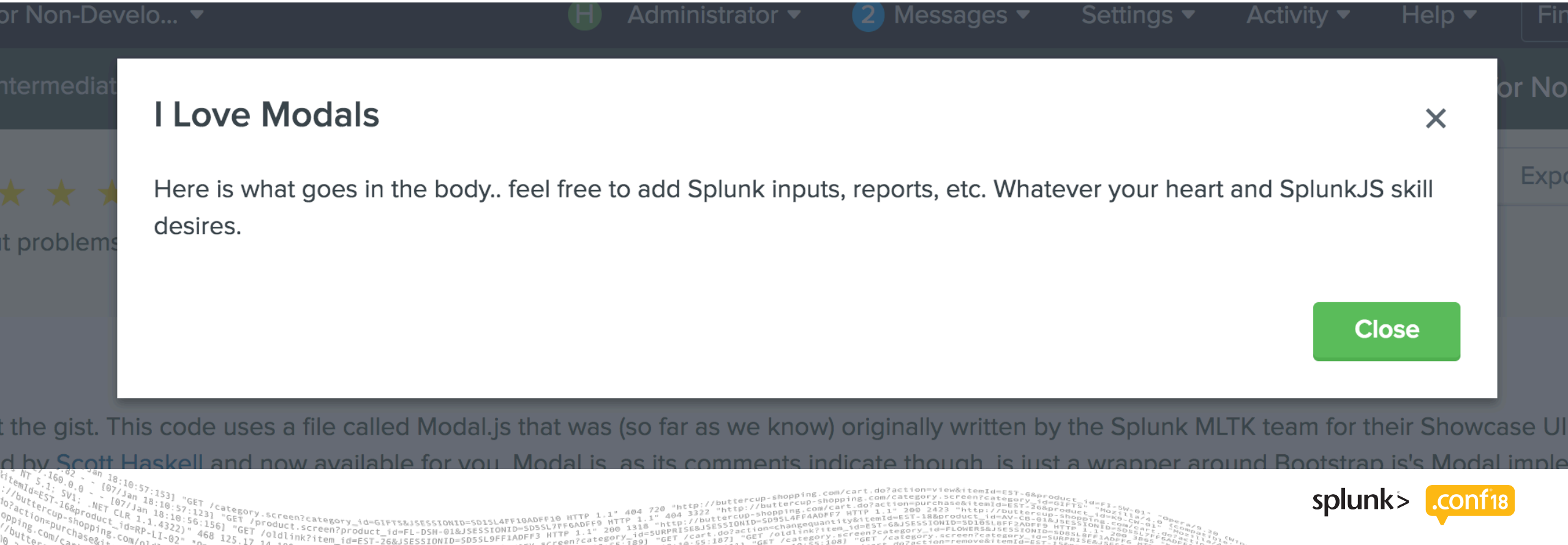
splunk> .conf18

First The Theory

splunk> .conf18

What is a Modal?

- A modal is fully known as a Modal Dialog. It's a box that pops up on the screen and confirms, asks for details, etc.
- In other words, it's one of these:



Modals Come From Bootstrap

- Bootstrap.js ships with Splunk, and it does all the really heavy lifting here
- We *do* need to create a new object for the modal, though.
- We'll create a new file (well, copy-paste from the app) and load via require

Modals have actions

- You can do things on modal hide (start of hide action), on modal hidden (end of hide action), etc.
- You can also add buttons to modals.

Let's Do It!

splunk> .conf18

Demo Plan

- If you're looking at this slide, you're viewing the PDF copy of the slides. That means you're missing out on the demo again!
- In this demo, I will start with a SimpleXML dashboard to add a new item into a threat intel dashboard – a text form input, and then a <button> that calls "addElement()"
  - Have a comment which includes the search string that should be run
  - Have a panel that includes the current # of elements and the last element added
- Copy-paste example from the app to create a confirmation modal
- Copy-paste example from the app to run a search if the user clicks Yes

Herrald Example

Code Example

Top 5 Elements for a Great App

splunk> .conf18

#5 – Use Modals

- Modals are really easy to use
- They provide a more polished user experience and more interactivity

- You can even include Splunk dashboard elements in them (dropdowns, charts, etc.)
  - Trick: you may need to add a setTimeout or add them after the modal finishes rendering

#4 - Herrald

splunk> .conf18

#3 – Maintain State

- An application remembers what you've done before
- An application does not repeatedly prompt you for the same information

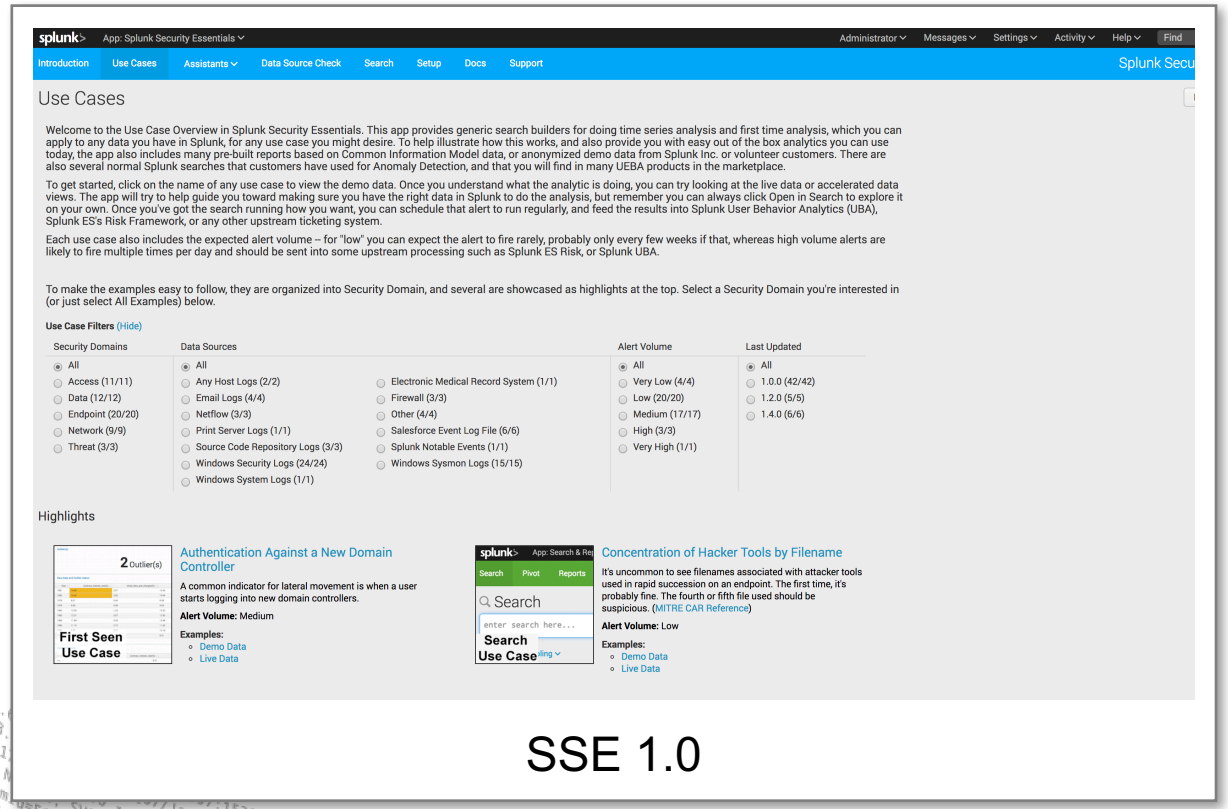
- There are several great methods for maintaining state:
  - Locally in the browser via localStorage
  - By accessing the kvstore
  - Even storing details in a macro or lookup

#2 - Herrald

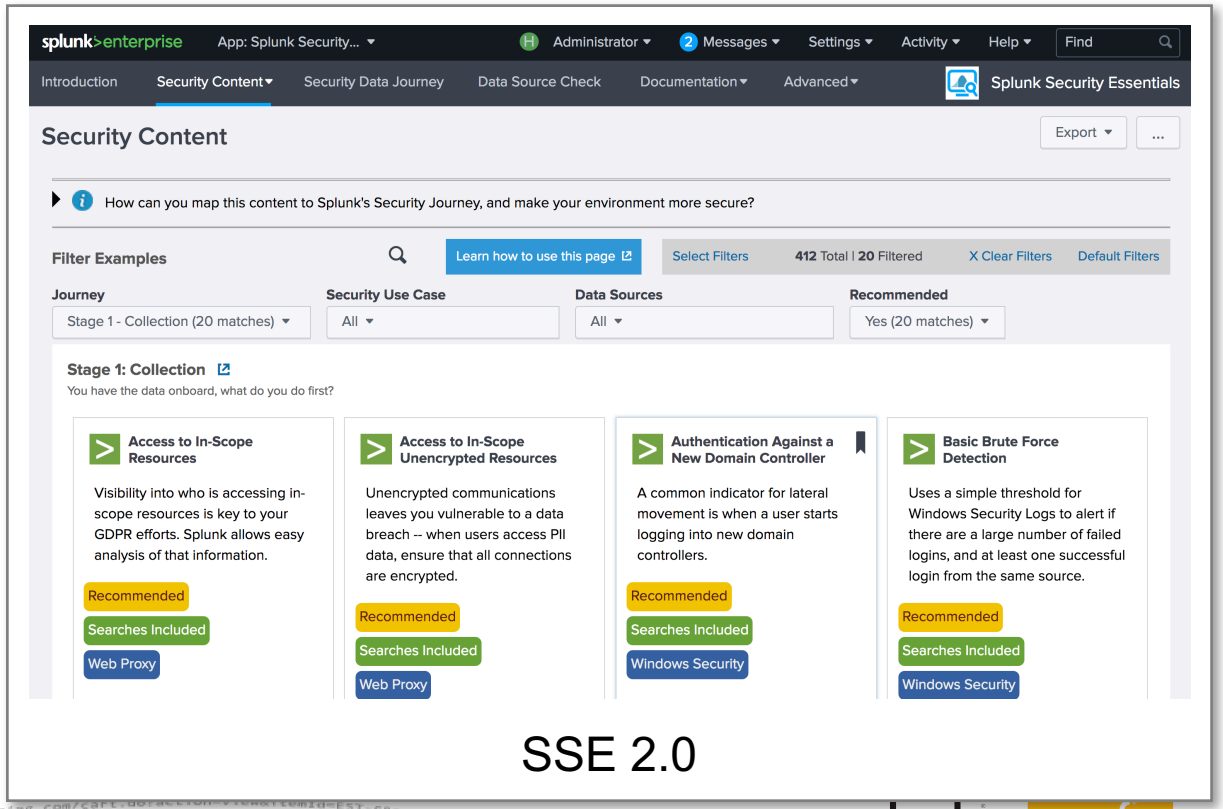
splunk> .conf18

#1 – Get Design Help

- If you aren't good at design, ask someone who is.
- If you don't know someone, buy some time on fiverr.com, upwork.com, etc.
  - $300 spent on outsourced design can net you a promotion



SSE 1.0



SSE 2.0

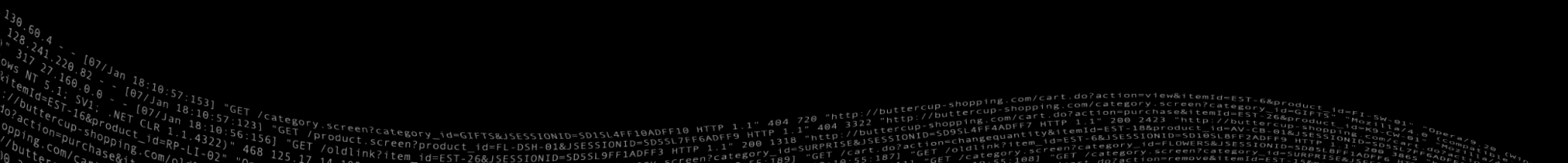
Key Takeaways

Download the app!

https://splunkbase.com/app/4104

Making more interactive and powerful UIs is easy

If you find content like this useful, please rate us in the app so that Splunk provides more content like this.



splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app