

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 ----->

4:18

≡ Best Practices & Better...

INFO FEEDBACK

FEEDBACK

How would you rate this session content: (Rate 1 to 5)
*

★★★★★

How would you rate the session speaker(s): (Rate 1 to 5)
*

★★★★★

How relevant is this session to your business / role?
(Rate 1 to 5)

★★★★★

General Feedback:

SUBMIT

* = Required fields



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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

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

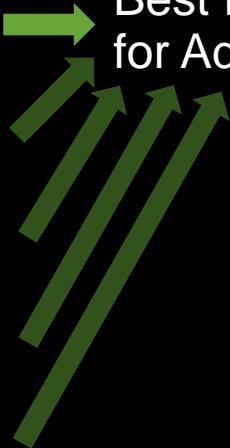
Creating Welcome Pages

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

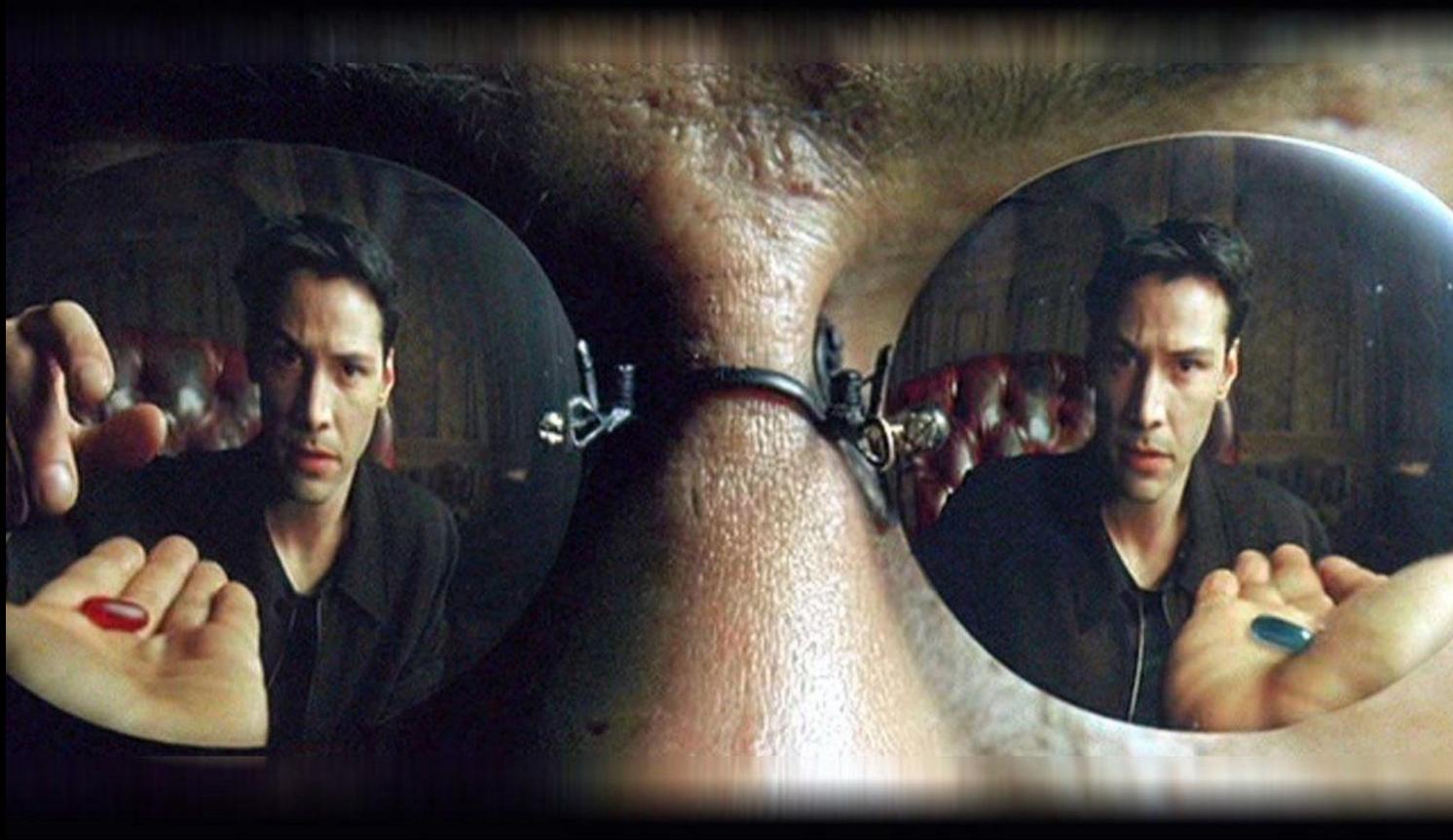


Use Case & Data Lifecycle



User & Team Lifecycle

Best Practices for a Best Practiced Deployment



Foundations

Best Practices for a Best Practiced Deployment



Charter



Executive Sponsor



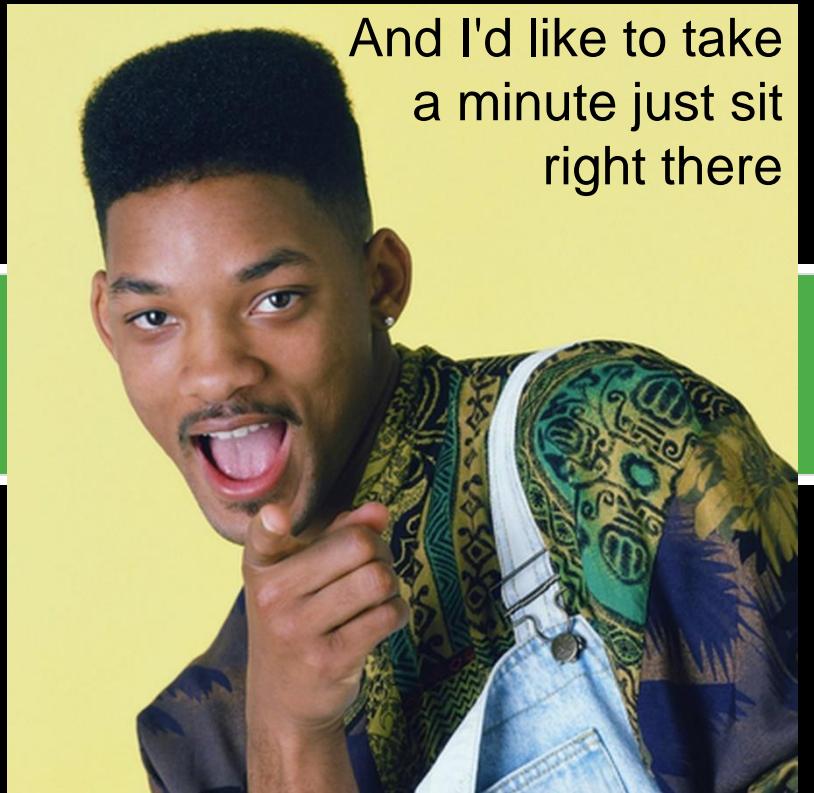
Metrics



Operating Model

Practice Politics

Scope == 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



Platform Management



Program Management &
Value Realization



Use Case & Data Lifecycle



User & Team Lifecycle

splunk> .conf18

Who wants to role play?

Choose Your Own Adventure!



Platform Management & Support

Program Management & Value Realization

Use Case & Data Lifecycle

User & Team Lifecycle

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...



Platform Management & Support



Program Management & Value Realization



User & Team Lifecycle



Dashboards

[Create New Dashboard](#)

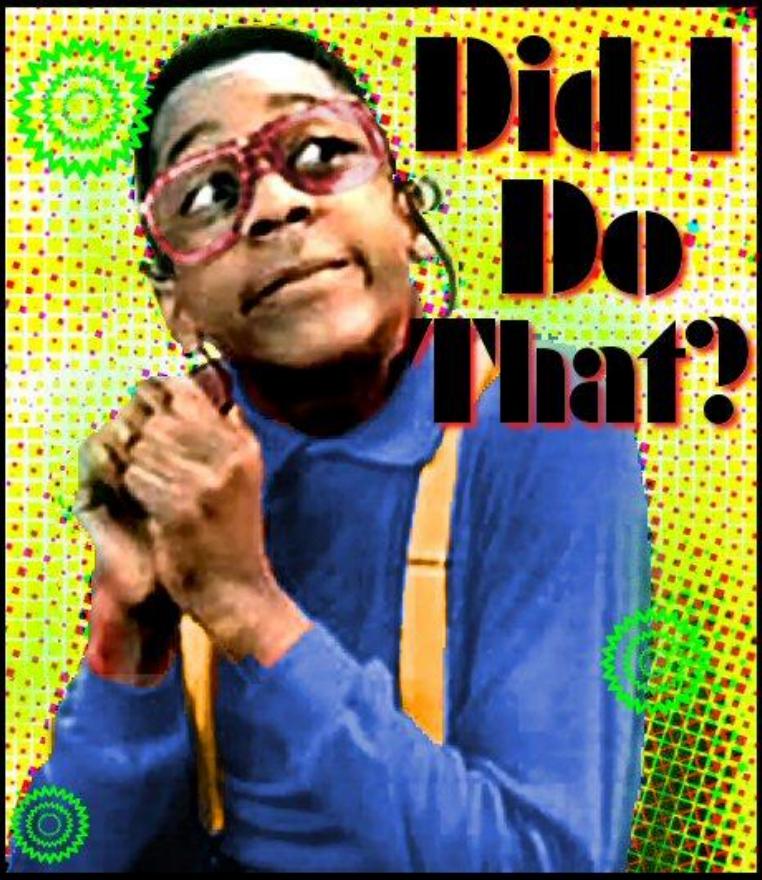
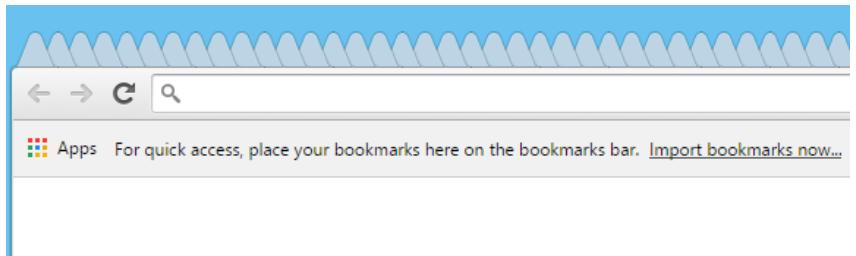
Dashboards include searches, visualizations, and input controls that capture and present available data.

33 Dashboards

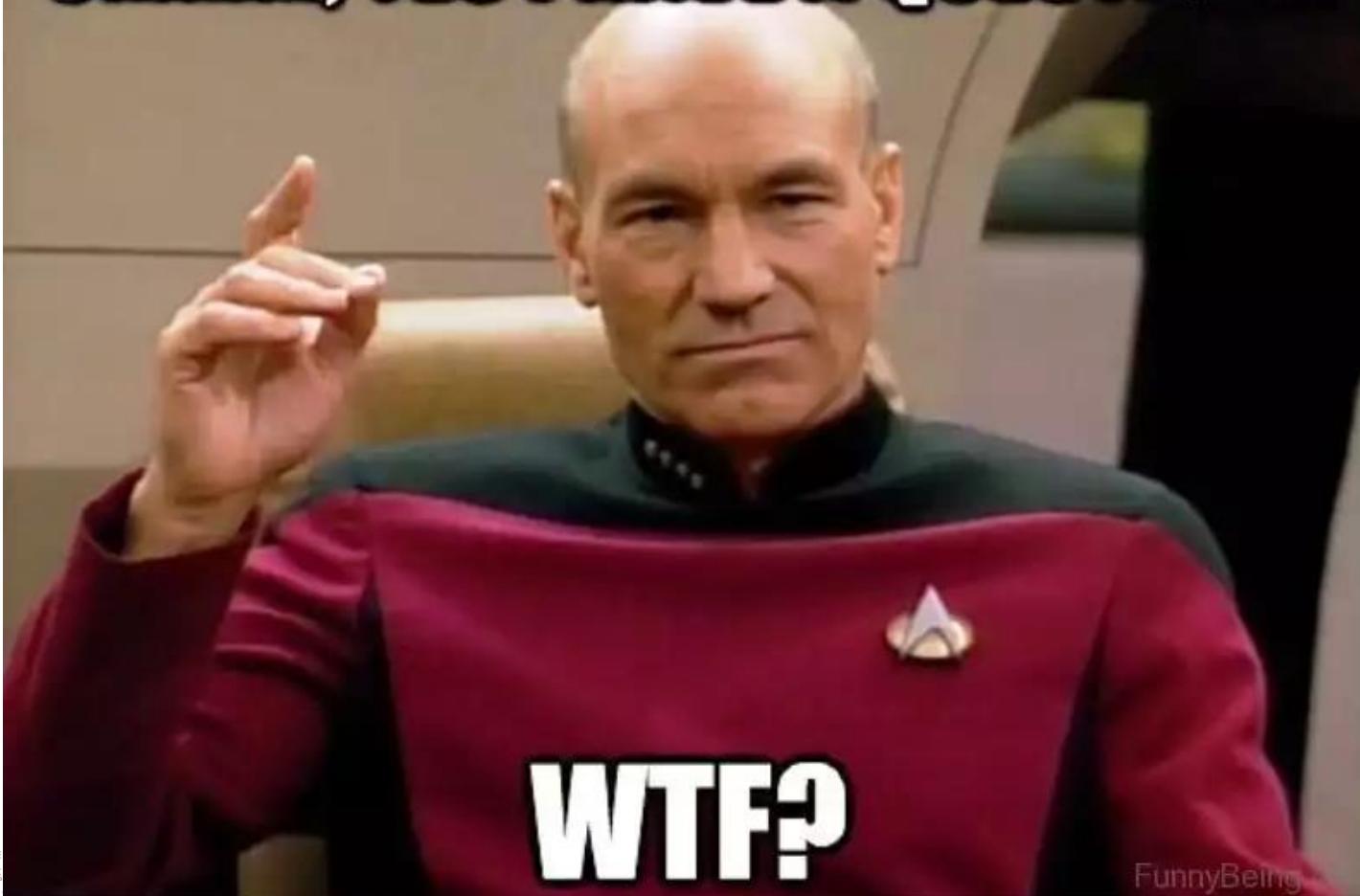
All	Yours	This App's	<input type="text" value="filter"/>	
-----	-------	------------	-------------------------------------	--

i	Title	Actions	Owner	App	Sharing
>	App Analytics	Edit ▾	nobody	splunk_app_stream	Global
>	Database Activity	Edit ▾	nobody	splunk_app_stream	Global
>	DNS Activity	Edit ▾	nobody	splunk_app_stream	Global
>	DNS Overview	Edit ▾	nobody	splunk_app_stream	Global
>	Error Details	Edit ▾	nobody	Splunk_TA_aws	Global
>	Event Analytics Audit	Edit ▾	nobody	itsi	Global
>	Example: Admin Landing Page	Edit ▾	nobody	welcome	Global
>	Example: New User Landing Page	Edit ▾	nobody	welcome	Global
>	GuardDuty - App Drilldown	Edit ▾	nobody	TA-aws_guardduty	Global
>	GuardDuty - Dashboard Drilldown	Edit ▾	nobody	TA-aws_guardduty	Global

All the Dashboards!



UMMM, YES I HAVE A QUESTION...



WTF?

I DEAL WITH THE GOD DAMN CUSTOMERS



Doug M.

SO THE ENGINEERS DON'T HAVE TO

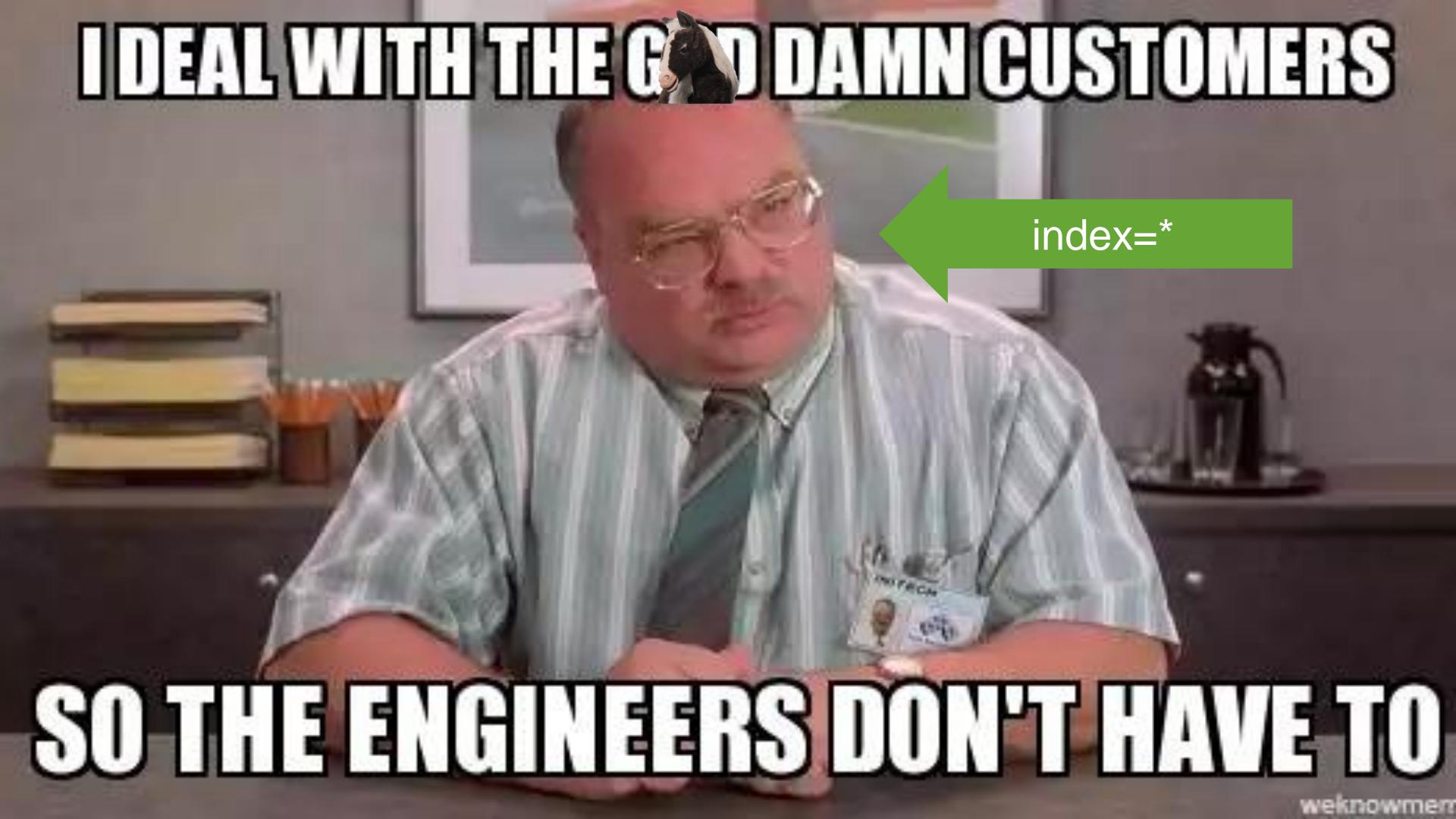
I DEAL WITH THE GOD DAMN CUSTOMERS



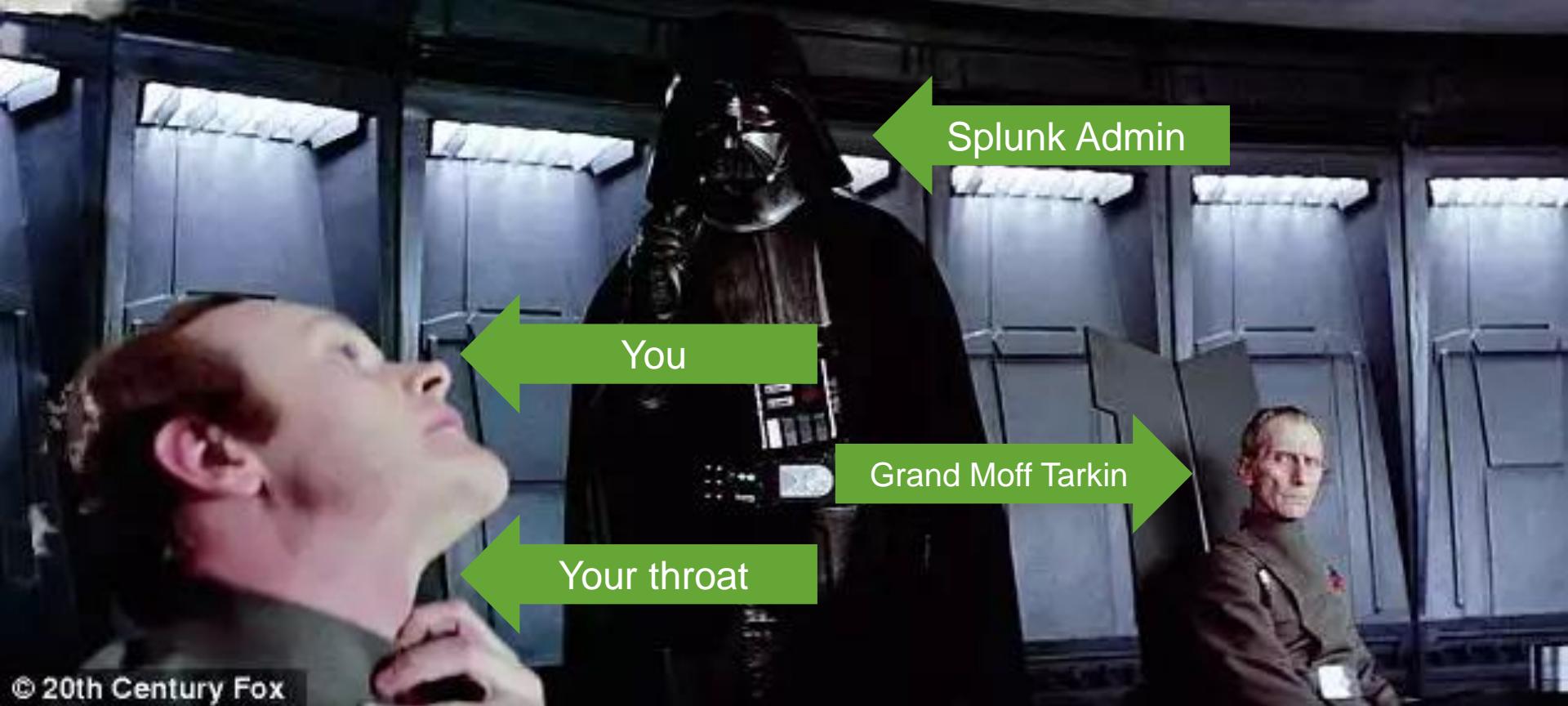
D. Merritt

SO THE ENGINEERS DON'T HAVE TO

I DEAL WITH THE GOD DAMN CUSTOMERS



SO THE ENGINEERS DON'T HAVE TO



Solution, you have?!



quickmeme.com



Platform Management & Support



Program Management & Value Realization



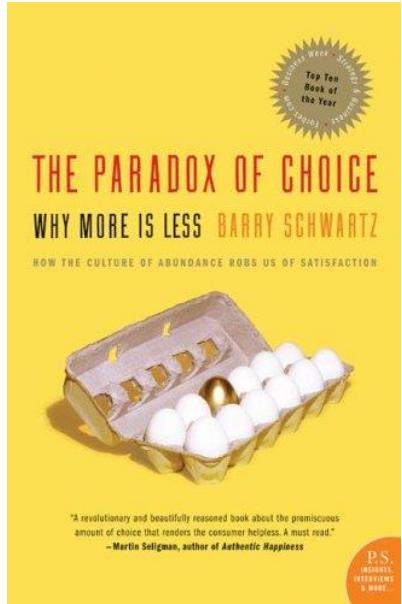
Use Case & Data Lifecycle



User & Team Lifecycle

The Paradox of Choice

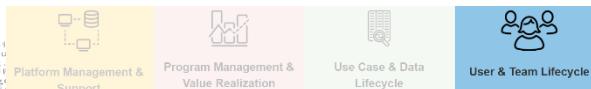
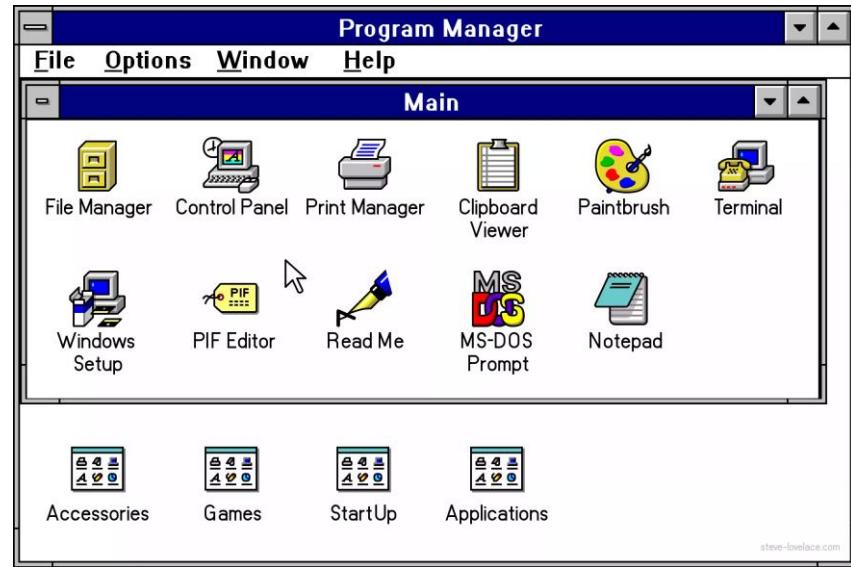
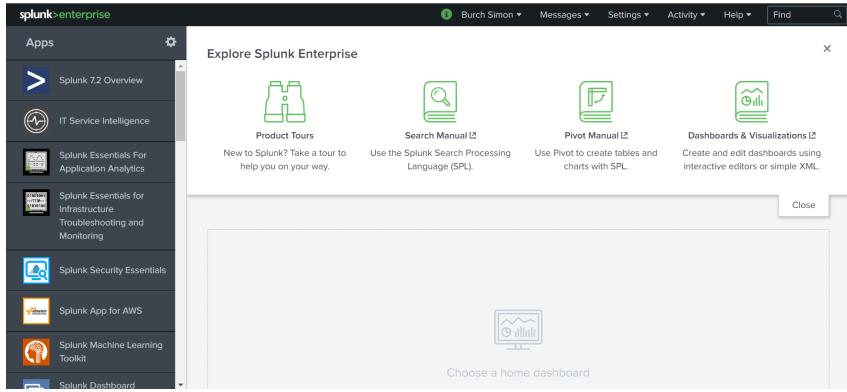
AKA Buyer's Remorse



“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

 App: Operations Administrator 1 Messages Settings Activity Help Find
Welcome Search Datasets Reports Alerts Dashboards Operations

Buttercup Games: Operation Team

Edit Export ...

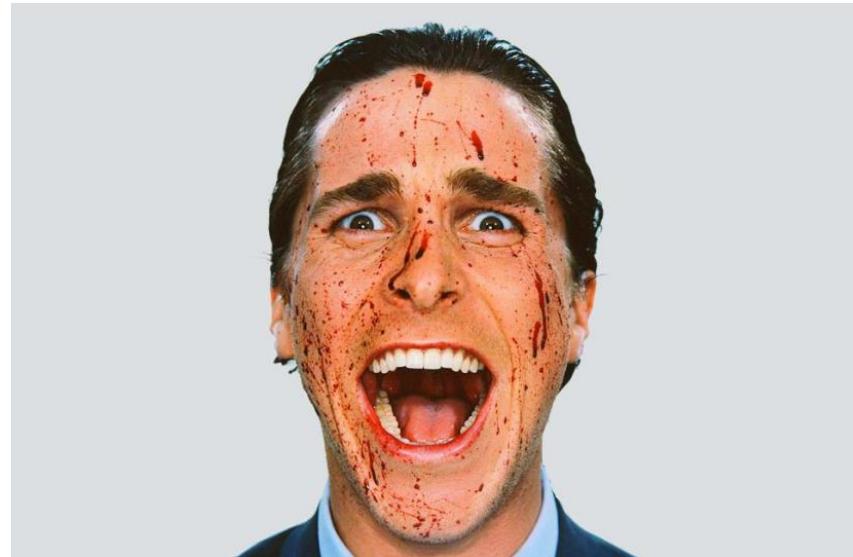


splunk> .conf18

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!



splunk> .conf18

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 can 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 company 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, and

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://imgtfy.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

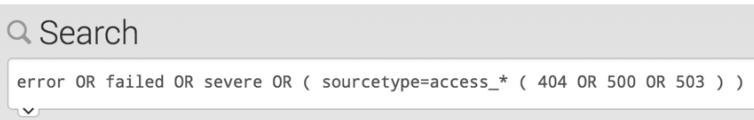
- <http://www.splunk.com/view/dominoes-pizza-transforms-e-commerce-with-splunk/SP-CAAAH92>

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 back



The search bar contains the following query:

```
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 still



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?



Platform Management

Program Management & Value Realization

Use Case & Data Lifecycle



1

splunk> .conf18

...so why do we do that in Splunk?

The screenshot shows the Splunk Enterprise homepage with a sidebar on the left containing links to various apps like Splunk 7.2 Overview, IT Service Intelligence, Splunk Essentials for Application Analytics, Splunk Essentials for Infrastructure, Splunk Security Essentials, Splunk App for AWS, Splunk Machine Learning Toolkit, and Splunk Dashboard. The main content area features a heading 'Explore Splunk Enterprise' with four cards: 'Product Tours' (binoculars icon), 'Search Manual' (magnifying glass icon), 'Pivot Manual' (document icon), and 'Dashboards & Visualizations' (gauge icon). Below these cards is a note: 'New to Splunk? Take a tour to help you on your way.' A large empty box at the bottom is labeled 'Choose a home dashboard'. The top navigation bar includes user profile, messages, settings, activity, help, and a search bar.

splunk • enterprise		Apps	Burch Simon	Messages	Settings	Activity	Help	Find	Search				
Search	Metrics	Datasets	Reports	Alerts	Dashboards	Search & Reporting							
Dashboards													
Dashboards include searches, visualizations, and input controls that capture and present available data.													
33 Dashboards	All	Yours	This App's	filter	Actions	Owner	App	Sharing	Create New Dashboard				
i	Title	Actions	Owner	App	Sharing								
>	App Analytics	Edit	nobody	splunk_app_stream	Global								
>	Database Activity	Edit	nobody	splunk_app_stream	Global								
>	DNS Activity	Edit	nobody	splunk_app_stream	Global								
>	DNS Overview	Edit	nobody	splunk_app_stream	Global								
>	Error Details	Edit	nobody	Splunk_TA_aws	Global								
>	Event Analytics Audit	Edit	nobody	itsi	Global								
>	Example: Admin Landing Page	Edit	nobody	welcome	Global								
>	Example: New User Landing Page	Edit	nobody	welcom	Global								
>	GuardDuty - App Drilldown	Edit	nobody	TA-aws_guardduty	Global								
>	GuardDuty - Dashboard Drilldown	Edit	nobody	TA-aws_guardduty	Global								
>	Health Overview	Edit	nobody	Splunk_TA_nod	Global								



splunk> .conf18

App as a Workspaces

Dedicated to one team/group/purpose

Welcome

Learn

Learning Splunk

If you're new to splunk, please start with these pages:

1. Product Overview: What is Splunk Enterprise? [🔗](#)
2. Video: Splunk Enterprise 6.3 Basic Search [🔗](#)
3. Splunk Tutorial [🔗](#)
4. Quick Reference Guide [🔗](#)
5. Splunk Education & Classes [🔗](#)

Get Help

Splunk Community & Events

Get an answer fast with...

- [answers.splunk.com](#) [🔗](#) - Q&A Forum
- [docs.splunk.com](#) [🔗](#) - Official Product Documentation

Events!

- Attend a free Splunk Live [🔗](#) event in your area
- Plan to join Splunk at The Annual Splunk Worldwide Users' Conference [🔗](#)
- Meet other users in your local Splunk User Group [🔗](#)

Go!

Waiting on your Splunk Admins?

Questions?

- Get better and faster answers by posting on [answers.splunk.com](#) [🔗](#).
- Follow the [answers.splunk.com](#) [🔗](#) usernames of peers and friends for greater collaboration! Simply click the "Follow" button within a user's profile within [answers.splunk.com](#) [🔗](#).

Field Extractions?

- Did you know you can extract fields yourself? Without any technical skill!
- With the [Field Extractor](#) [🔗](#), you can point and click what you want made into a field.

Leaderboard

Use the table below to identify the most active Splunkers (not you) in this workspace (app) over the last 30 days. These people are likely great candidates to learn more about Splunk from!

Most Popular Dashboards

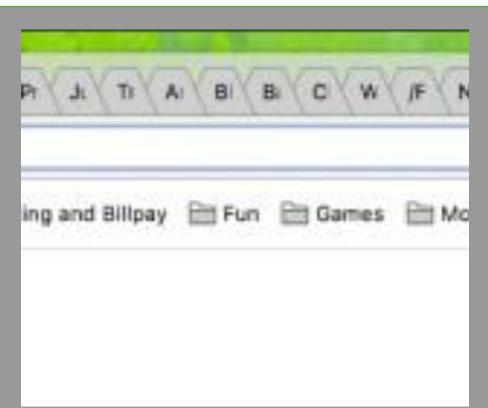
Not sure where to start? Check out the most popular dashboards of this app listed below. Select one to navigate directly to it.



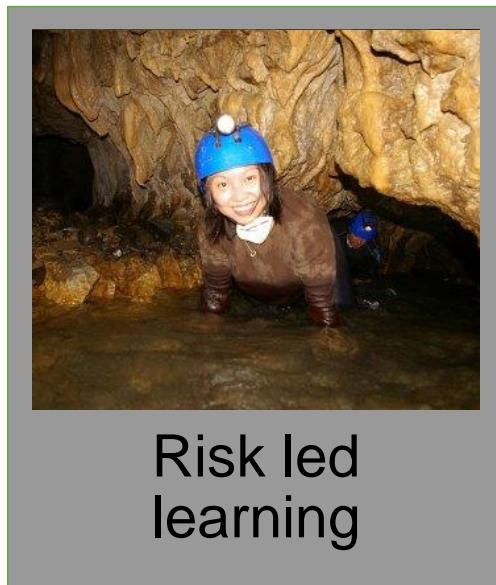
splunk> .conf18

Benefits

Increases in...



Safety



Risk led learning



Discovery led collaboration

Incentives



vs.



Is EDU Required?

Splunk Training + Certification

Splunk Fundamentals 1

Splunk Fundamentals 1

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.



“Yea, I took education”

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



Platform Management
Support

Program Management & Value Realization

Use Case & Data Lifecycle



User & Team Lifecycle

splunk> .conf18

Incentives



vs.



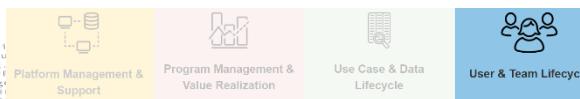
Alternative Approach: No Requirements

But limited impact...

You can't stop splunk-thusiasm...



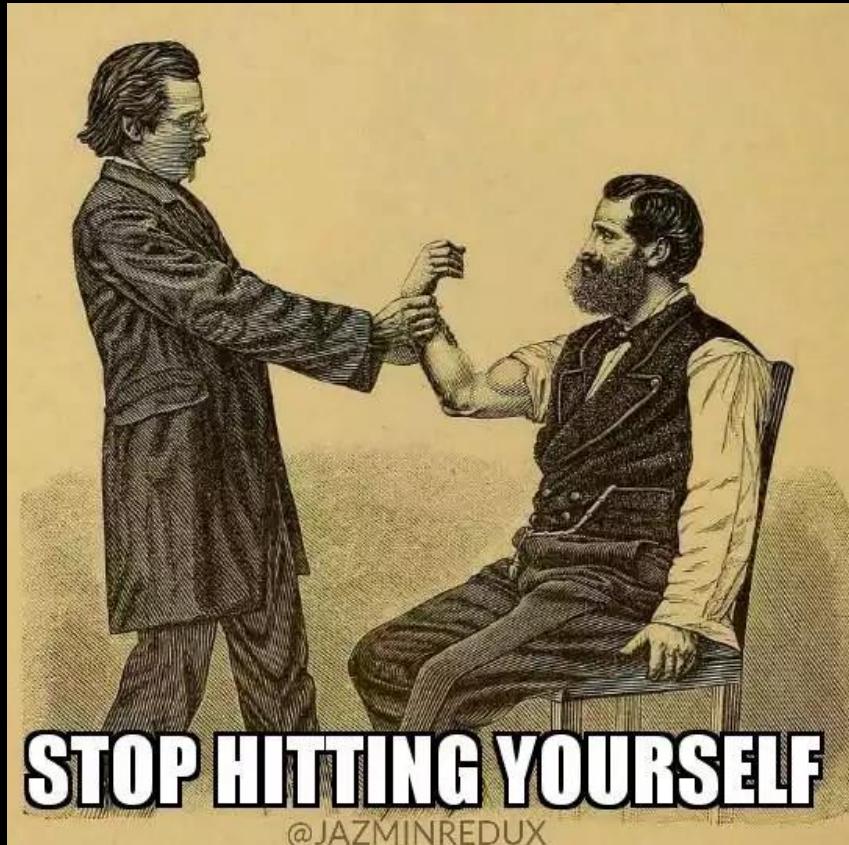
...so shape it in your favor!



splunk> .conf18

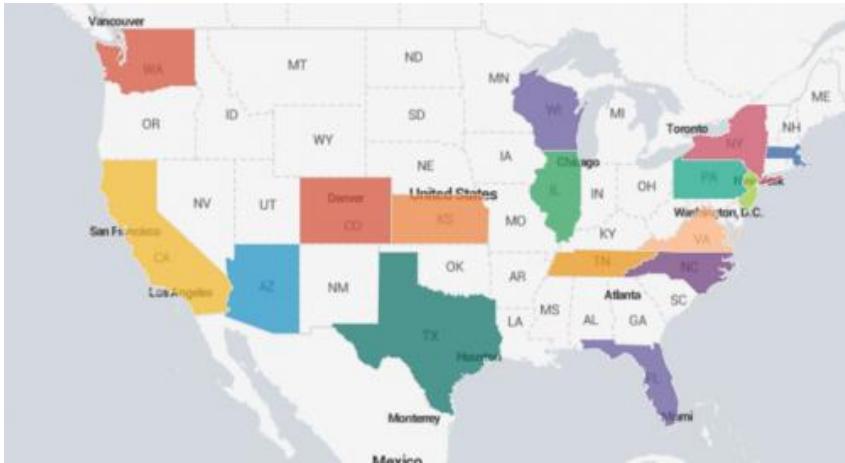
Incentive Driven User Onboarding

- ▶ “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



```
1 | makeresults
2 | eval curiosity="high"
3 | eval learning = if( curiosity=="high" , "success" , "datsooltoo" )
```



splunk> .conf18

Rinse & Repeat

Admin Teachers Power User



Power User Teaches User



Result

At first, more questions. Later, more disciples.



Clearly, now the fish can catch its own man...

Platform Management

Program Management & Major Realignment

Use Case & Data



1

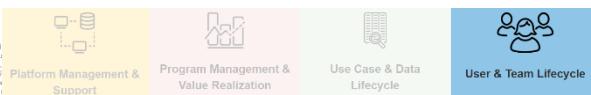
splunk> .conf18

Know thy Role?

English vs Splunk

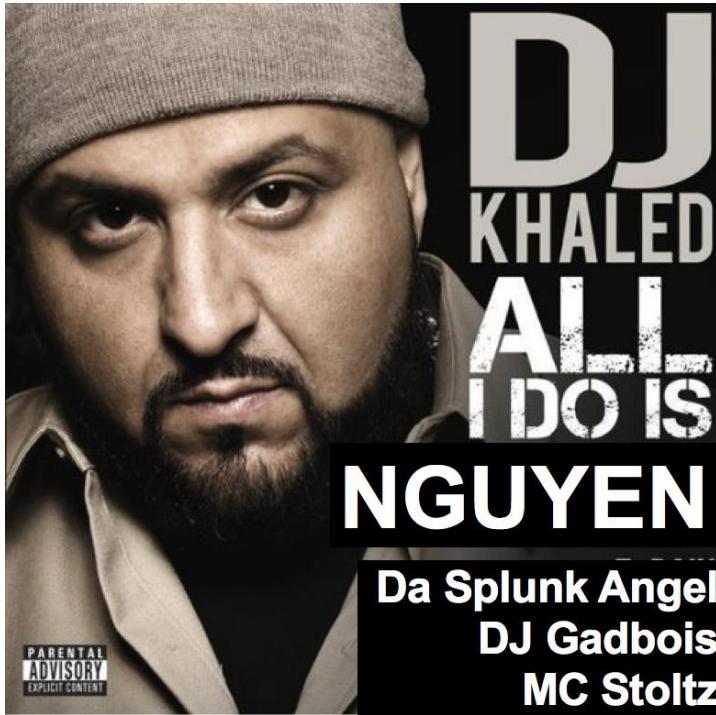
- ▶ Data Access
- ▶ Search Retention
- ▶ Product Feature Capabilities
- ▶ Knowledge Object Permissions
- ▶ Default App

 capability_admin	Security Group - Global
 capability_batch	Security Group - Global
 capability_developer	Security Group - Global
 capability_power	Security Group - Global
 capability_user	Security Group - Global
 data_all	Security Group - Global
 data_customerinfo	Security Group - Global
 data_dreamhost	Security Group - Global
 data_internal	Security Group - Global
 data_maple	Security Group - Global
 data_operatingsystems	Security Group - Global
 rdp	Security Group - Global
 workspace_admin	Security Group - Global
 workspace_default	Security Group - Global
 workspace_developer	Security Group - Global
 workspace_power	Security Group - Global
 workspace_user	Security Group - Global



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 —Leigh Valley live flavor
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



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...



Platform Management & Support



Program Management & Value Realization



User & Team Lifecycle

...only what you need

With clear information on where to go/learn next

Welcome Page

Workspace

Capabilities!

The screenshot illustrates the 'Burch Rocks!' app within the Splunk mobile interface. It features a clean, organized layout designed to guide users through various Splunk resources and capabilities. The 'Welcome Page' is prominently displayed at the bottom left, while the 'Workspace' and 'Capabilities!' sections are highlighted with large green arrows pointing towards the central 'Learn' and 'Get Help' areas respectively. The overall design emphasizes accessibility and ease of navigation for users new to Splunk or looking for specific help and resources.

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



 Program Management & Major Realization



 Use Case & Data

1

splunk> .conf18

Tighter Coupling

Use Case with Data



Program Management & Value Realization



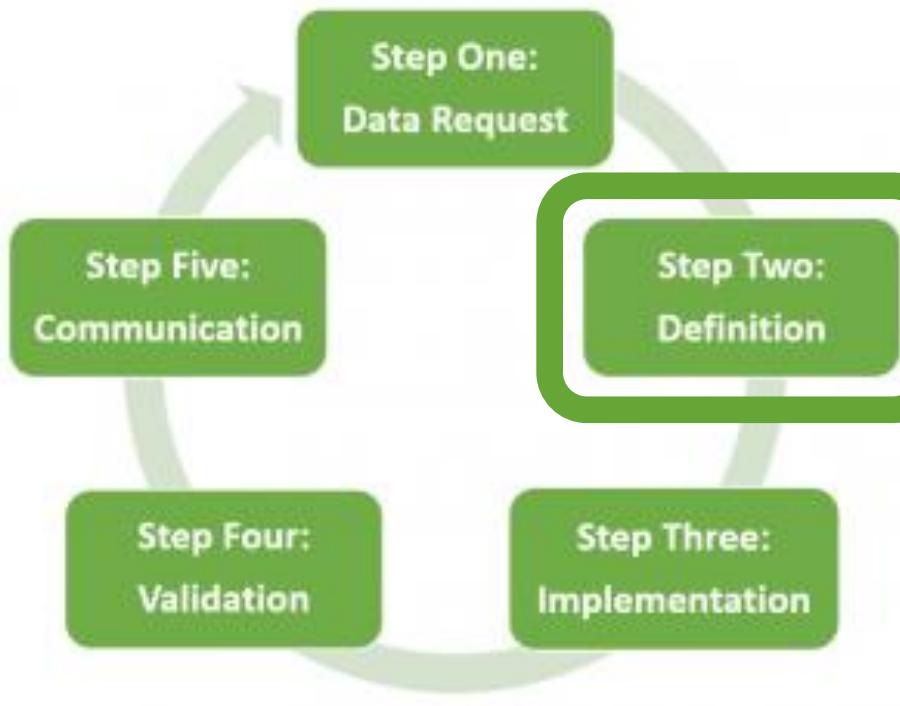
Use Case & Data

1

splunk> .conf18

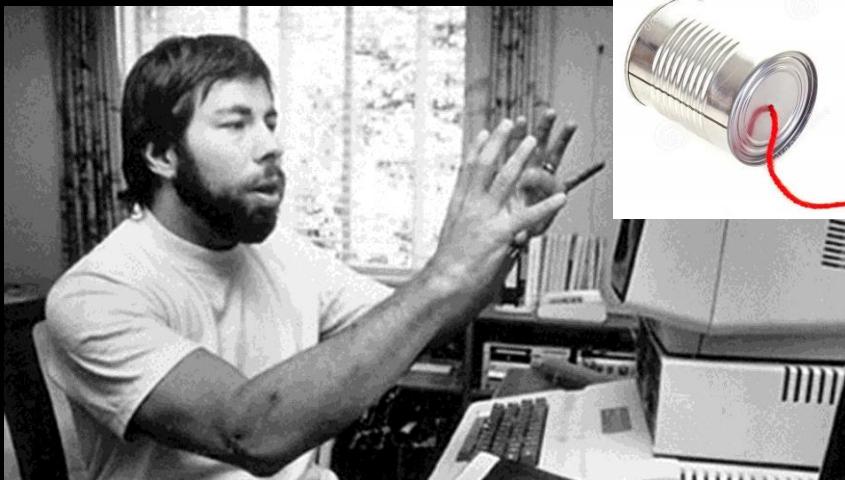
Onboarding != Ingestion

A David Paper Joint!



SME != admin && admin != SME

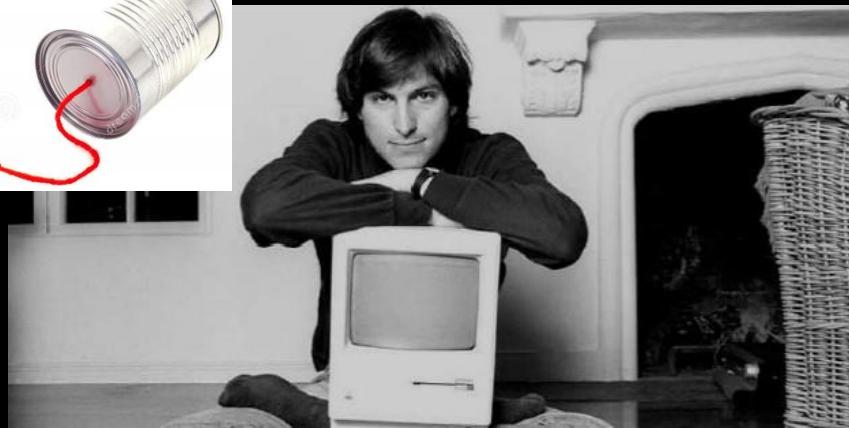
Technical SME



*"What index do you need?
What do you want for a sourcetype?"*



Product SME



"I like black turtlenecks."



Platform Management & Support



Program Management &
Value Realization



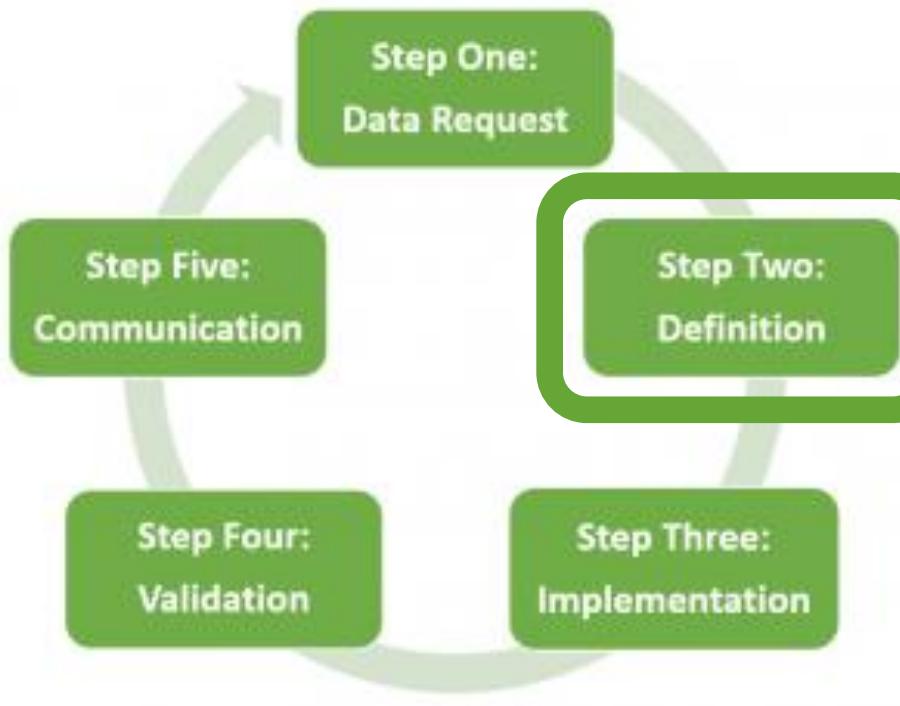
Use Case & Data
Lifecycle



User & Team Lifecycle

Onboarding != Ingestion

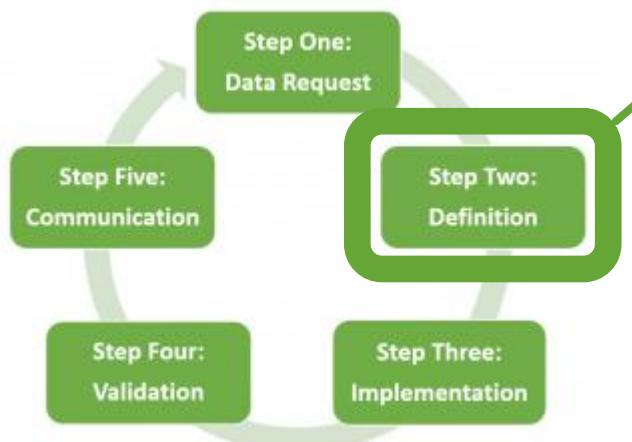
A David Paper Joint!



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



Platform Management &

 Program Management & Value Realization



Use Case & Data

splunk> .conf18

Give 'em the first hit free!

They'll be hooked on Splunk!



Platform Management

Program Management &
Value Realization



Use Case & Data

splunk> .conf18

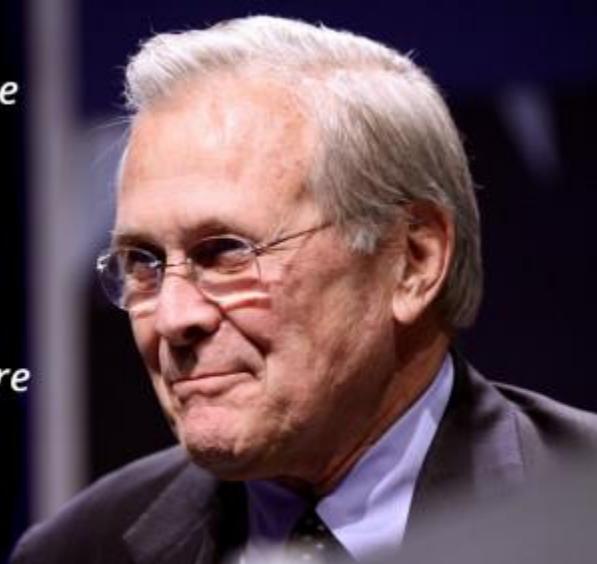
Crafting the Use Case

There are known knowns; there are things we know that we know.

There are known unknowns; that is to say, there are things that we now know we don't know.

But there are also unknown unknowns – there are things we do not know we don't know.

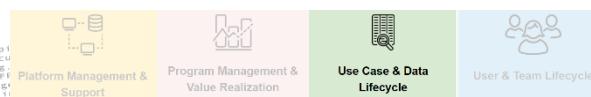
-Donald Rumsfeld



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

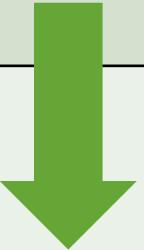
	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	<p>Listening</p> <ul style="list-style-type: none"> • Dashboards & Glass Tables • Odd symptom combo 	
Aware Issue Exists		



Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

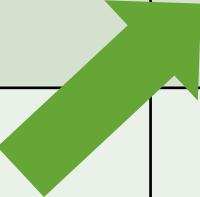
	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	<p>Listening</p> <ul style="list-style-type: none"> • Dashboards & Glass Tables • Odd symptom combo 	
Aware Issue Exists	<p>Investigating</p> <ul style="list-style-type: none"> • Go Spelunking! • Hunting for RC 	



Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	<p>Listening</p> <ul style="list-style-type: none"> • Dashboards & Glass Tables • Odd symptom combo 	<p>Monitoring</p> <ul style="list-style-type: none"> • Scheduled Searches & Alert Actions
Aware Issue Exists	<p>Investigating</p> <ul style="list-style-type: none"> • Go Spelunking! • Hunting for RC 	



Workflow Phase: Use Case Definition

Alerts vs Dashboards vs Searches

	Root Cause Unknown	Root Cause Known
Unaware Issue Exists	<p>Listening</p> <ul style="list-style-type: none"> • Dashboards & Glass Tables • Odd symptom combo 	<p>Monitoring</p> <ul style="list-style-type: none"> • Scheduled Searches & Alert Actions
Aware Issue Exists	<p>Investigating</p> <ul style="list-style-type: none"> • Go Spelunking! • Hunting for RC 	<p>Attacking</p> <ul style="list-style-type: none"> • Adaptive Response



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



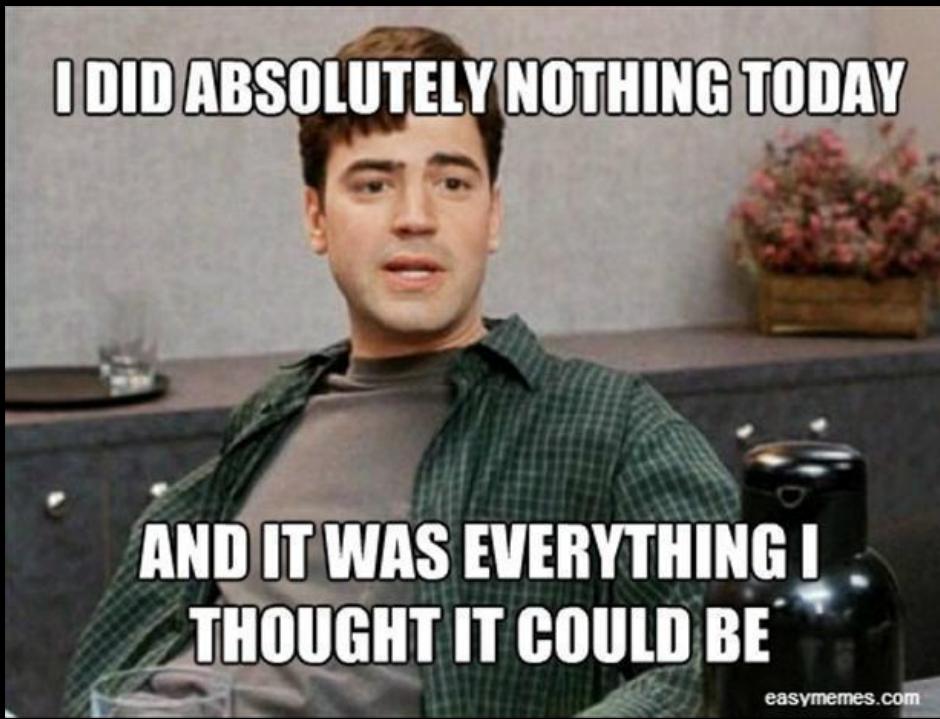
Program Management & Value Realization



Use Case & Data Lifecycle



User & Team Lifecycle



pasvmemes.com



Platform Management



Program Management & Value Realization



Use Case & Data

splunk> .conf18

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

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:

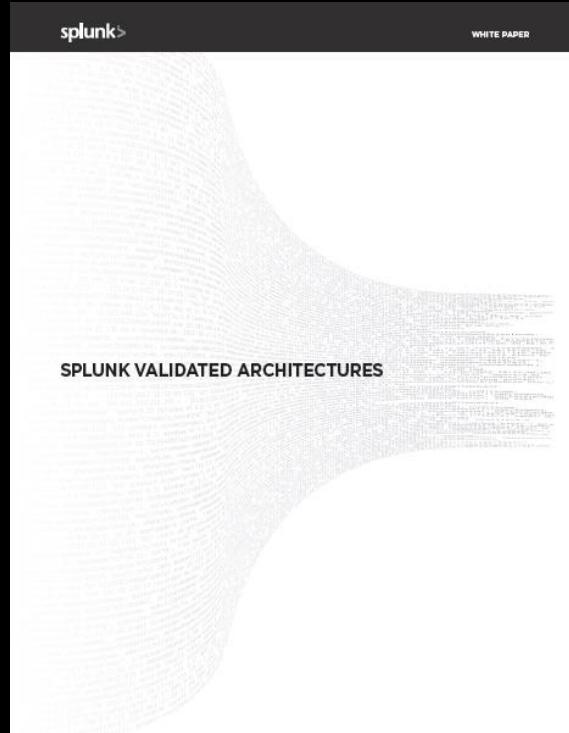
This is the first in a series of posts covering Splunk-related activities you can do from the comfort of your own...workstation.

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



BAU Account

Dog Food!

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



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

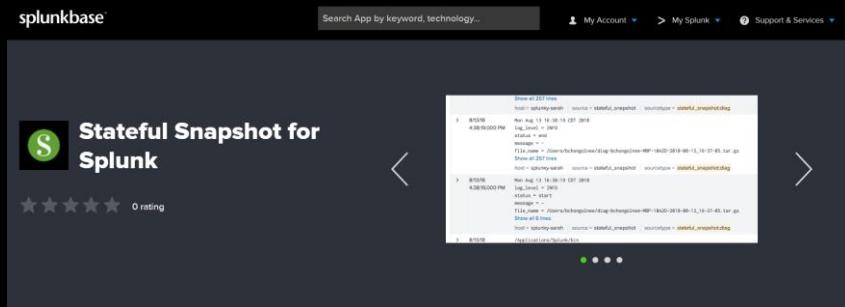


User & Team Lifecycle

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



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](#).



Platform Management & Support



Program Management & Value Realization



Use Case & Data Lifecycle



User & Team Lifecycle

Delay Backfill

Validate new process first



Platform Management &



Program Management &
Value Realization



Use Case & Data Lifecycle

splunk> .conf18

Hiring Practices

Qualify staffing needs

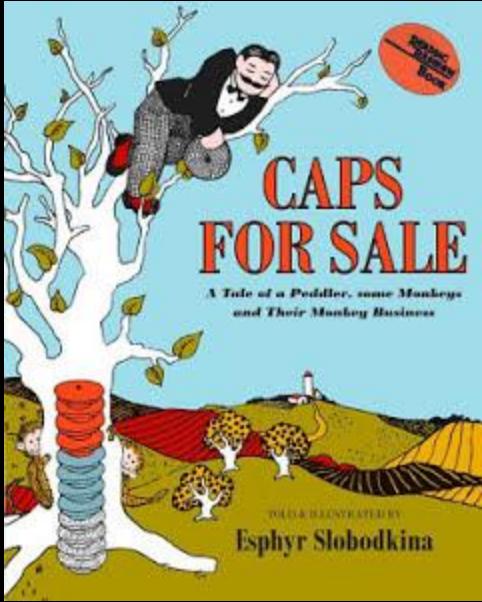


- ▶ Complexity
 - Distributed Deployment
 - Indexer Clustering
 - Search Head Clustering
 - Data Collection Tier
 - Complex Utility Deployments

- ▶ 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



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

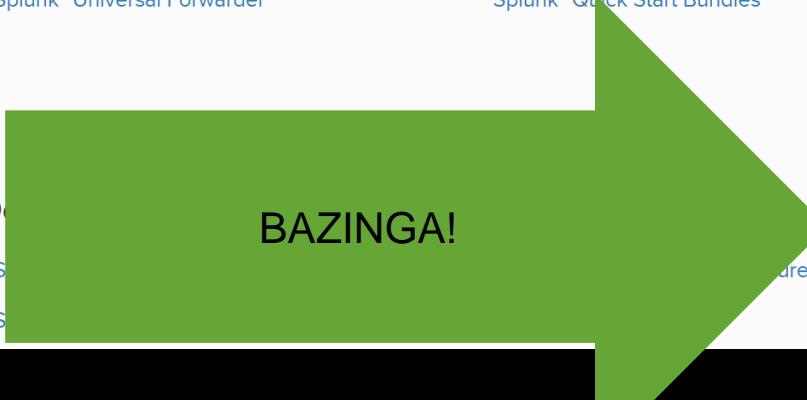


Use Case & Data Lifecycle



User & Team Lifecycle

New Manual. Who dis?



Core products

- Splunk® Enterprise
- Splunk® Light
- Splunk Cloud™
- Splunk® Universal Forwarder

Premium solutions

- Splunk® Enterprise Security
- Splunk® IT Service Intelligence
- Splunk® User Behavior Analytics
- Splunk® Quick Start Bundles

Apps and add-ons

- Splunk® Supported Add-ons
- Splunk® Add-on Builder
- Splunk® Connect for Kafka
- Splunk® Add-on for Microsoft Active Directory
- Splunk® Add-on for Unix and Linux

More ›

DevOps

BAZINGA!

Best Practices

Splunk® Center of Excellence

Splunk Center of Excellence Handbook

[!\[\]\(11b8a6fcceb832986de0c749ec79ed59_img.jpg\) Download manual as PDF](#)[Hide Contents ▾](#)

[Documentation](#) / [Splunk® Center of Excellence](#) / [Splunk Center of Excellence Handbook](#)
/ [About the Splunk Center of Excellence](#)

[Previously Viewed](#)

Splunk Center of Excellence Handbook

Overview

About the Splunk Center of Excellence

How to use the Splunk Center of Excellence handbook

Release notes for the Splunk Center of Excellence

Release history for the Splunk Center of Excellence

Preparation

Create a Splunk Center of Excellence roadmap

Take the Splunk Center of Excellence self-assessment

[!\[\]\(3b939224b0d40b7e722185bcc84abcb9_img.jpg\) 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

About the Splunk Center of Excellence

A best practices deployment

Foundations, Activities and Service Areas

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

