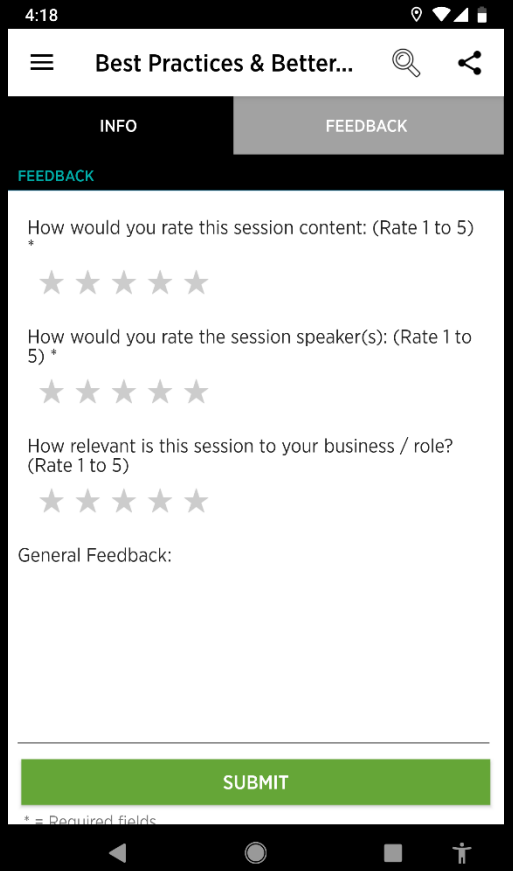
Best Practices and Better Practices for Admins

…while you get settled…

- Latest Slides:
  - https://splunk.box.com/v/conf18-coe
- Collaborate: #bestpractices
  - Sign Up @ http://splk.it/slack
- Load Feedback ---------->



Best Practices and Better Practices for Admins

Building a Best Practiced Deployment (CoE)

Burch | Manager, Product Best Practices

.conf18 > Presented by Splunk's Digital Customer Success

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

What's a "Burch"?

Manager, Product Best Practices

- Education: Comp Sci + MBA
- Werk: Middleware Eng

- Splunk Customer since 2012
  - Admin for four environments
  - This is based on a true story…

- Splunk Employee since 2014
  - Sales Engineer
  - Best Practices Engineer
  - "Best Practiced Deployment" (CoE)

Scope = Difficult Concepts

http://conf.splunk.com/sessions/2017-sessions.html#search=burch

.conf2017

Best Practices and Better Practices for Admins

Best Practices and Better Practices for Users

Blueprints for Onboarding Teams

Creating Welcome Pages

Sandboxing with Splunk (with Docker)

Blueprints for Actionable Alerts

.conf18

Best Practices and Better **Practices** for Admins

Blueprints for Actionable Alerts

Best Practiced Deployment

A.K.A Center of Excellence

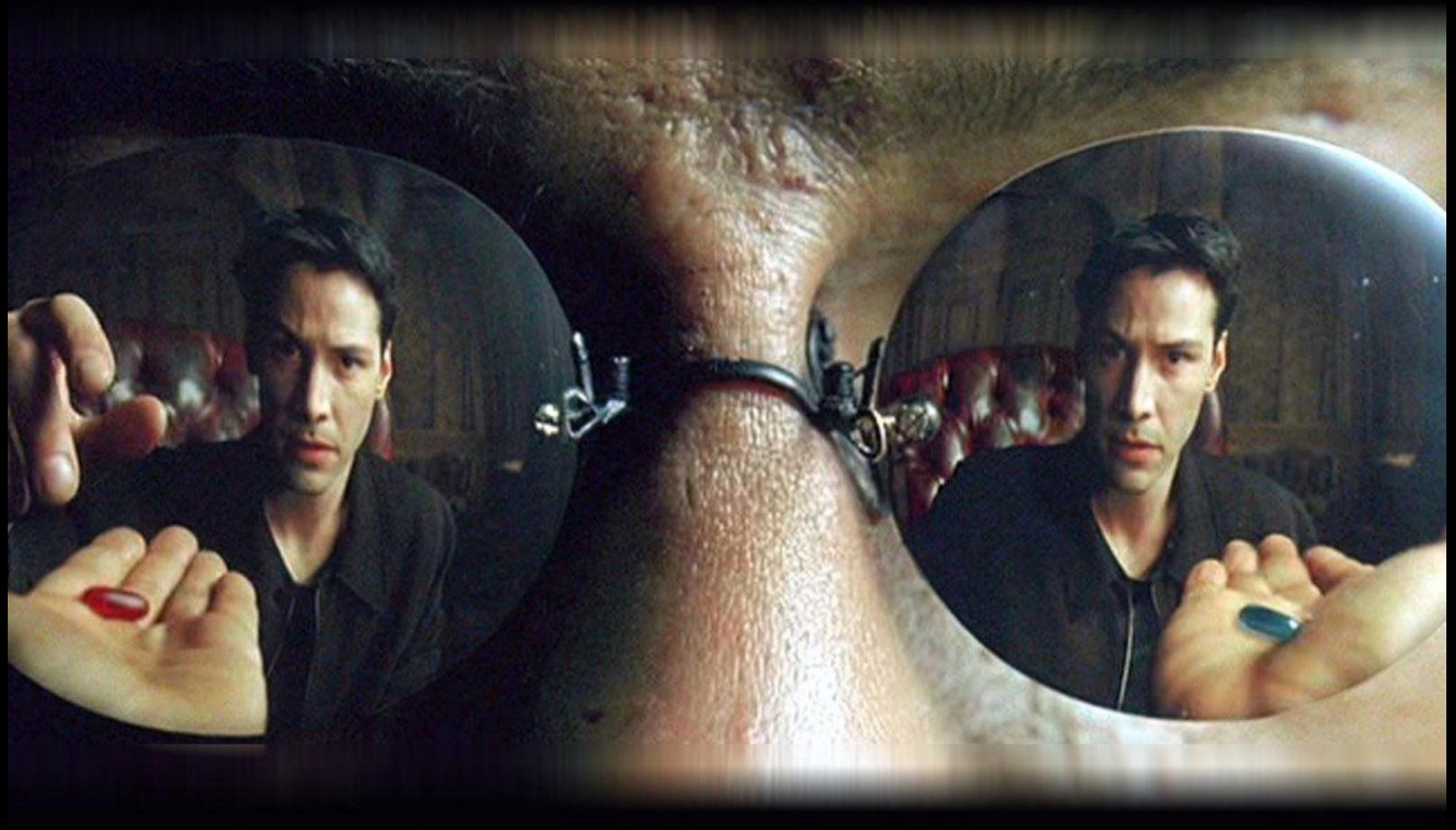
Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

Best Practices for a Best Practiced Deployment



Foundations

Best Practices for a Best Practiced Deployment

Practice Politics

Scope == Executive Sponsor

Charter

Executive Sponsor

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

User vs Team

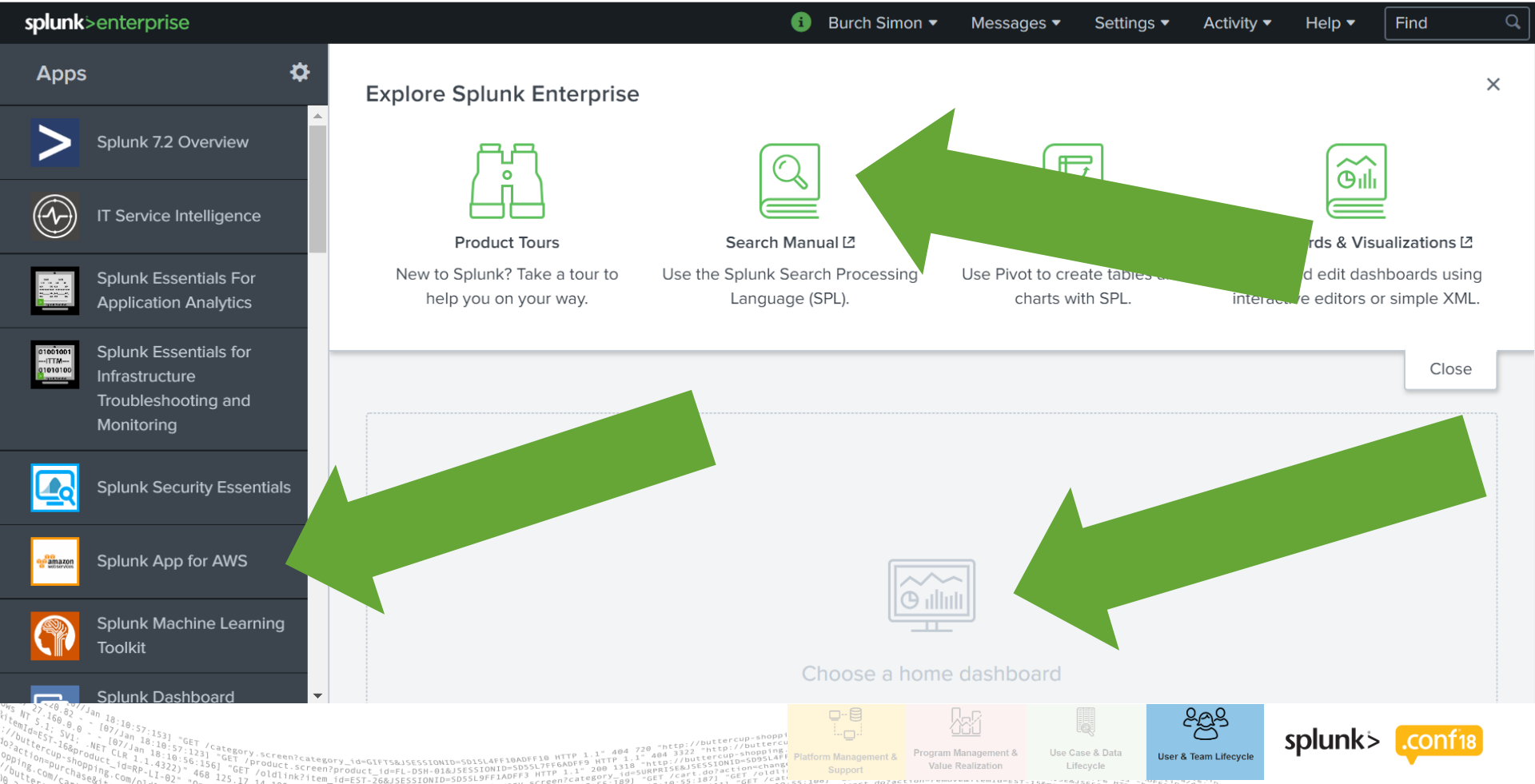
Who wants to role play?

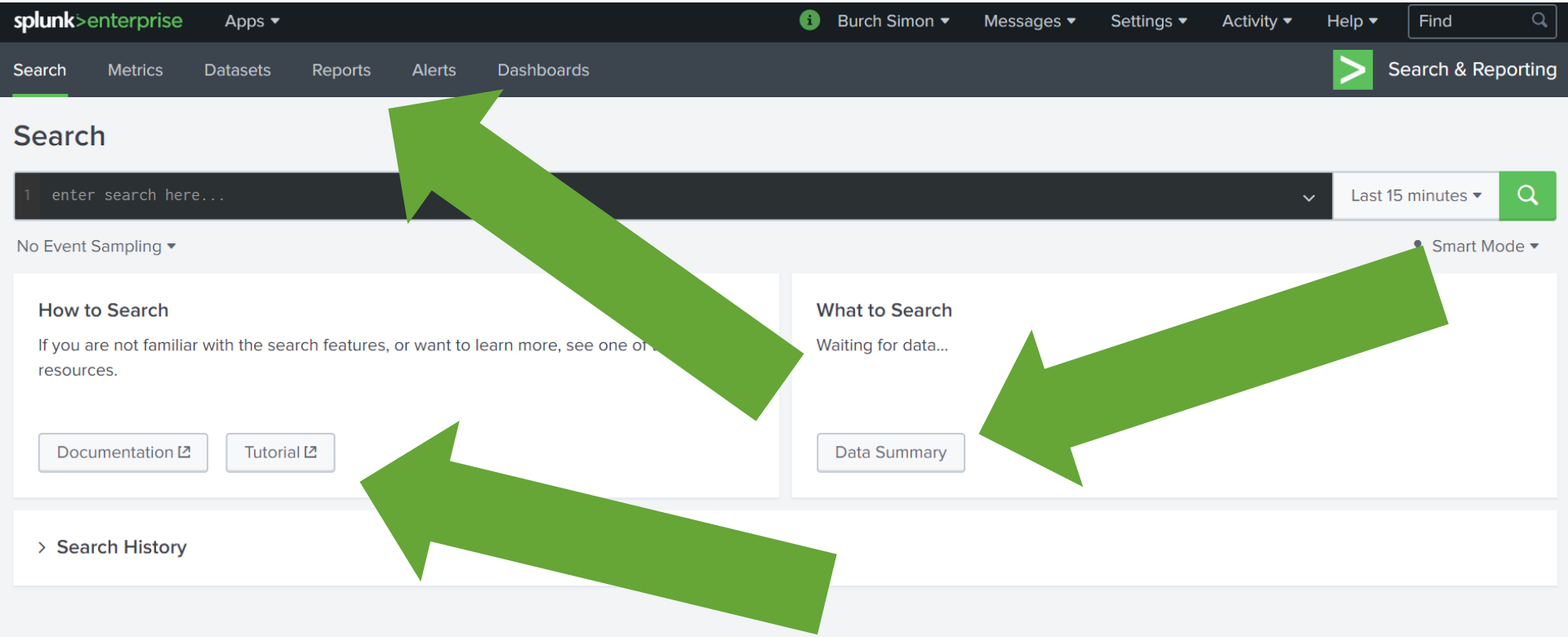
Choose Your Own Adventure!

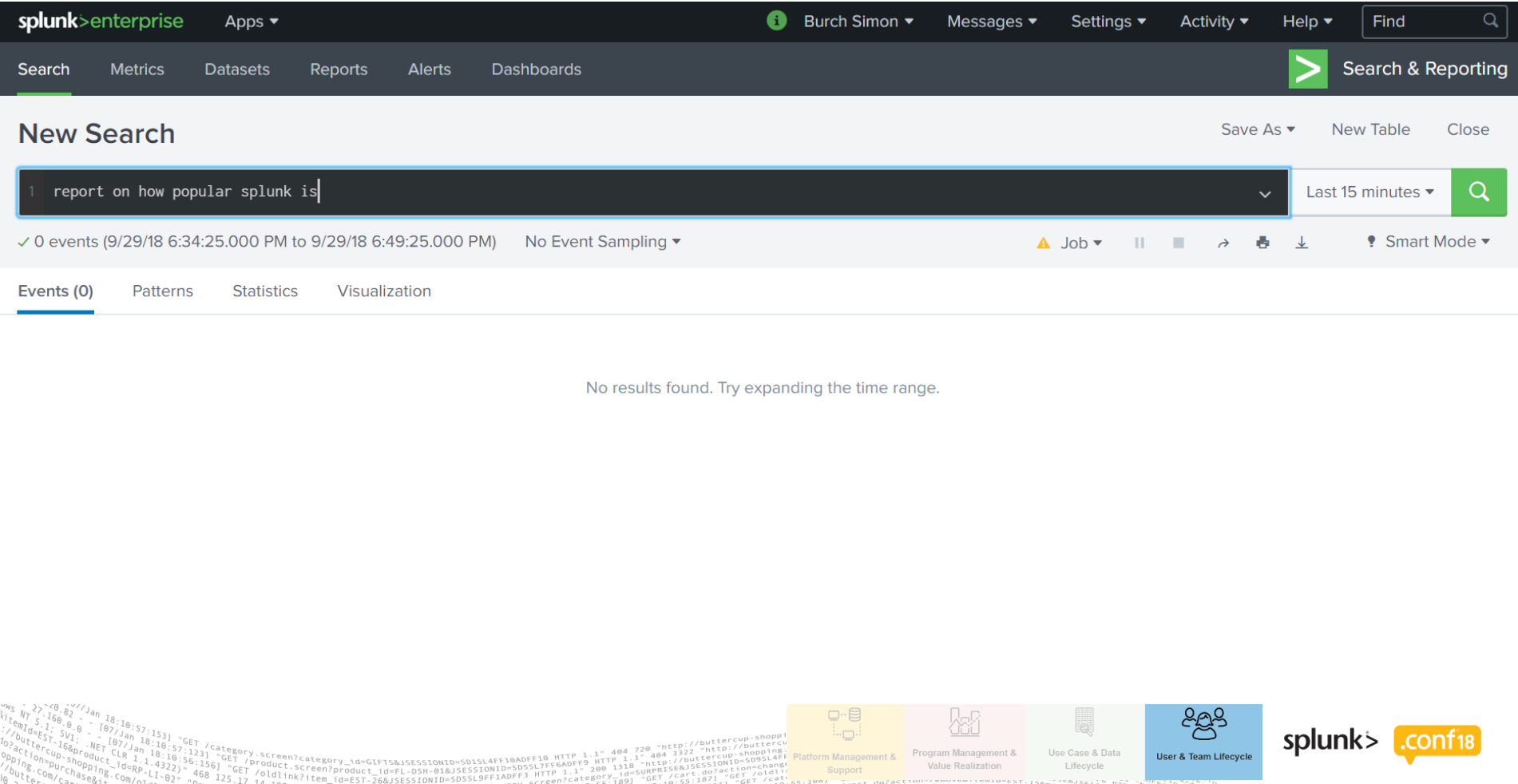
splunk> .conf18

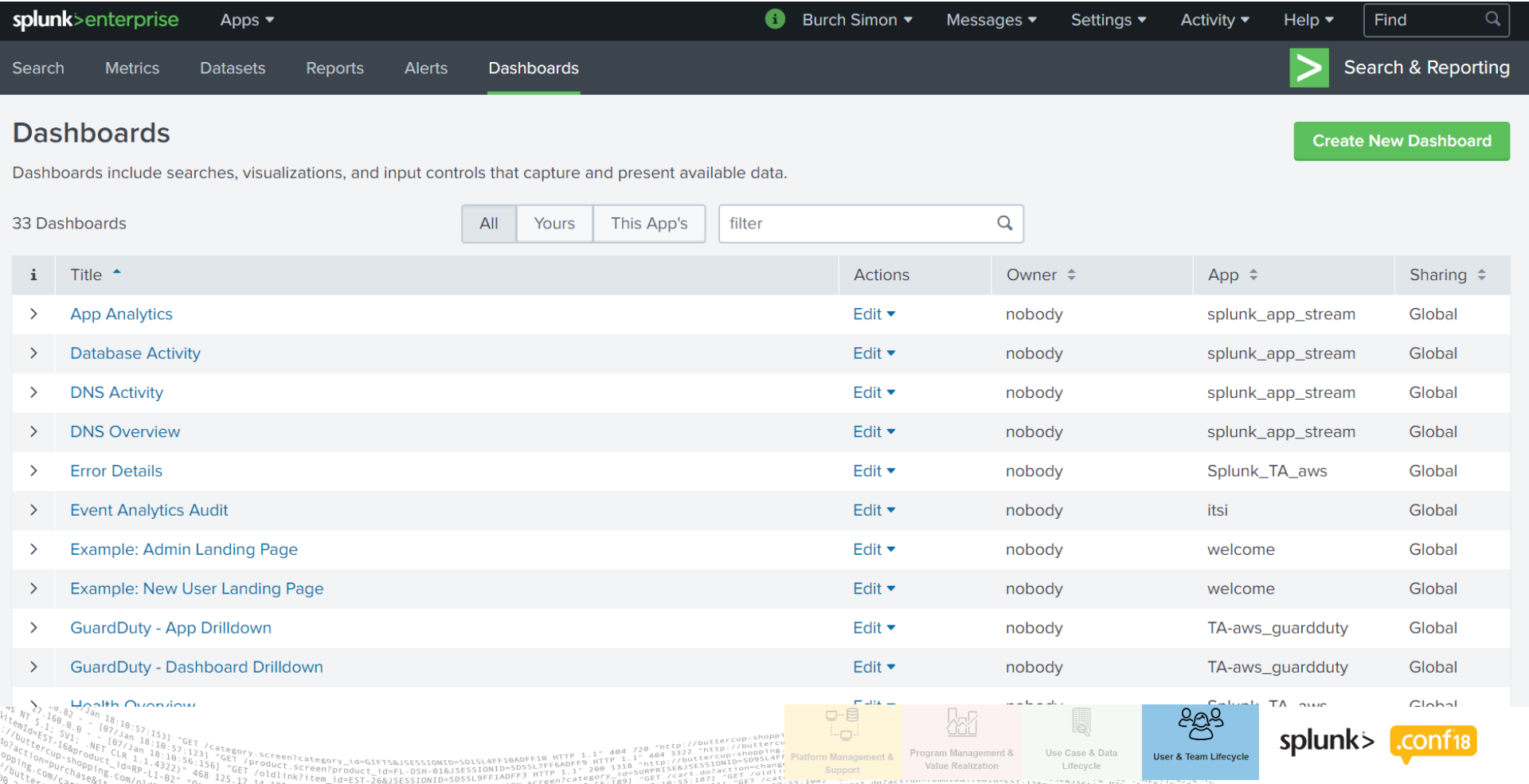
Scenario

- New employee at Buttercup Games
- Lied on your resume about Splunk experience (no experience)
- Company has no HR. Punishment is Pony Diaper Duty (pun intended)
- Given same Splunk access as peer.
- You log in to see…

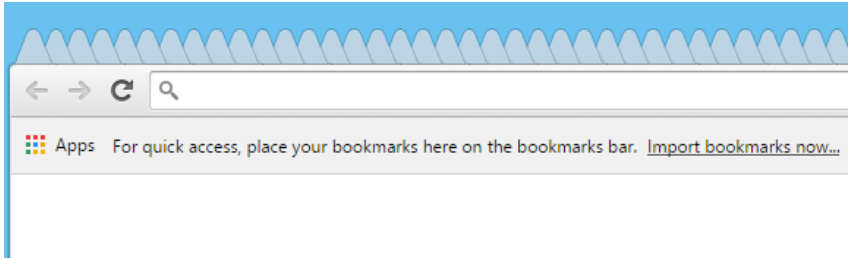


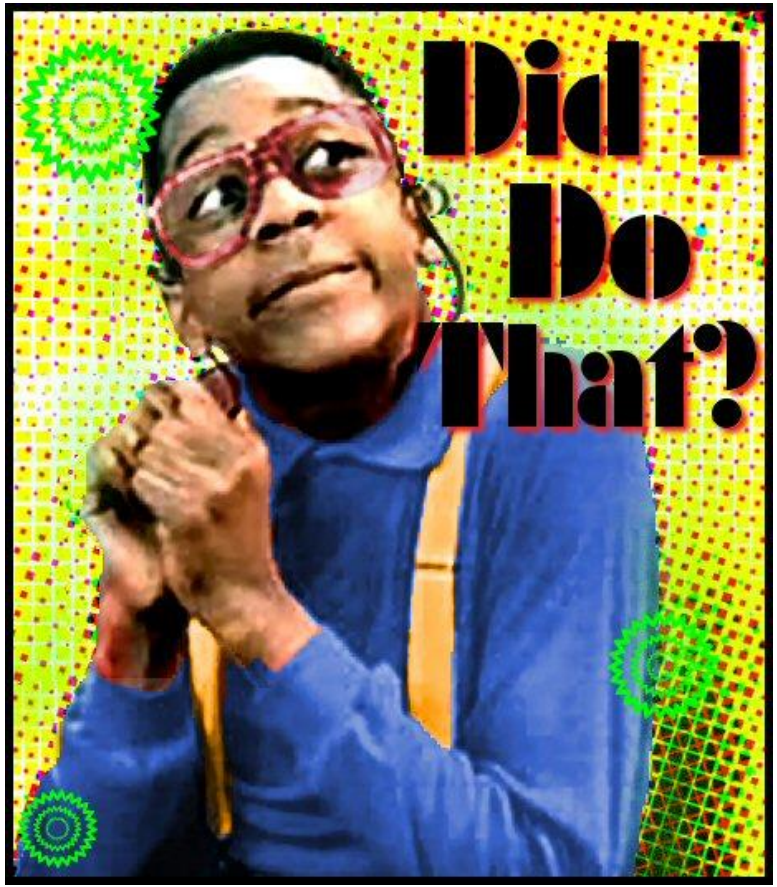


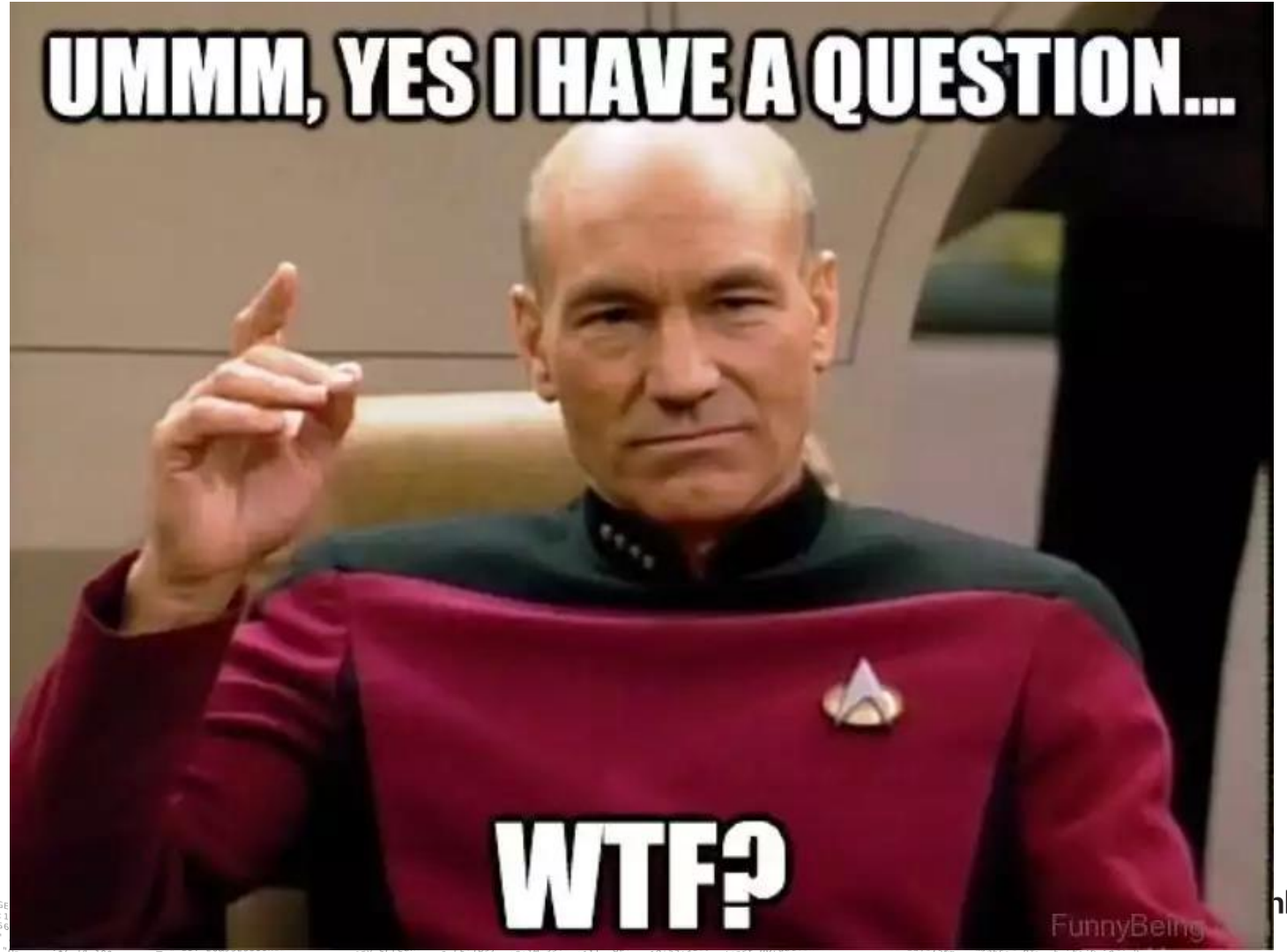




All the Dashboards!








I DEAL WITH THE G D DAMN CUSTOMERS
Doug M.
SO THE ENGINEERS DON'T HAVE TO


I DEAL WITH THE G D DAMN CUSTOMERS
D. Merritt
SO THE ENGINEERS DON'T HAVE TO

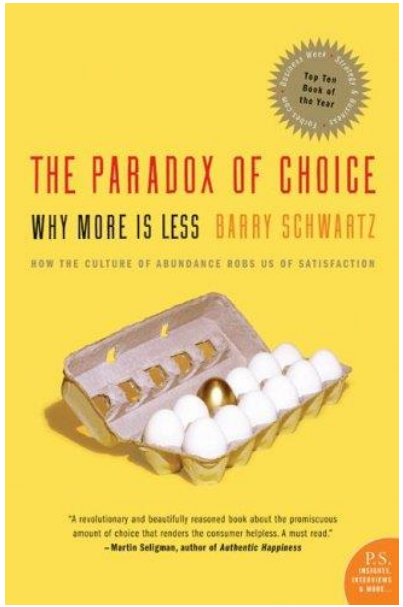

I DEAL WITH THE G D DAMN CUSTOMERS
index=*
SO THE ENGINEERS DON'T HAVE TO


Splunk Admin
You
Grand Moff Tarkin
Your throat
© 20th Century Fox

Solution, you have?!

The Paradox of Choice

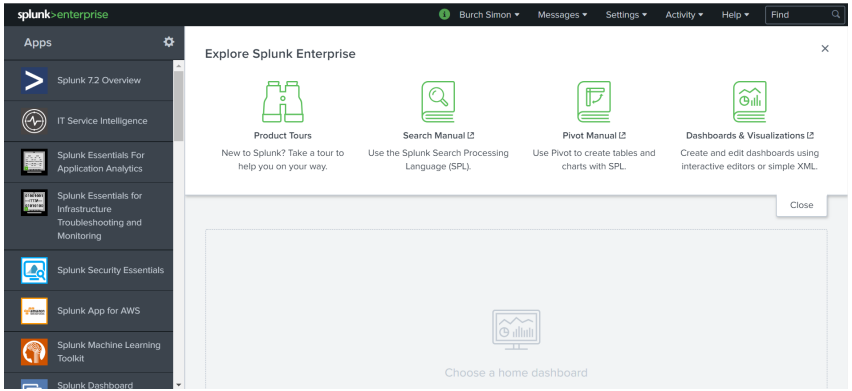
AKA Buyer's Remorse

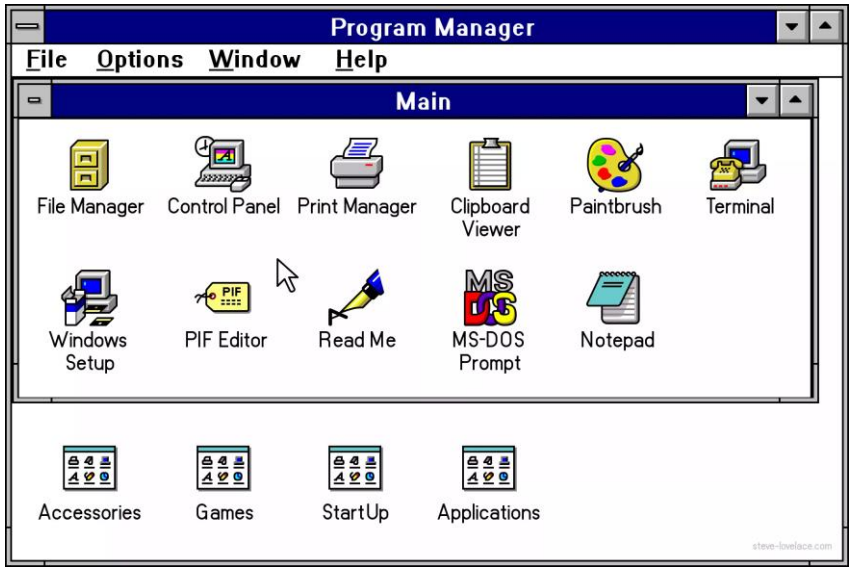


"eliminating consumer choices can greatly reduce anxiety"

Oh, the Places You'll Go

Too many options!





splunk> .conf18

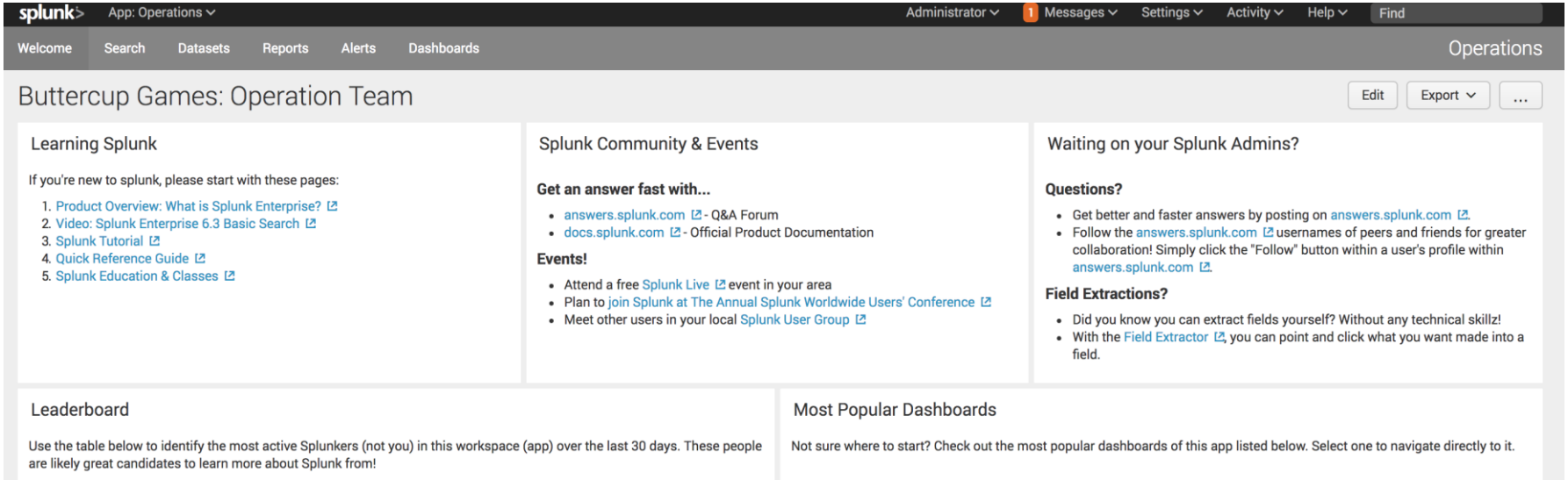
Same Challenge. Different Platforms.

What did this button do for user design?

- Mislead?
- Restrict?
- Guidance!
- Confidence!
- Comfort!

Eureka! Welcome Page!

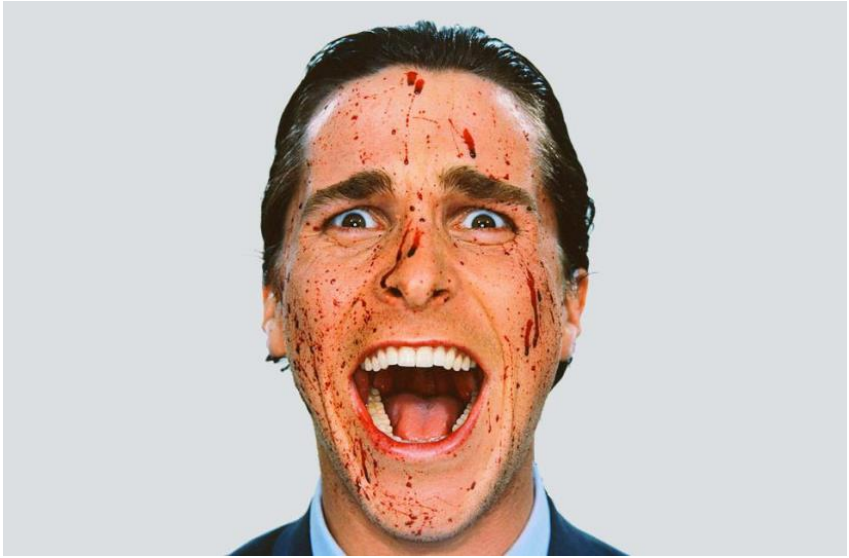
Effective material presented at every log in



Burch's Experience

Same questions and confusions over and over

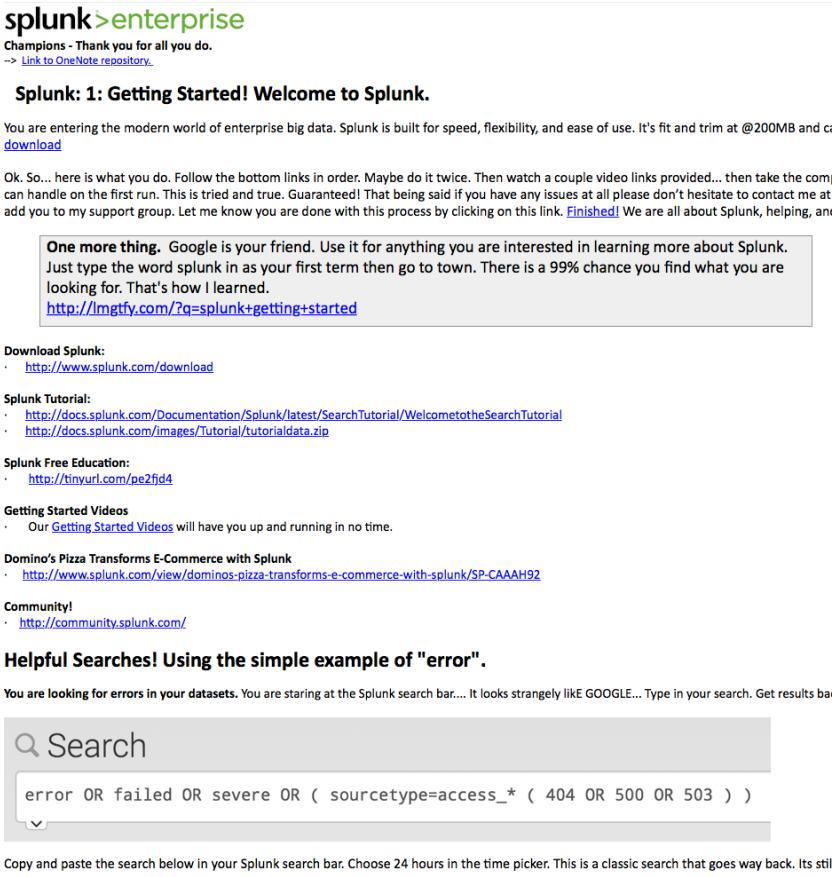
- What is Splunk?
- What report/dashboard to use?
- What data available?
- Want to learn more!



Welcome Email

Lost in their mailbox…

- Lost in their mailbox
- Static == Ineffective
- Requires effort from user



splunk>enterprise

Champions - Thank you for all you do.
--> Link to OneNote repository.

Splunk: 1: Getting Started! Welcome to Splunk.

You are entering the modern world of enterprise big data. Splunk is built for speed, flexibility, and ease of use. It's fit and trim at @200MB and ca
download

Ok. So... here is what you do. Follow the bottom links in order. Maybe do it twice. Then watch a couple video links provided... then take the com
can handle on the first run. This is tried and true. Guaranteed! That being said if you have any issues at all please don't hesitate to contact me at
add you to my support group. Let me know you are done with this process by clicking on this link. Finished! We are all about Splunk, helping, an

One more thing. Google is your friend. Use it for anything you are interested in learning more about Splunk. Just type the word splunk in as your first term then go to town. There is a 99% chance you find what you are looking for. That's how I learned.
http://lmgtfy.com/?q=splunk+getting+started

Download Splunk:
- http://www.splunk.com/download

Splunk Tutorial:
- http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/WelcometotheSearchTutorial
- http://docs.splunk.com/images/Tutorial/tutorialdata.zip

Splunk Free Education:
- http://tinyurl.com/pe2fjd4

Getting Started Videos
- Our Getting Started Videos will have you up and running in no time.

Domino's Pizza Transforms E-Commerce with Splunk
- http://www.splunk.com/view/dominos-pizza-transforms-e-commerce-with-splunk/SP-CAAAH92

Community!
- http://community.splunk.com/

Helpful Searches! Using the simple example of "error".

You are looking for errors in your datasets. You are staring at the Splunk search bar.... It looks strangely likE GOOGLE... Type in your search. Get results ba

Search

```
error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503 ) )
```

Copy and paste the search below in your Splunk search bar. Choose 24 hours in the time picker. This is a classic search that goes way back. Its stil

User Education & Enablement

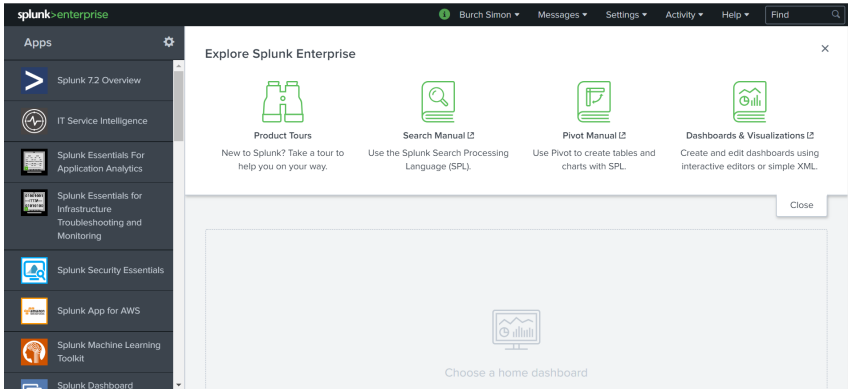
- Creating Content:
  - Teaching + Videos + Wikis
- Is that your core competency?
- Outsource it to us!
  - Capture unique things

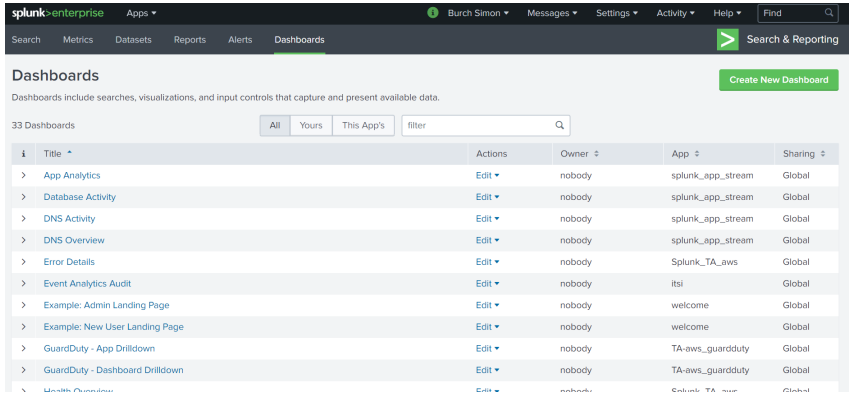
Workspace

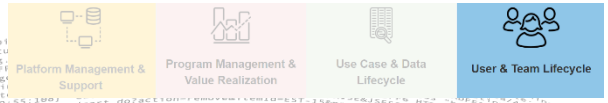
Do you keep everyone's work on everyone's desk?

splunk> .conf18

…so why do we do that in Splunk?



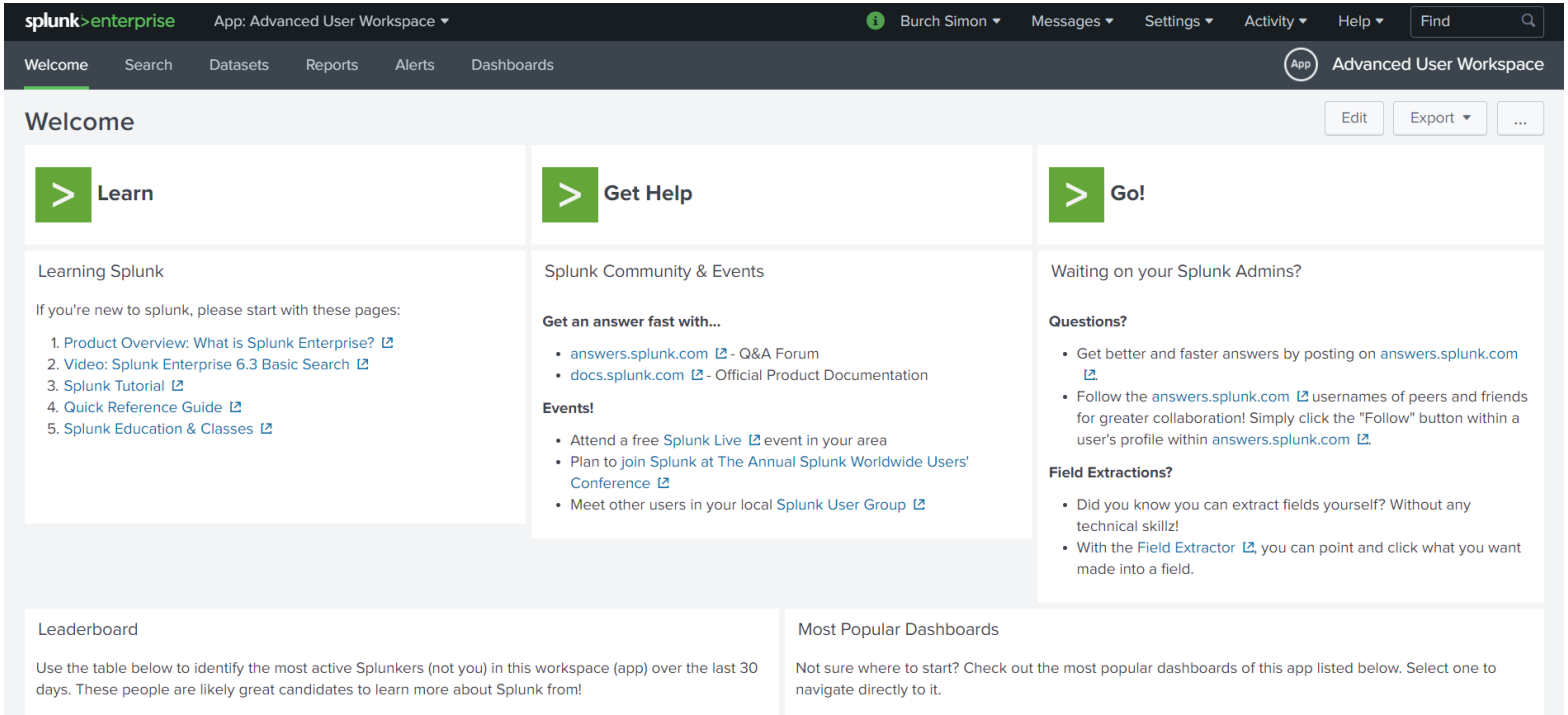


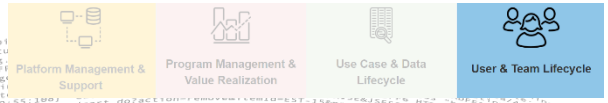


splunk> .conf18

App as a Workspaces

Dedicated to one team/group/purpose





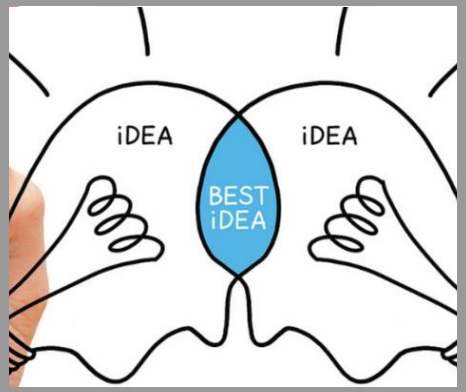
splunk> .conf18

Benefits

Increases in…

Safety

Risk led learning



Discovery led collaboration

Incentives

vs.

Is EDU Required?

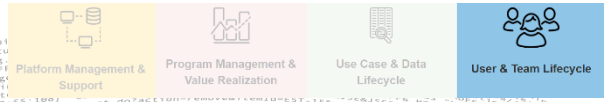
Training + Certification

Free Courses

- Free Splunk Fundamentals 1
- Splunk User Behavior Analytics
- Splunk Infrastructure Overview

Course Description

This course teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts. It will also introduce you to Splunk's datasets features and Pivot interface.

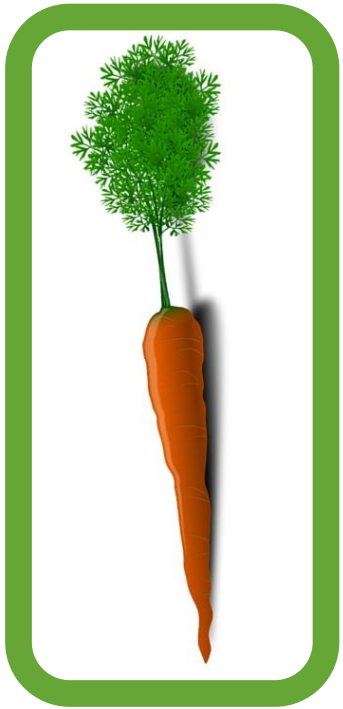


splunk> .conf18

“Yea, I took education”

“But I didn’t care, nor pay attention”

Incentives



vs.

Alternative Approach: No Requirements

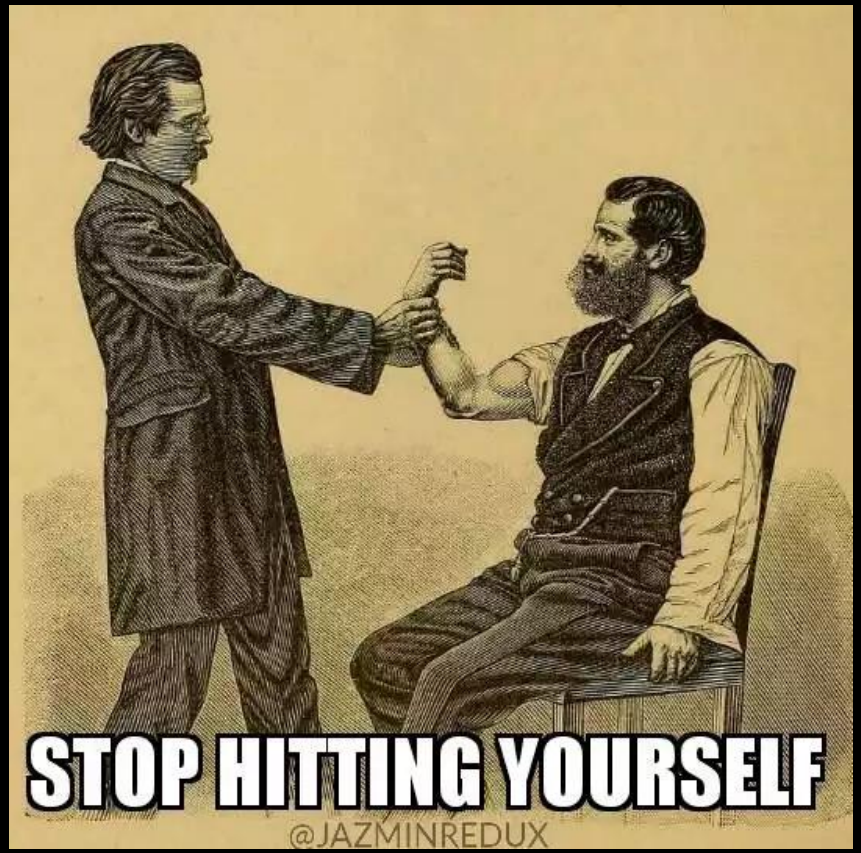
But limited impact…

You can't stop splunk-thusiasm…

…so shape it in your favor!

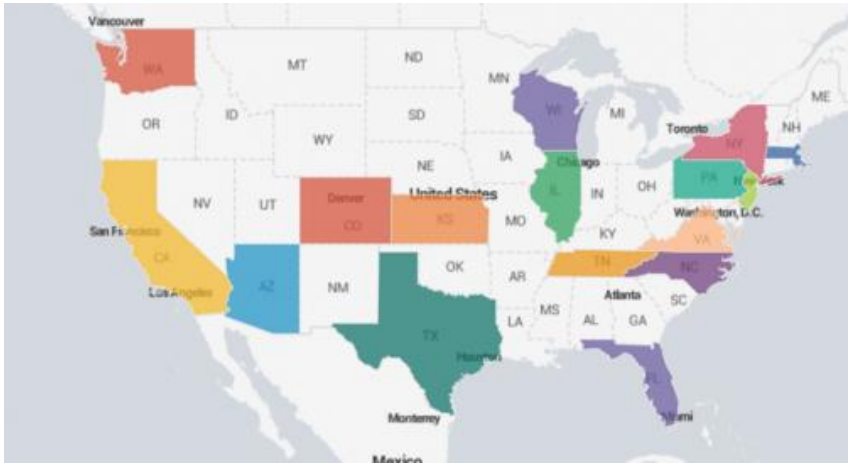
Incentive Driven User Onboarding

- “I can’t believe those users did those things I let them do!”
- Don’t be a data butler
- Identify & coach & promote to power
- Work with you to implement and learn best practices



Result

Curiosity and exploration




```
| makeresults
| eval curiosity="high"
| eval learning = if( curiosity=="high" , "success" , "datscooltoo" )
```

Rinse & Repeat

Admin Teachers Power User

Power User Teaches User

Result

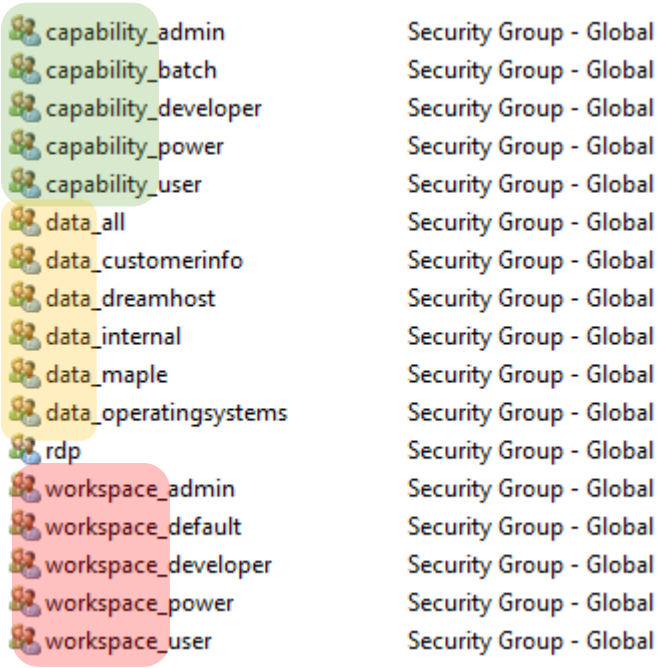
At first, more questions. Later, more disciples.

Clearly, now the fish can catch it’s own man…

Know thy Role?

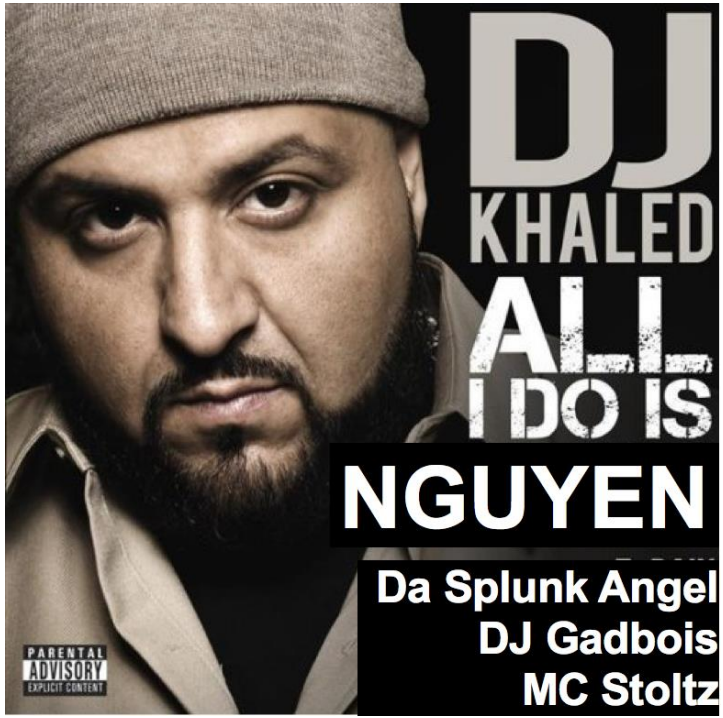
English vs Splunk

- Data Access
- Search Retention
- Product Feature Capabilities
- Knowledge Object Permissions
- Default App



Sub-Concept: For The Nguyen (FTN)

Separate Roles & Capabilities & Groups



The Standard

Prix Fixe Menu 25

(Choose one from each of the following)

First Course

Homemade Beef Chili
French Onion Soup
Caesar Salad
House Salad

Second Course

Southwest Chicken Egg Rolls
chicken, black beans, corn, pepper jack cheese,
red peppers and spinach, cajun ranch
Cajun Butter Pierogies –Lehigh valley live finalist
Sautéed in Cajun butter, caramelized
onions & sour cream
The Standard Wings
Original or Boneless
(Mild, Hot, Suicide, Sweet-n-Sweaty, BBQ, Cajun)
choice of ranch or bleu cheese.

Third Course

Creole Fish Tacos
Cajun seasoned cod, apple cider vinegar slaw,
cilantro, lime and chili aioli in soft shell tacos
Smokehouse Burger
cheddar cheese, bacon, BBQ sauce,
raw onion served on a brioche bun
Mac n Cheese
Three cheese and shells
Choice of Bacon Truffle or pulled pork

Fourth Course

Dessert of the day

splunk> .conf18

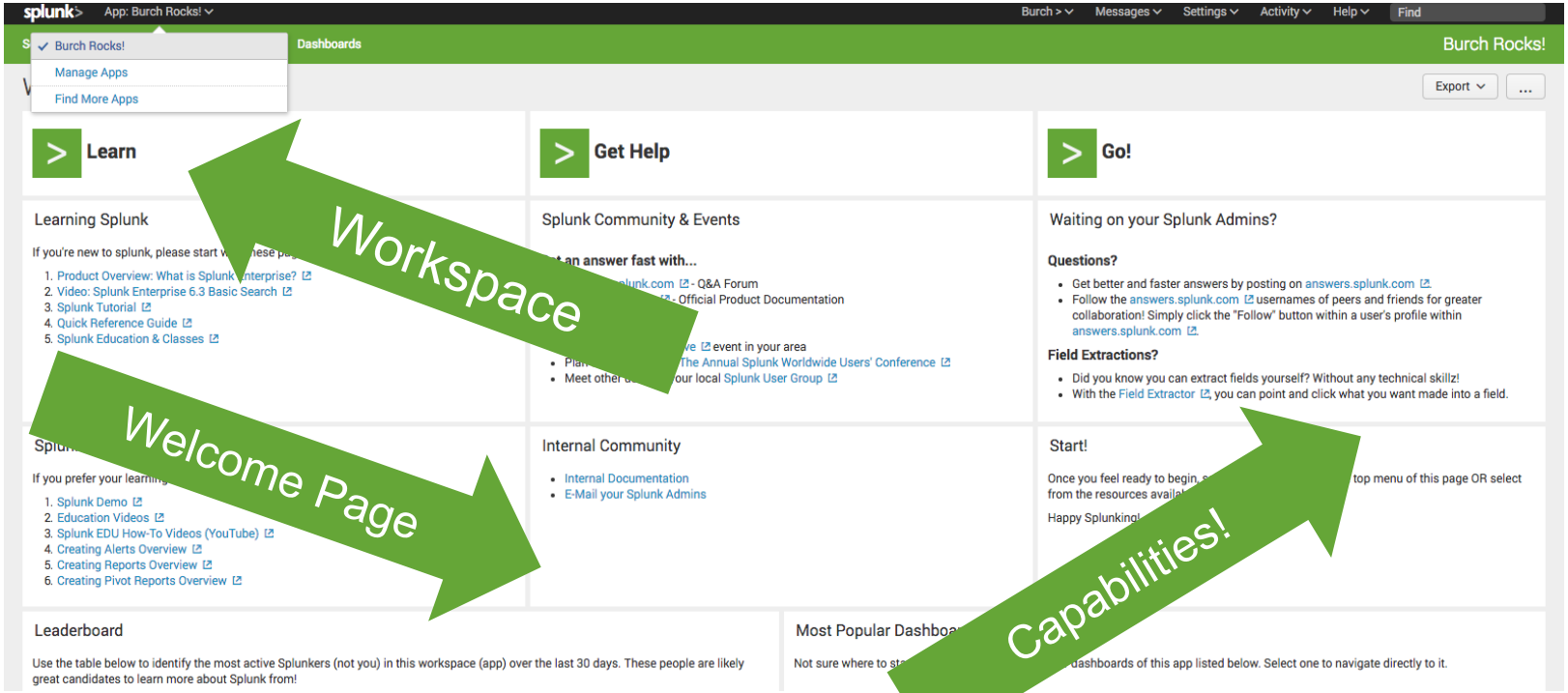
Scenario

REMIX

- New employee at Buttercup Games
- Lied on your resume about Splunk experience (no experience)
- Company has no HR. Punishment is Pony Diaper Duty (pun intended)
- Splunk Admins attended this session!
- You log in to see…

…only what you need

With clear information on where to go/learn next



splunk> .conf18

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

Tighter Coupling

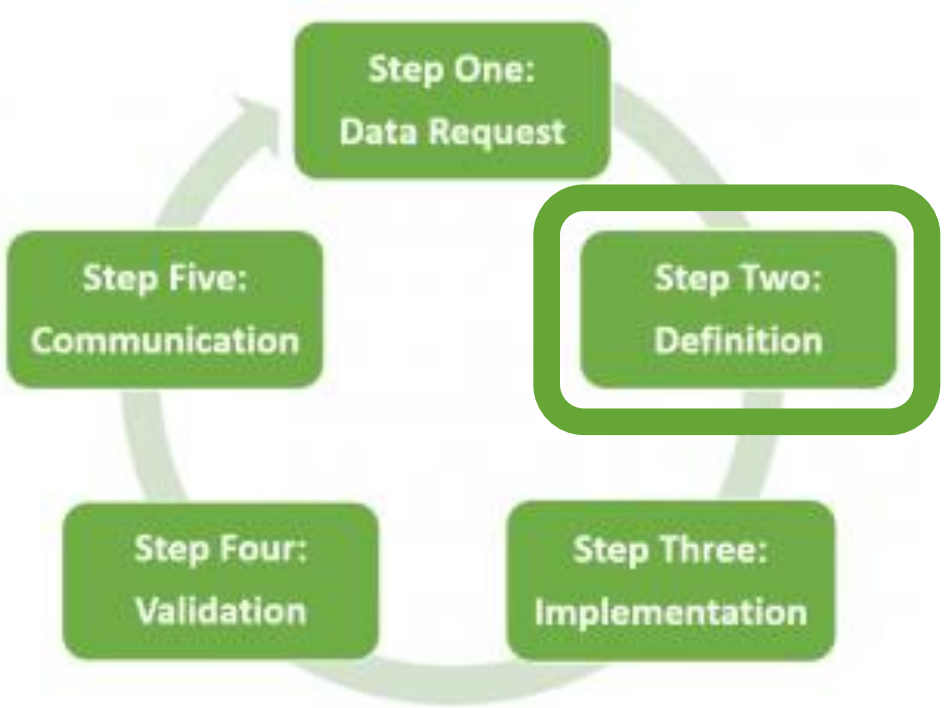
Use Case with Data

Tighter Coupling

Use Case with Data

Onboarding != Ingestion

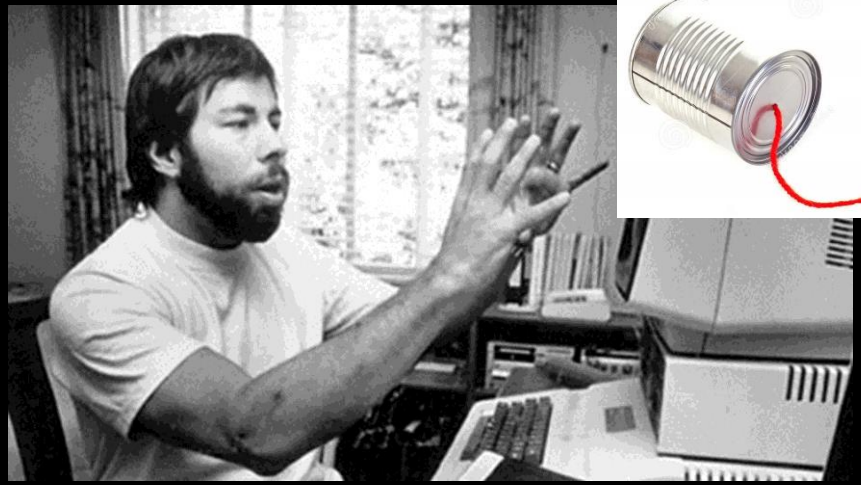
A David Paper Joint!



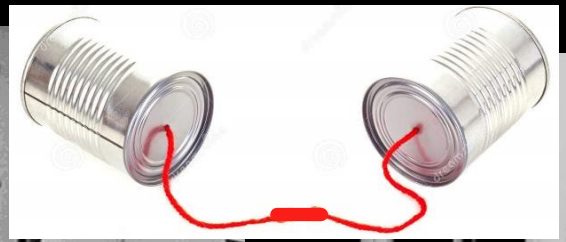
splunk> .conf18

SME != admin && admin != SME

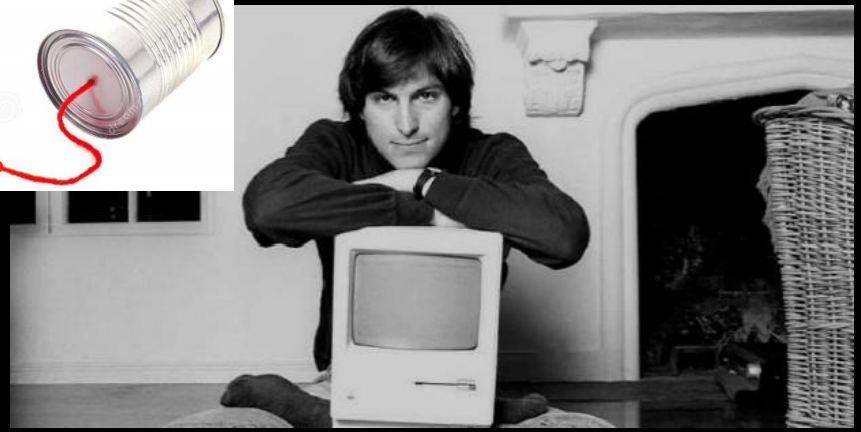
Technical SME



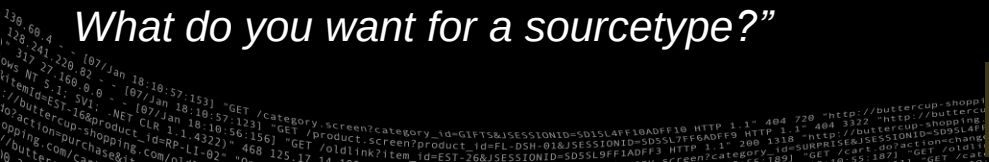
“What index do you need?
What do you want for a sourcetype?”



Product SME



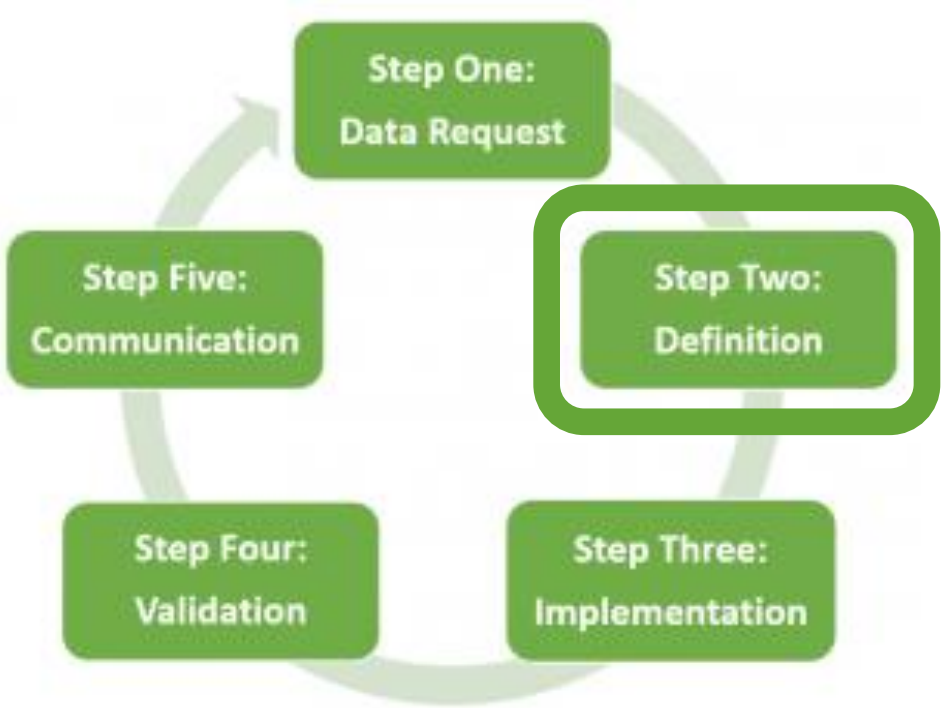
“I like black turtlenecks.”



splunk> .conf18

Onboarding != Ingestion

A David Paper Joint!

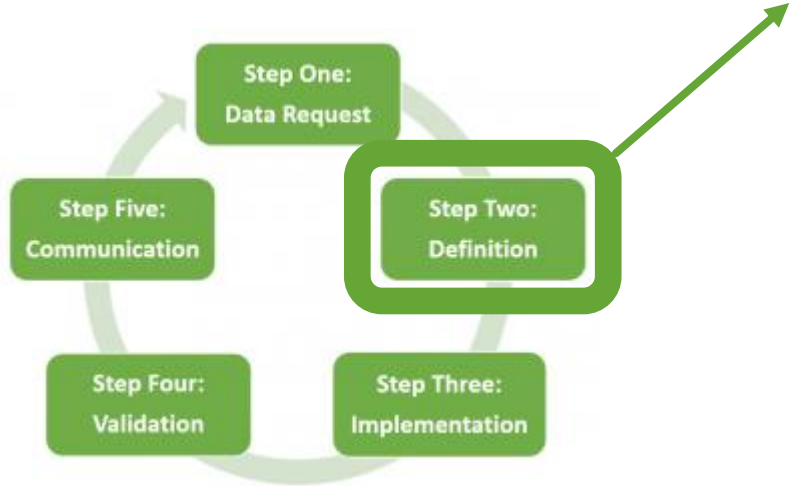


splunk> .conf18

Onboarding != Ingestion

A David Paper Joint!

Onboarding Phases



Ingestion

- Fetch from source:
  - Read access
  - Data volume estimate
  - Sample
- Use sample for:
  - Event Breaks
  - Time Stamps

What to create?

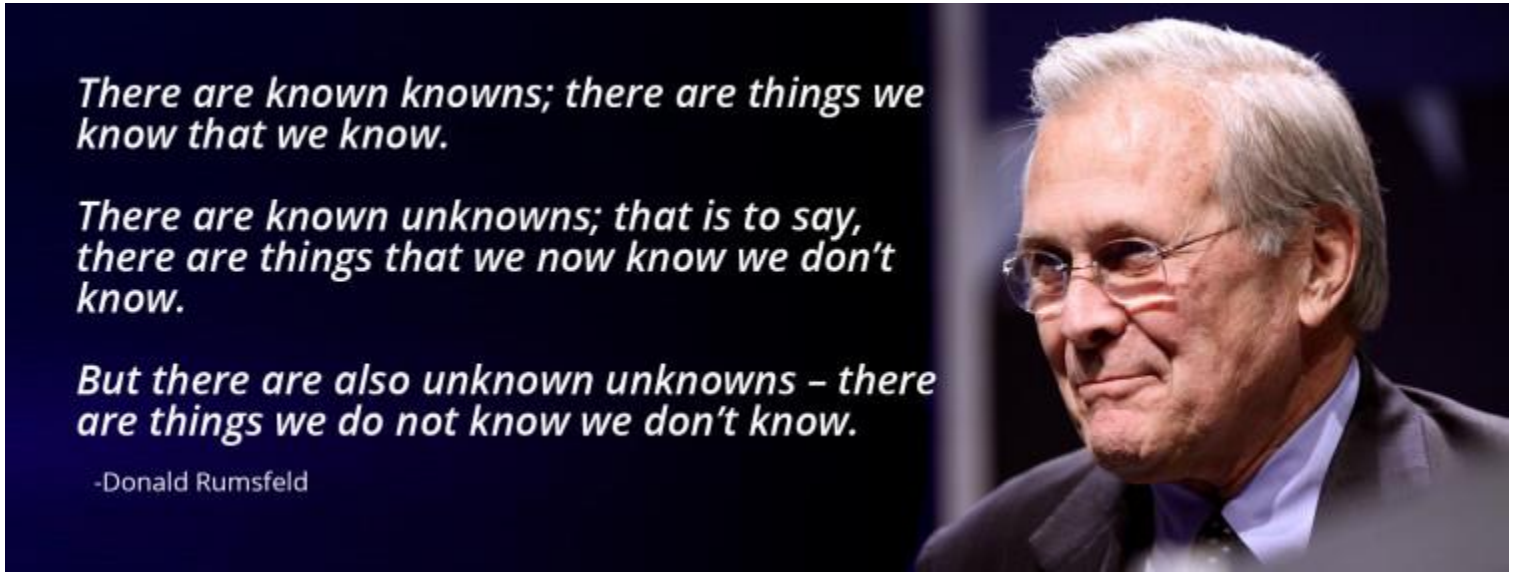
Dashboards and reports and scheduled searches, Oh My

splunk> .conf18

Give ‘em the first hit free!

They’ll be hooked on Splunk!

Crafting the Use Case



Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
Unaware Issue Exists		
Aware Issue Exists		

Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	**Listening** • Dashboards & Glass Tables • Odd symptom combo	
Aware Issue Exists		

Workflow Phase: Use Case Definition

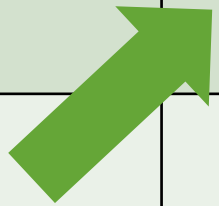
Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	**Listening** • Dashboards & Glass Tables • Odd symptom combo	
Aware Issue Exists	**Investigating** • Go Spelunking! • Hunting for RC	

Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

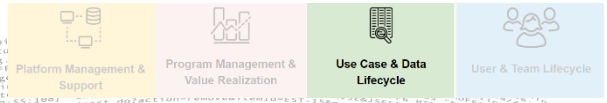
	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	**Listening** • Dashboards & Glass Tables • Odd symptom combo	**Monitoring** • Scheduled Searches & Alert Actions
Aware Issue Exists	**Investigating** • Go Spelunking! • Hunting for RC	



Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	**Listening** • Dashboards & Glass Tables • Odd symptom combo	**Monitoring** • Scheduled Searches & Alert Actions
Aware Issue Exists	**Investigating** • Go Spelunking! • Hunting for RC	**Attacking** • Adaptive Response



Best Practiced Deployment

A.K.A Center of Excellence

Best Practiced Deployment

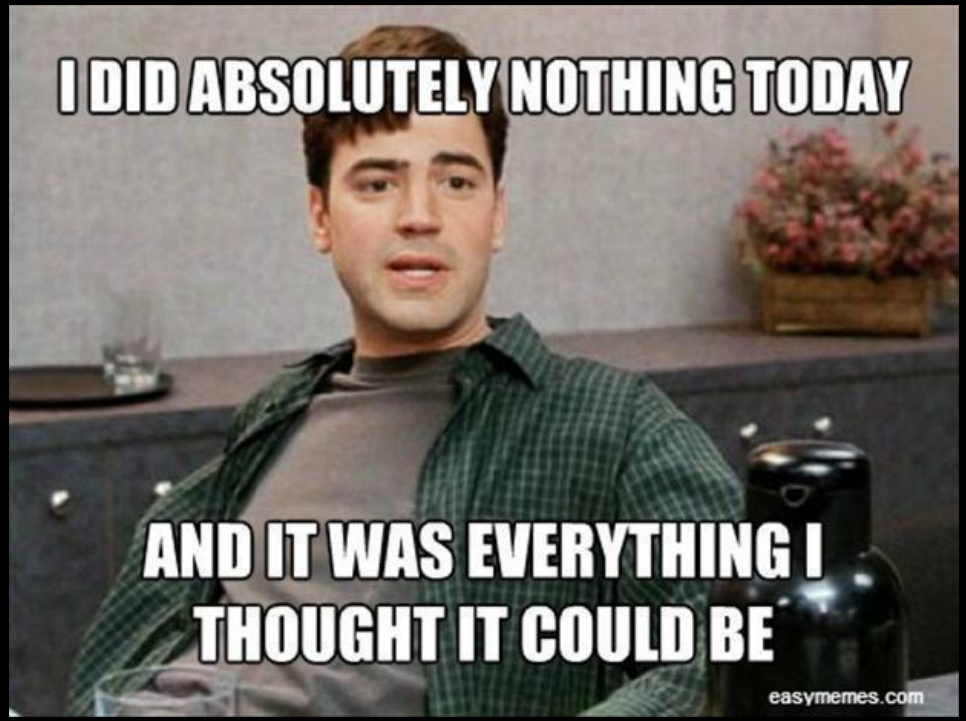
A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle



Prepared to answer at 4 a.m.

Thanks to Learning Paths

Learning Paths

Whether you are Splunk Cloud customer or Splunk App developer there's a path for you. Take the journey that's best for you.

For Splunk Users

Splunk Education's learning path for power users takes you from investigative keyword searches to creating rich reports and visualizations to becoming a Splunk search ninja!

View Courses

For Splunk Enterprise Administrators

Whether you're responsible for a single Splunk instance or a massive deployment, our Administrator curriculum teaches you the tasks and best practices to keep your Splunk installation happy and healthy.

View Courses

For Splunk Cloud Customers

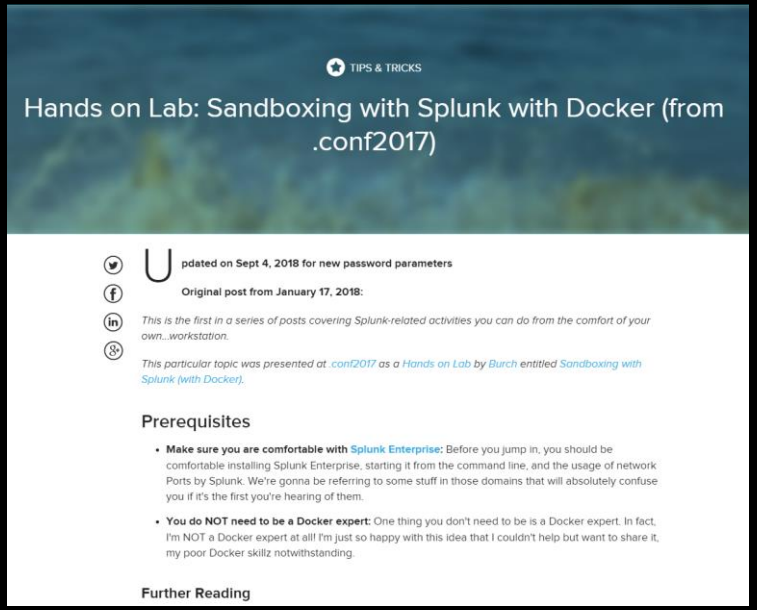
Splunk Education's learning path for

For Splunk App Developers

Harness the power of Splunk's Web

splunk> .conf18

Architecture vs Lab vs Sandbox



TIPS & TRICKS

Hands on Lab: Sandboxing with Splunk with Docker (from .conf2017)

Updated on Sept 4, 2018 for new password parameters

Original post from January 17, 2018:

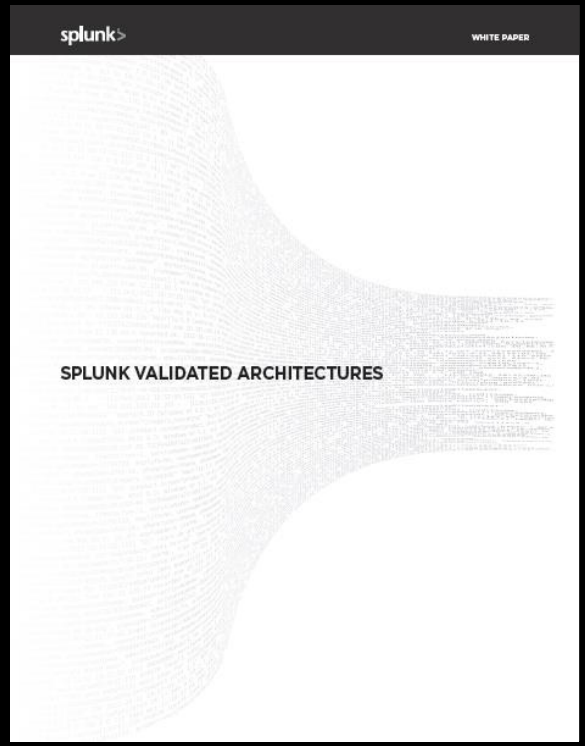
This is the first in a series of posts covering Splunk-related activities you can do from the comfort of your own...workstation.

This particular topic was presented at .conf2017 as a Hands on Lab by Burch entitled Sandboxing with Splunk (with Docker).

Prerequisites

- **Make sure you are comfortable with Splunk Enterprise:** Before you jump in, you should be comfortable installing Splunk Enterprise, starting it from the command line, and the usage of network Ports by Splunk. We're gonna be referring to some stuff in those domains that will absolutely confuse you if it's the first you're hearing of them.
- **You do NOT need to be a Docker expert:** One thing you don't need to be is a Docker expert. In fact, I'm NOT a Docker expert at all! I'm just so happy with this idea that I couldn't help but want to share it, my poor Docker skillz notwithstanding.

Further Reading



splunk> WHITE PAPER

SPLUNK VALIDATED ARCHITECTURES

Platform Management & Support | Program Management & Value Realization | Use Case & Data Lifecycle | User & Team Lifecycle

splunk> .conf18

BAU Account

Dog Food!

- Use non-admin account
  - Prevents accidents
  - Live with limitations
  - Appreciate user experience

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

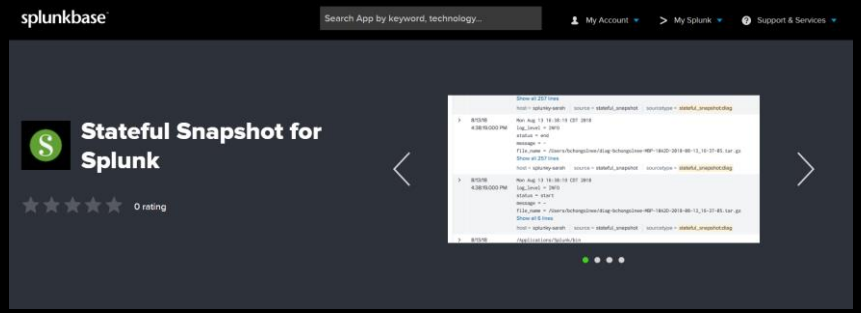
Use Case & Data Lifecycle

User & Team Lifecycle

Change Control

Enablement through experimentation

- Impacting
  - Platform settings
  - Critical Knowledge Objects
- Non Impacting
  - Searching
  - Private KO
  - Impact while logged in
  - Nominate to Impacting
- Version Snapshots



splunk> .conf18

Service Catalog

Force yourself to deliver

Learn more about how to work with us through these areas...

Foundations of Zero

Scope

Today's platform provides **Splunk as a Service** with a future goal to establish Splunk, here at Splunk, as a Strategy for our Business.

Timeline

Within Splunk's FY18 we aim to establish two primary domains of Splunk usage here at Splunk:

0. ***SplunkZero***: Bleeding edge builds of Splunk Enterprise
1. ***SplunkOne***: Production grade Splunk deployment for Security and Business Analytics

People

@Declan Morris is our **Executive** Sponsor. @Tamara Gardner is our **Program** Manager for delivering our service.

Check out the Staff and Skillz to learn about team members and their skillz.

Structure

Our governance is designed as a Centralized model with one team providing decision making authority.

Services Offered

Use Case & Data Lifecycle

- New data? New Use Case?
- Learn how to be "Making machine data accessible, usable, and valuable to everyone."
- Learn more about our Service Offering for Use Case & Data Lifecycle

User & Team Lifecycle

- "Taking the SH out of IT"
- Stop blaming Canada and learn how to be a better Splunker
- Learn more about our Service Offering for User & Team Lifecycle

Platform Management & Support

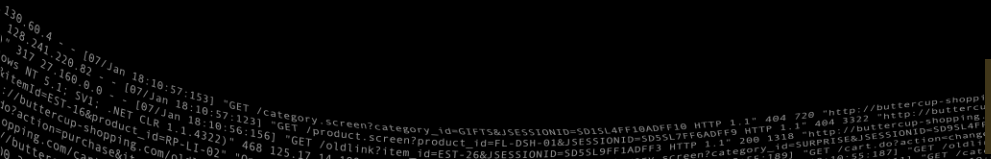
- Learn about the Zero team!
- Delivering Splunk @ Splunk is more than just keeping the lights on!
- Explore our Service Level Definitions and operational excellence
- Learn more about our Service Offering for Platform Management & Support

Program Management & Value Realization

- Our Governance, standards, and practices
- Case studies, successes, and wins here at Splunk
- Learn more about our Service Offering for Program Management & Value Realization

Frequently Asked Questions

Zero subscribes to a Best-Practiced Deployment philosophy.



splunk> .conf18

Delay Backfill

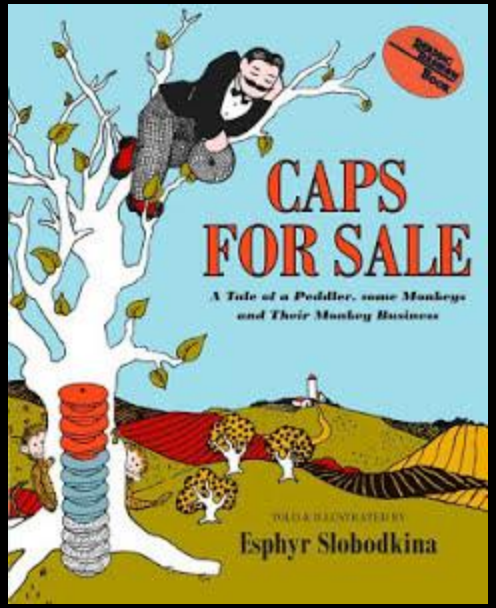
Validate new process first

Hiring Practices

Qualify staffing needs

- Complexity
  - Distributed Deployment
  - Indexer Clustering
  - Search Head Clustering
  - Data Collection Tier
  - Complex Utility Deployments
- Work Expectations
  - Platform HA means People HA
  - CoE staff vs End Users workload

We Wear Many Hats



- Architect
- Developer
- Engineer
- Executive Sponsor
- Search Expert
- Knowledge Manager
- Program Manager
- Project Manager
- User Community

Mind the Gap

Staffing model

Team Member	Architect	Developer	Engineer	Executive Sponsor	Expert User	Knowledge Manager	Program Manager	Project Manager

splunk> .conf18

Best Practiced Deployment

A.K.A Center of Excellence

Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

Best Practiced Deployment

A.K.A Center of Excellence

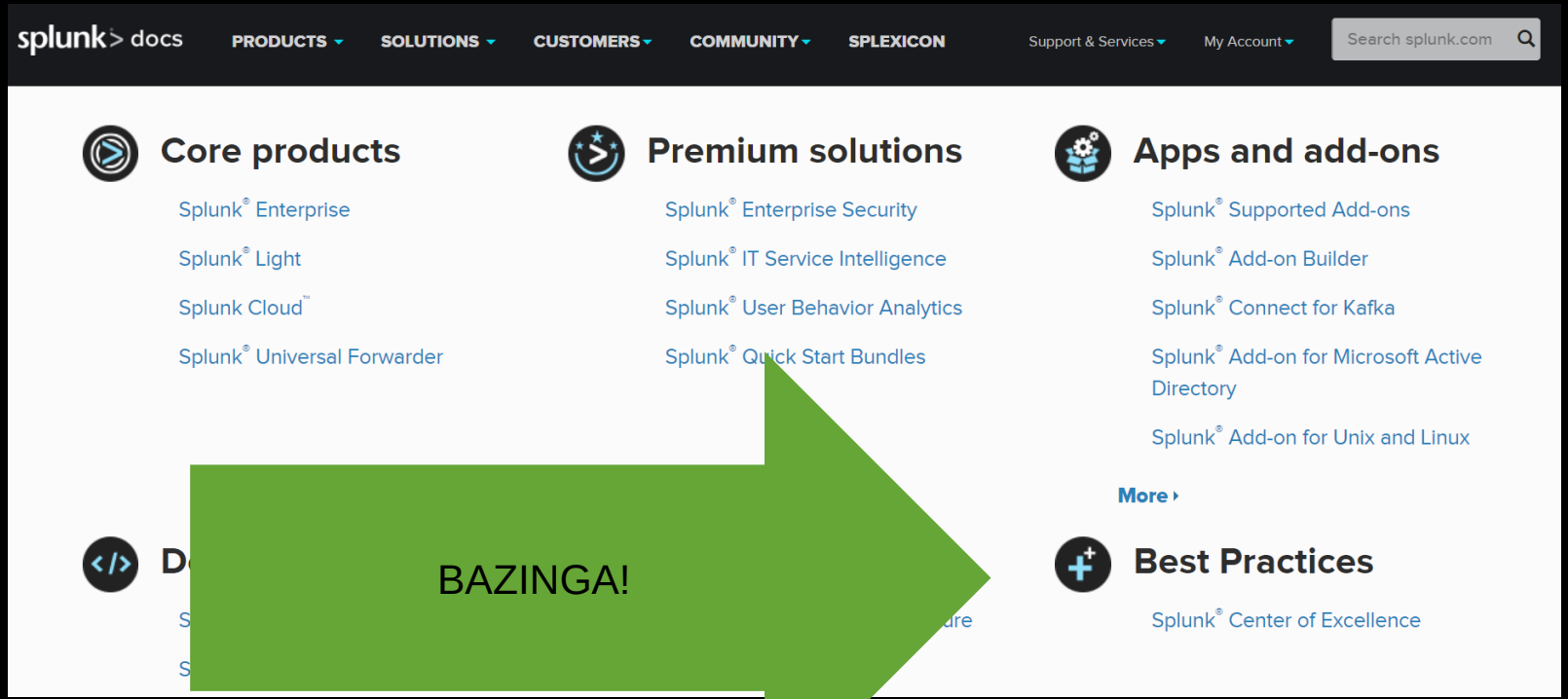
Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

New Manual. Who dis?



splunk> .conf18

Download topic as PDF

About the Splunk Center of Excellence

A best practices deployment

The Splunk Center of Excellence (CoE) is a vehicle for the implementation of Splunk best practices. The CoE provides reference materials, templates, and expert guidance for all aspects of your deployment.

For example, have you ever wondered what the recommended process is for data onboarding? Would you like to know how you can improve your organization's procedures for platform management? Do you need standards in place for user education? The Splunk CoE has you covered, from A to Z.

Foundations, Activities, and Service Areas

The CoE is comprised of Foundations, Activities, and Service Areas. Foundations are one-time definitions that ensure the sustainability and success of your CoE. Activities are designed to improve and support your day-to-day operations. You choose which Activities to implement according to the level of sophistication your organization wants to achieve. Within your service catalog, these Activities are grouped into four distinct Service Areas.

Foundations

What Now?

Related breakout sessions and activities…

1. Rate this! (be honest)
2. Collaborate: #bestpractices
   - Sign Up @ http://splk.it/slack
3. More talks, search for
   - Burch
   - Jeff Champagne
   - Delaney
   - Stefan
   - Veuve

Questions & Discussion?

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