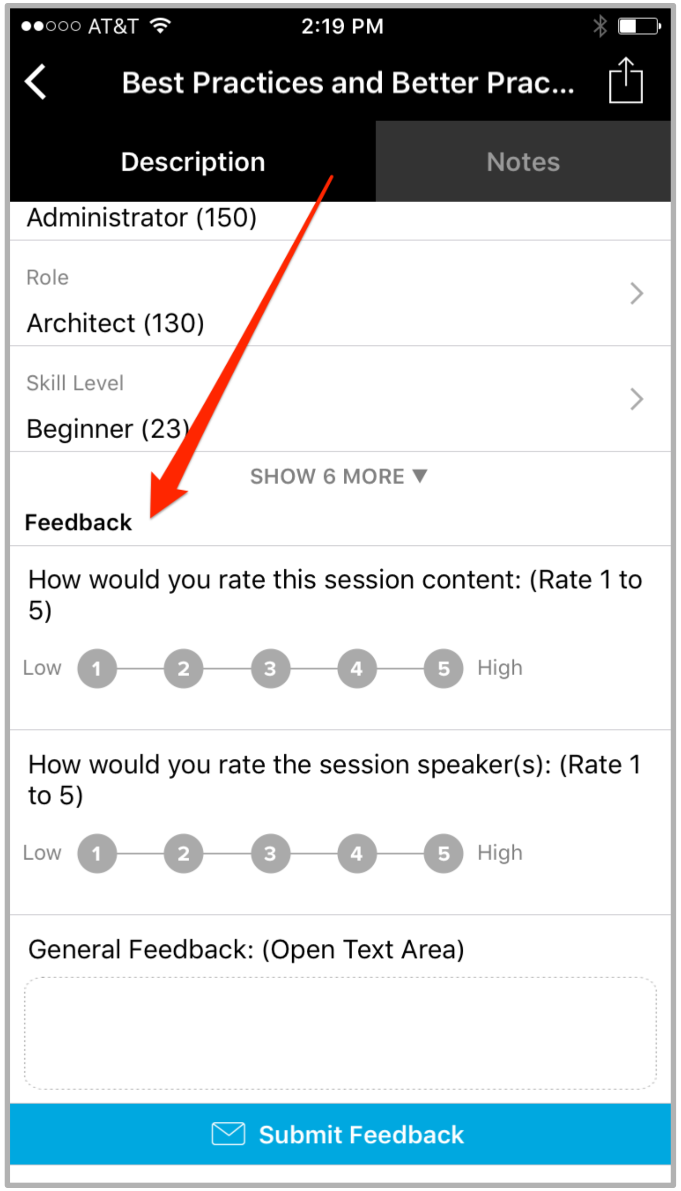
© 2017 SPLUNK INC.

Blueprints for Onboarding Teams

…while you get settled…

- Latest Slides:
  - https://splunk.box.com/v/blueprints-onboarding-teams
- Collaborate: #success
  - Sign Up @ http://splk.it/slack
- Load Feedback --------------------------------------->


●●○○○ AT&T 2:19 PM

Best Practices and Better Prac...

Description | Notes

Administrator (150)

Role

Architect (130)

Skill Level

Beginner (23)

SHOW 6 MORE ▼

Feedback

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

Low ① ② ③ ④ ⑤ High

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

Low ① ② ③ ④ ⑤ High

General Feedback: (Open Text Area)

Submit Feedback

© 2017 SPLUNK INC.

splunk> .conf2017

Blueprints for Onboarding Teams

Presented by Splunk Blueprints

Burch | Senior Best Practices Engineer

.conf2017 | Version 0.0

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. © 2017 Splunk Inc. All rights reserved.

© 2017 SPLUNK INC.

Right Session?

Mo Teams,
Mo Problems.

splunk> .conf2017

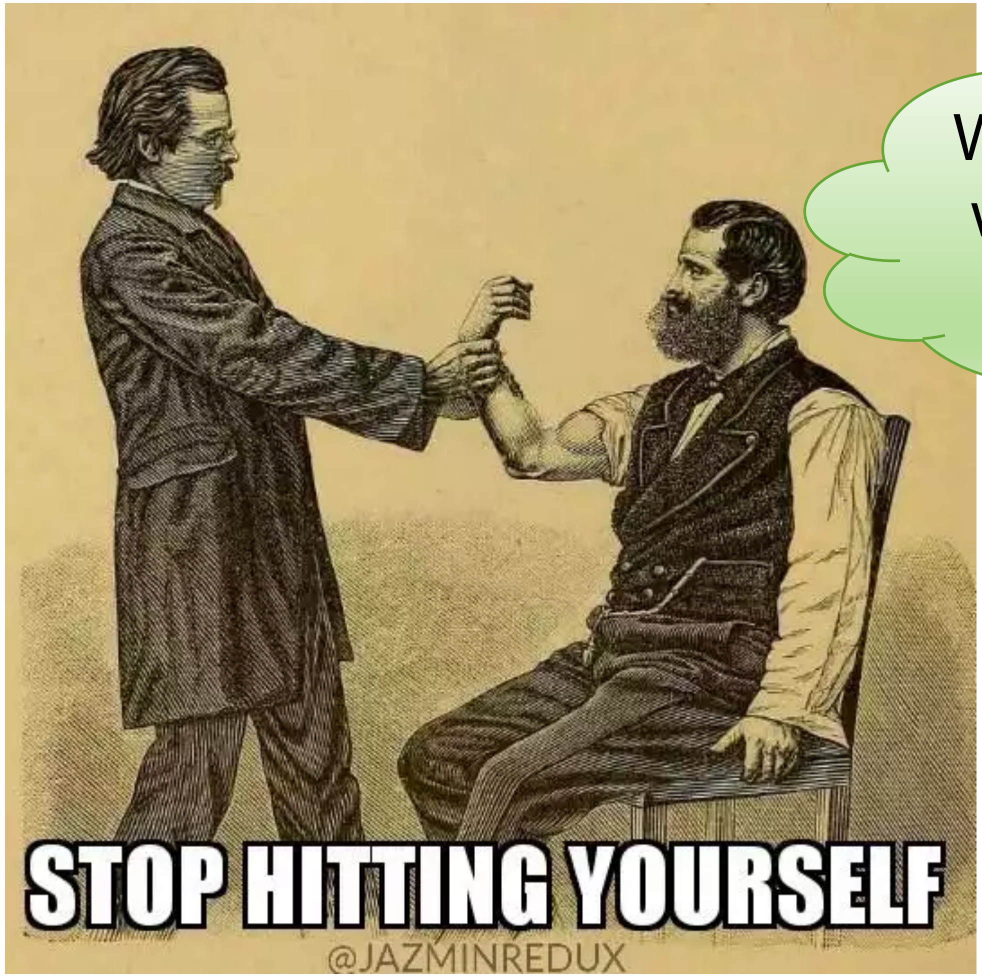
© 2017 SPLUNK INC.

Clutter clutter everywhere…

Not yo’ Splunk on fleek.

© 2017 SPLUNK INC.

Admins got you all…

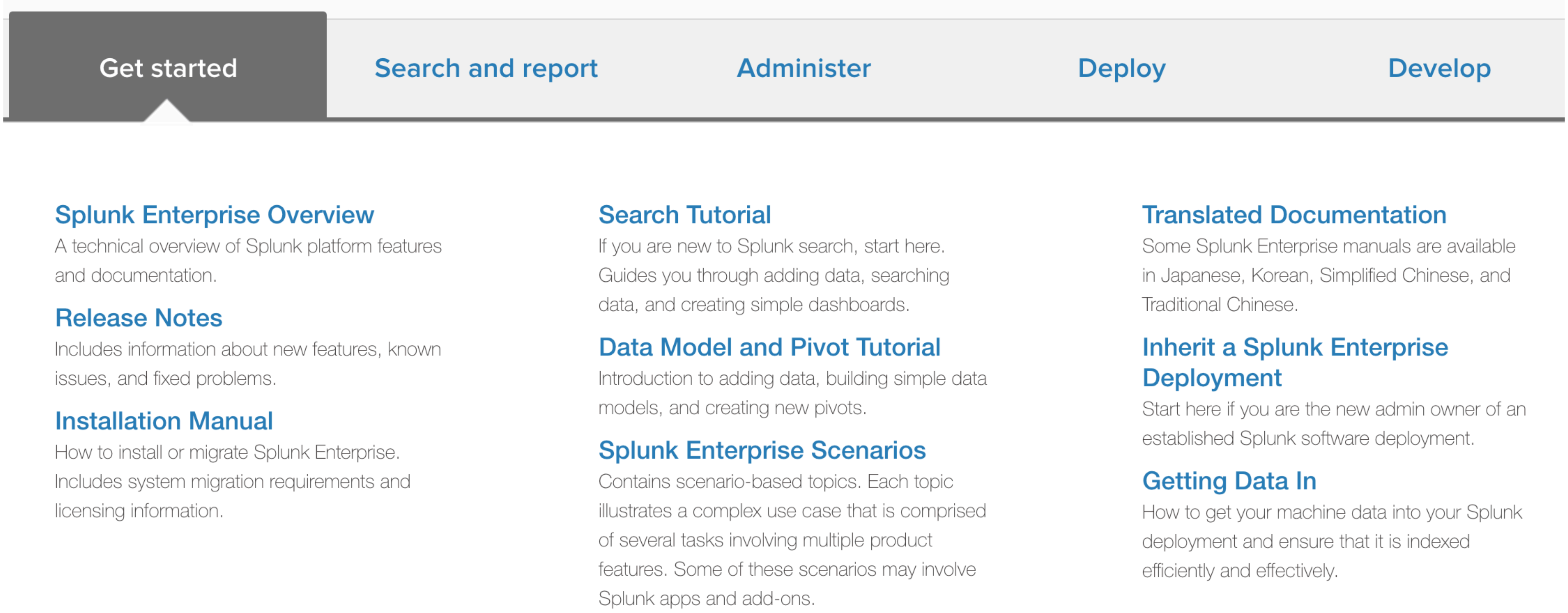


Well, if it’s so bad, why’d you let me do it?!

© 2017 SPLUNK INC.

What’s that? Want more places to look?

docs, and dev, and answers, oh my!



Splunk Enterprise Overview

A technical overview of Splunk platform features and documentation.

Release Notes

Includes information about new features, known issues, and fixed problems.

Installation Manual

How to install or migrate Splunk Enterprise. Includes system migration requirements and licensing information.

Search Tutorial

If you are new to Splunk search, start here. Guides you through adding data, searching data, and creating simple dashboards.

Data Model and Pivot Tutorial

Introduction to adding data, building simple data models, and creating new pivots.

Splunk Enterprise Scenarios

Contains scenario-based topics. Each topic illustrates a complex use case that is comprised of several tasks involving multiple product features. Some of these scenarios may involve Splunk apps and add-ons.

Translated Documentation

Some Splunk Enterprise manuals are available in Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Inherit a Splunk Enterprise Deployment

Start here if you are the new admin owner of an established Splunk software deployment.

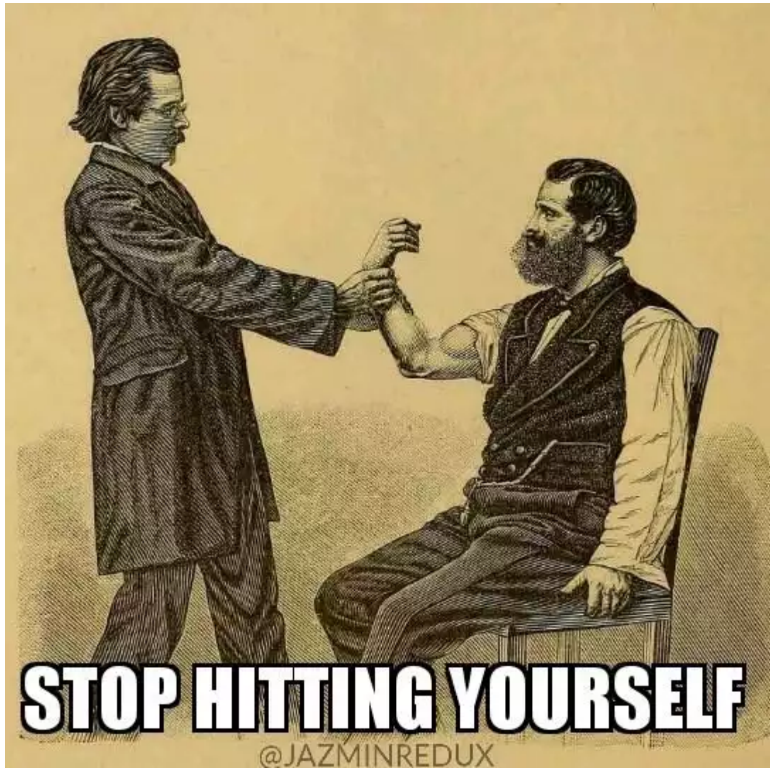
Getting Data In

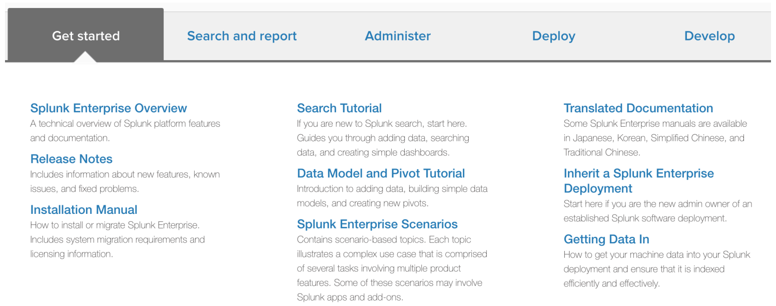
How to get your machine data into your Splunk deployment and ensure that it is indexed efficiently and effectively.

© 2017 SPLUNK INC.

Domains-o-Discussion

tots kewl to bounce





Splunk Enterprise Overview
A technical overview of Splunk platform features and documentation.

Release Notes
Includes information about new features, known issues, and fixed problems.

Installation Manual
How to install or migrate Splunk Enterprise. Includes system migration requirements and licensing information.

Search Tutorial
If you are new to Splunk search, start here. Guides you through adding data, searching data, and creating simple dashboards.

Data Model and Pivot Tutorial
Introduction to adding data, building simple data models, and creating new pivots.

Splunk Enterprise Scenarios
Contains scenario-based topics. Each topic illustrates a complex use case that is comprised of several tasks involving multiple product features. Some of these scenarios may involve Splunk apps and add-ons.

Translated Documentation
Some Splunk Enterprise manuals are available in Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Inherit a Splunk Enterprise Deployment
Start here if you are the new admin owner of an established Splunk software deployment.

Getting Data In
How to get your machine data into your Splunk deployment and ensure that it is indexed efficiently and effectively.

© 2017 SPLUNK INC.

What's a "Burch"?

Senior Best Practices Engineer

- Was a Senior Sales Engineer
- Before that, Splunk **Customer**
- Before that, Middleware Eng
- Before that, Computer Science
- Before that, an idea of my parents

© 2017 SPLUNK INC.

“Scale customer success through the automation of adoption services and best practices”

Blueprint’s Mission

© 2017 SPLUNK INC.

Our World Today

© 2017 SPLUNK INC.

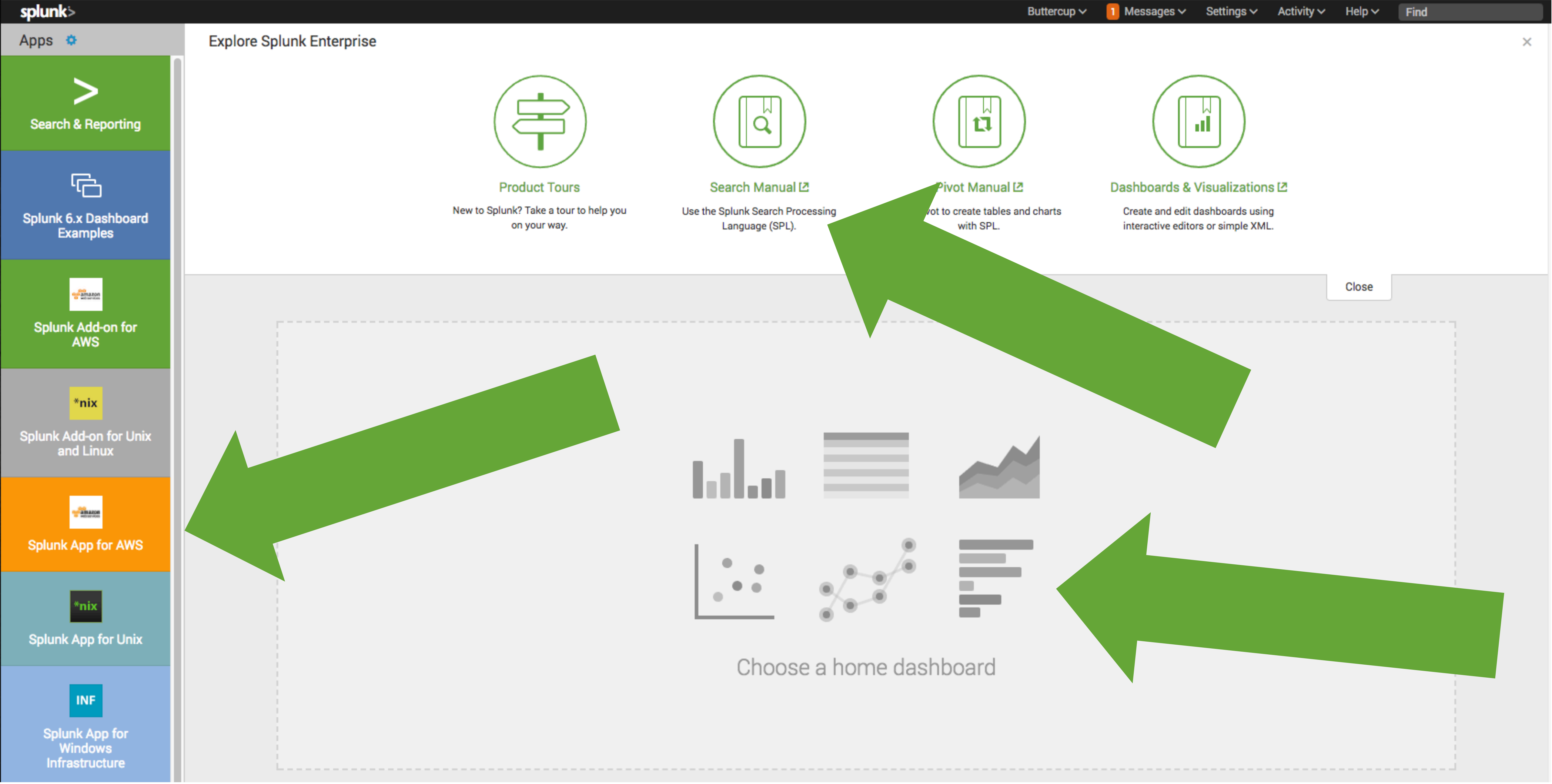
Who wants to role play?

Choose Your Own Adventure!

© 2017 SPLUNK INC.

Scenario

- New employee at Buttercup Games
- Responsibilities include Data Driven Decisions (so power user)
- Lied on your resume about Splunk experience (no experience)
- Company has no HR. Punishment is Pony Diaper Duty (pun intended)
- Just got Splunk access and you log in to see…



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

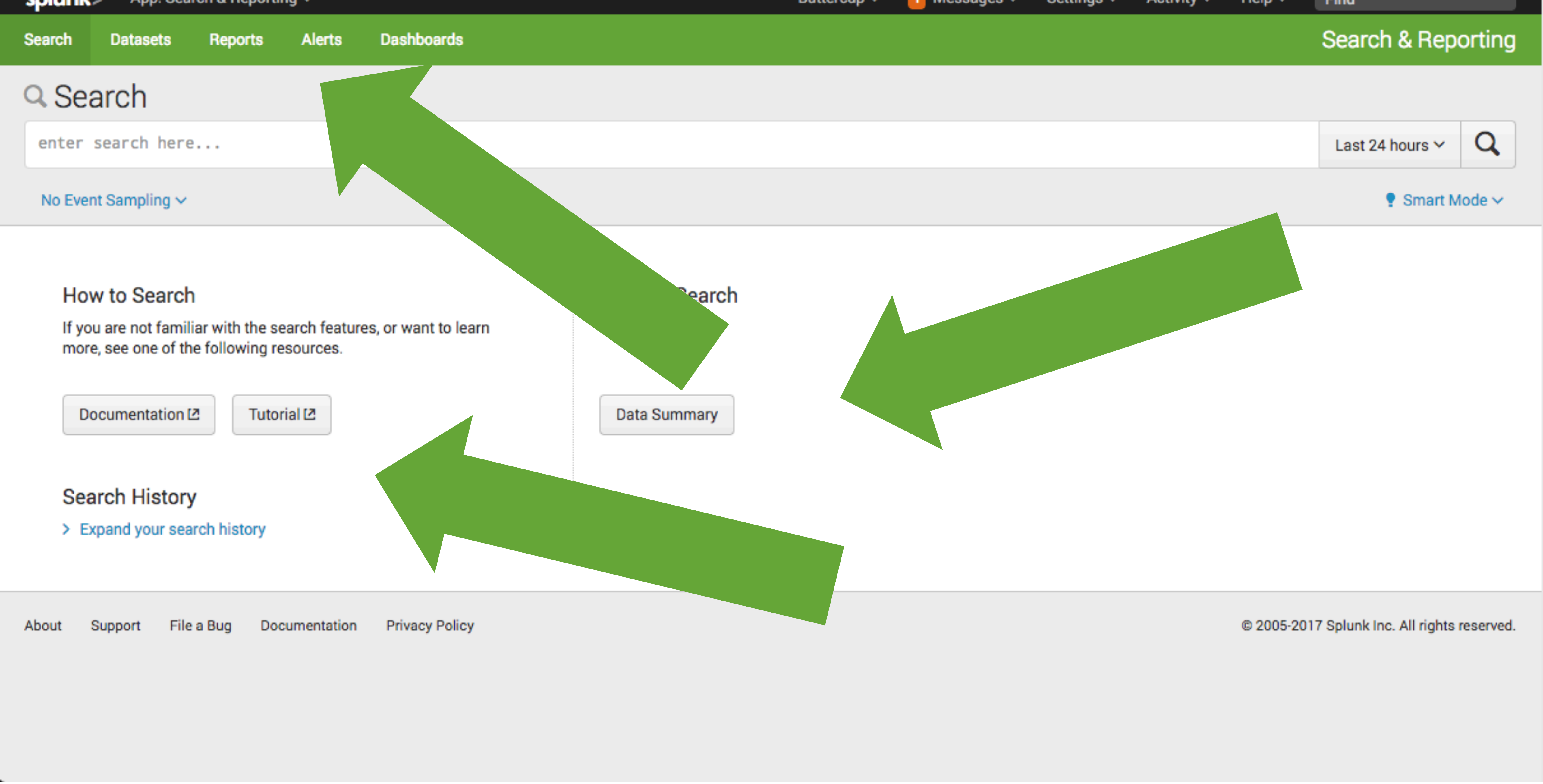
Search Manual
Use the Splunk Search Processing Language (SPL).

Pivot Manual
…vot to create tables and charts with SPL.

Dashboards & Visualizations
Create and edit dashboards using interactive editors or simple XML.

Choose a home dashboard

- Search & Reporting
- Splunk 6.x Dashboard Examples
- Splunk Add-on for AWS
- Splunk Add-on for Unix and Linux
- Splunk App for AWS
- Splunk App for Unix
- Splunk App for Windows Infrastructure

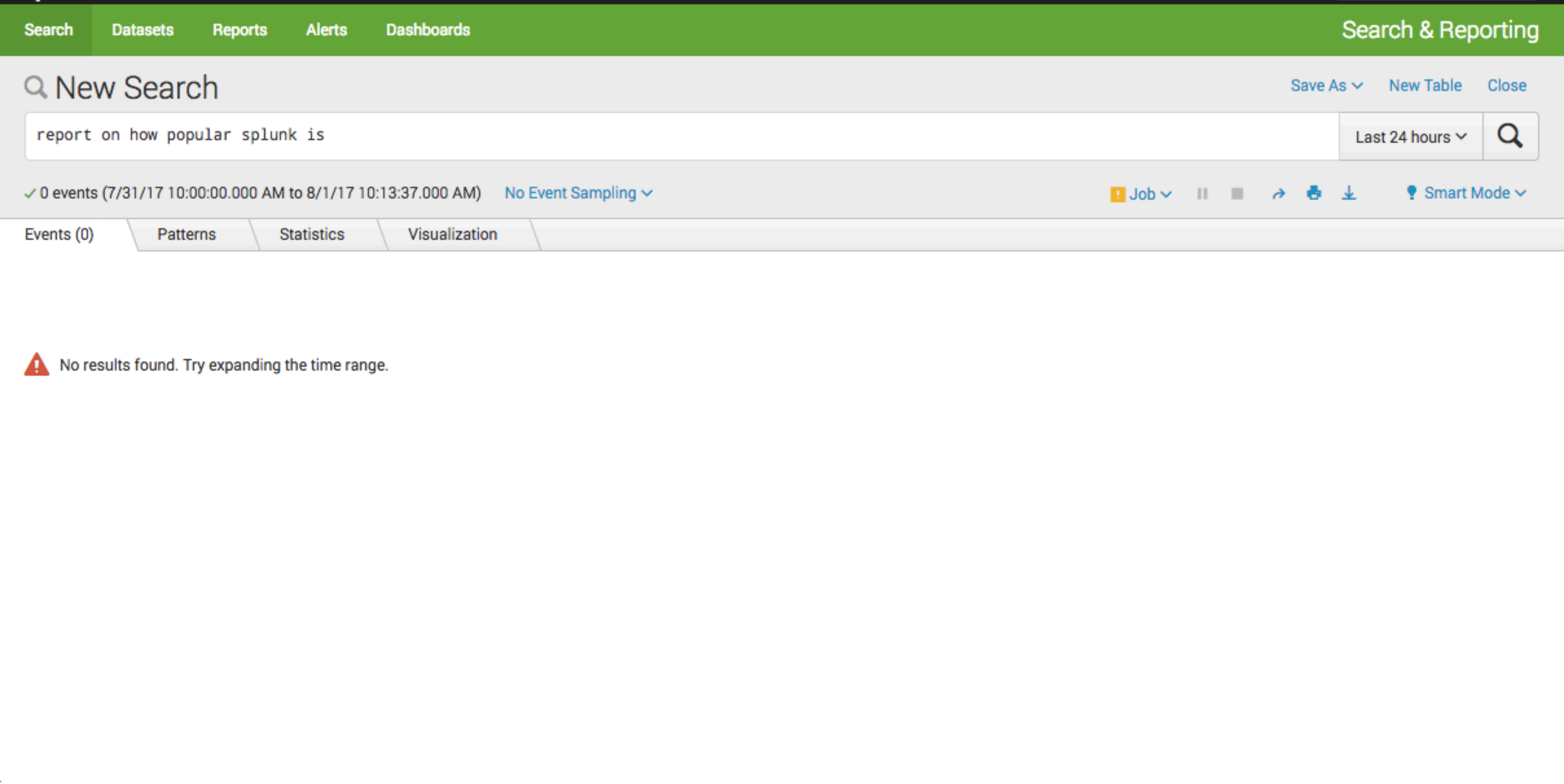


How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

Search History

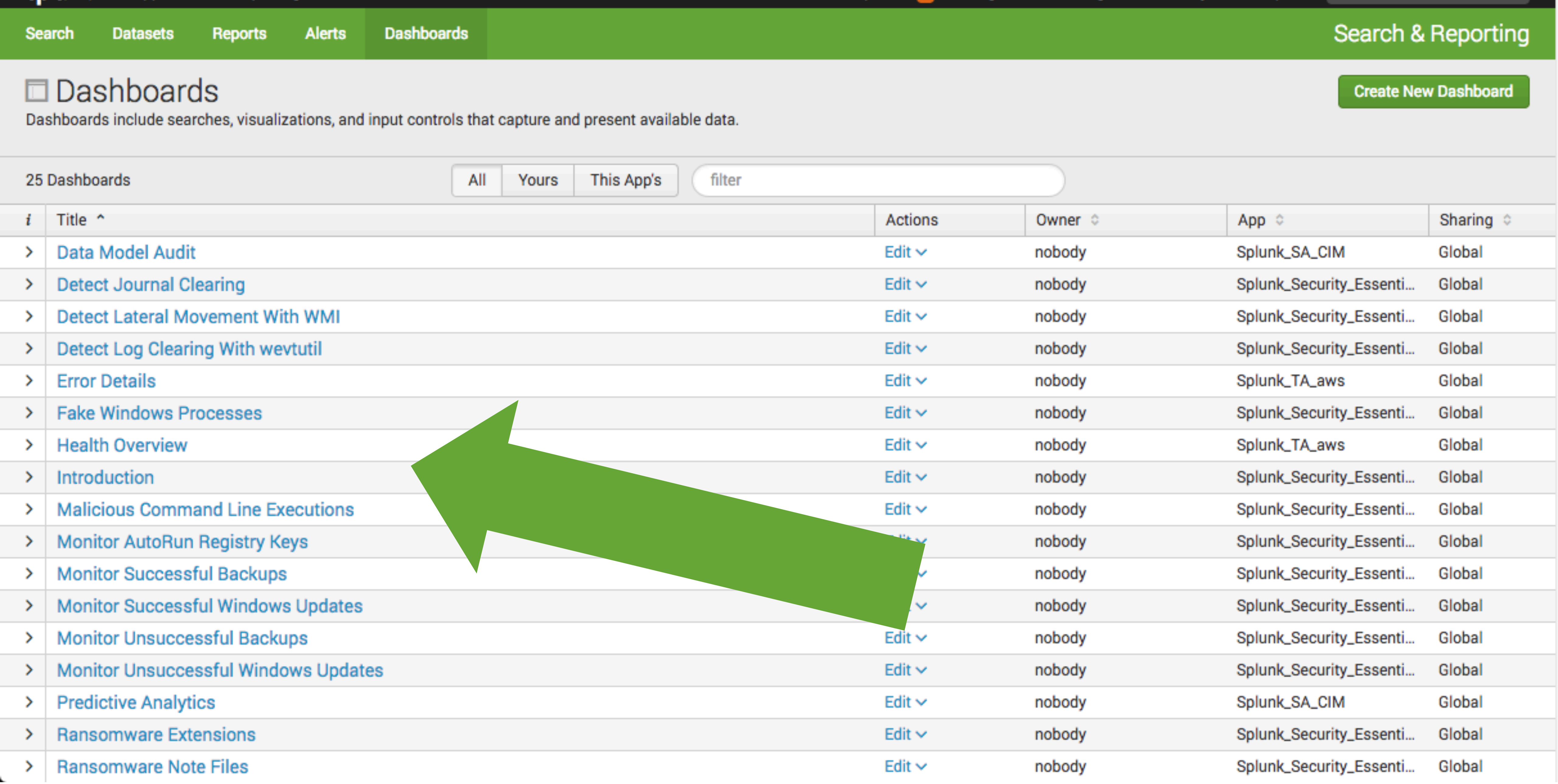
© 2005-2017 Splunk Inc. All rights reserved.



```
report on how popular splunk is
```

✓ 0 events (7/31/17 10:00:00.000 AM to 8/1/17 10:13:37.000 AM)

No results found. Try expanding the time range.



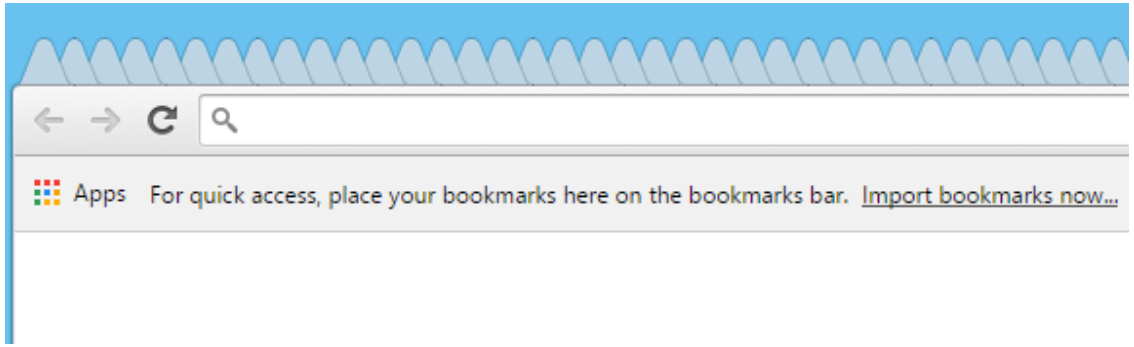
Dashboards

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

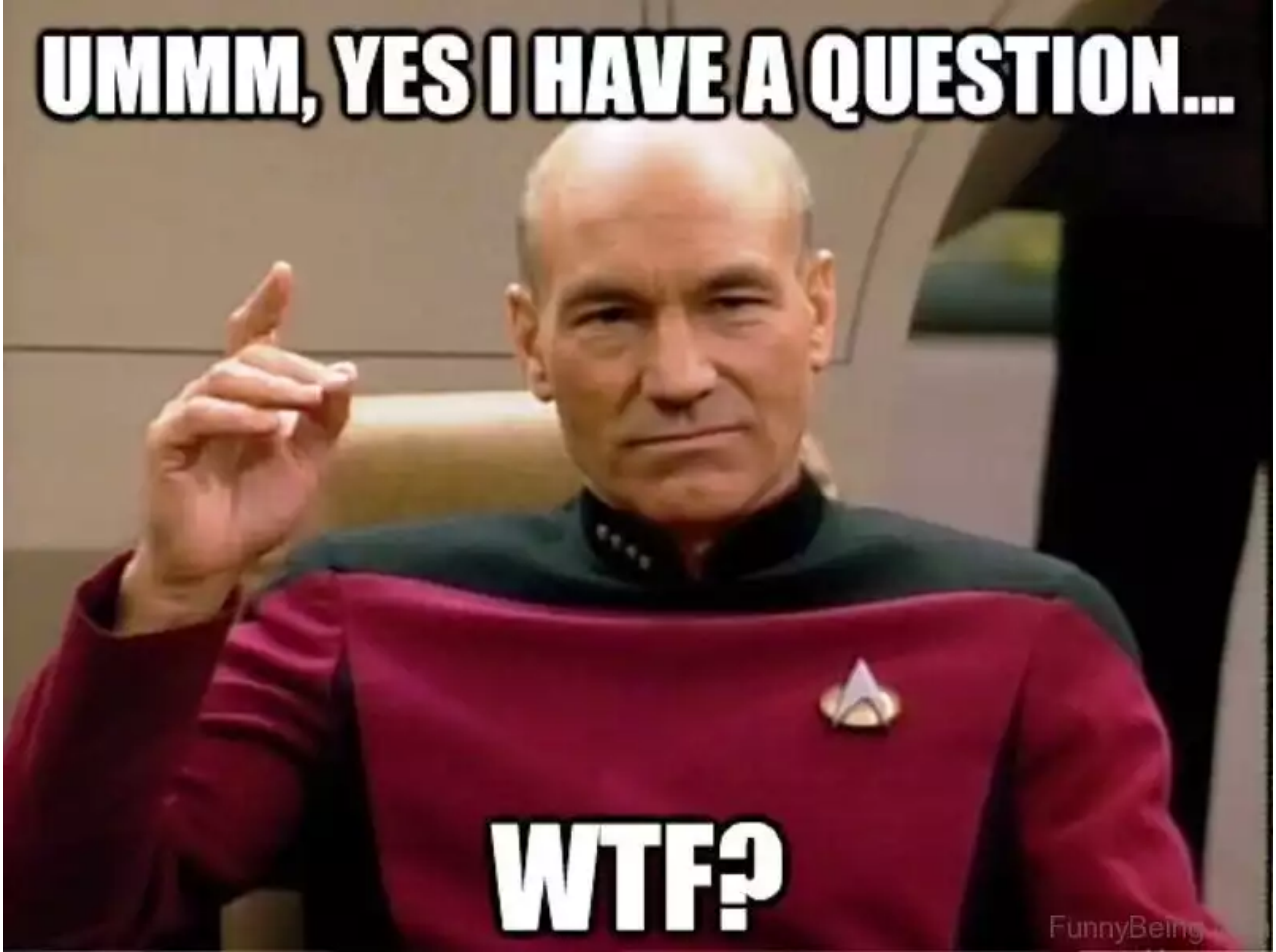
25 Dashboards

i	Title ^	Actions	Owner	App	Sharing
>	Data Model Audit	Edit ⌄	nobody	Splunk_SA_CIM	Global
>	Detect Journal Clearing	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Detect Lateral Movement With WMI	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Detect Log Clearing With wevtutil	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Error Details	Edit ⌄	nobody	Splunk_TA_aws	Global
>	Fake Windows Processes	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Health Overview	Edit ⌄	nobody	Splunk_TA_aws	Global
>	Introduction	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Malicious Command Line Executions	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Monitor AutoRun Registry Keys	[illegible]	nobody	Splunk_Security_Essenti...	Global
>	Monitor Successful Backups	[illegible]	nobody	Splunk_Security_Essenti...	Global
>	Monitor Successful Windows Updates	[illegible]	nobody	Splunk_Security_Essenti...	Global
>	Monitor Unsuccessful Backups	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Monitor Unsuccessful Windows Updates	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Predictive Analytics	Edit ⌄	nobody	Splunk_SA_CIM	Global
>	Ransomware Extensions	Edit ⌄	nobody	Splunk_Security_Essenti...	Global
>	Ransomware Note Files	Edit ⌄	nobody	Splunk_Security_Essenti...	Global

All the Dashboards!



Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...


UMMM, YES I HAVE A QUESTION...
WTF?
FunnyBeing

I DEAL WITH THE GOD DAMN CUSTOMERS
SO THE ENGINEERS DON'T HAVE TO
weknowmem

Doug M.

I DEAL WITH THE GOD DAMN CUSTOMERS
SO THE ENGINEERS DON'T HAVE TO
weknowmem

D. Merritt

I DEAL WITH THE GOD DAMN CUSTOMERS
SO THE ENGINEERS DON'T HAVE TO
weknowmem

index=*

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

© 2017 SPLUNK INC.

Solution, you have?!

© 2017 SPLUNK INC.

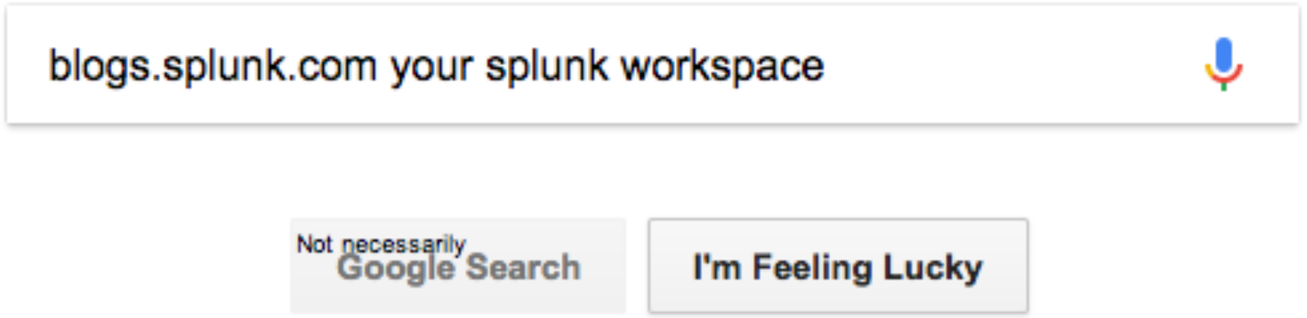
Three Concepts

Let’s pause and explore some new ideas

© 2017 SPLUNK INC.

Workspaces

Concept I of III



blogs.splunk.com your splunk workspace

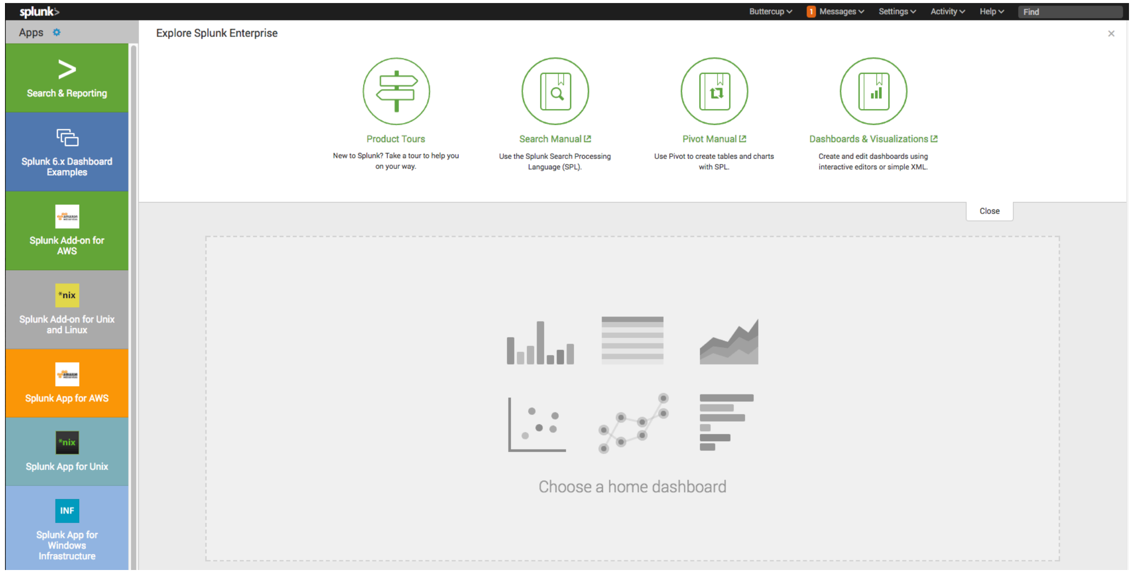
© 2017 SPLUNK INC.

Workspace

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

© 2017 SPLUNK INC.

…so why do we do that in Splunk?



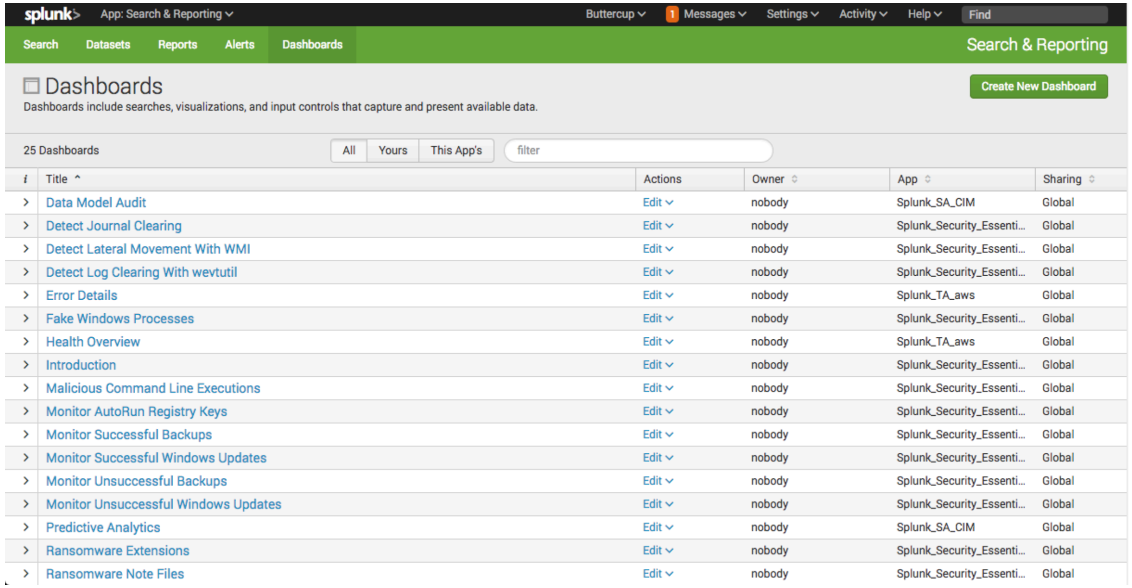
Explore Splunk Enterprise

Product Tours: New to Splunk? Take a tour to help you on your way.

Search Manual: Use the Splunk Search Processing Language (SPL).

Pivot Manual: Use Pivot to create tables and charts with SPL.

Dashboards & Visualizations: Create and edit dashboards using interactive editors or simple XML.



Dashboards

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

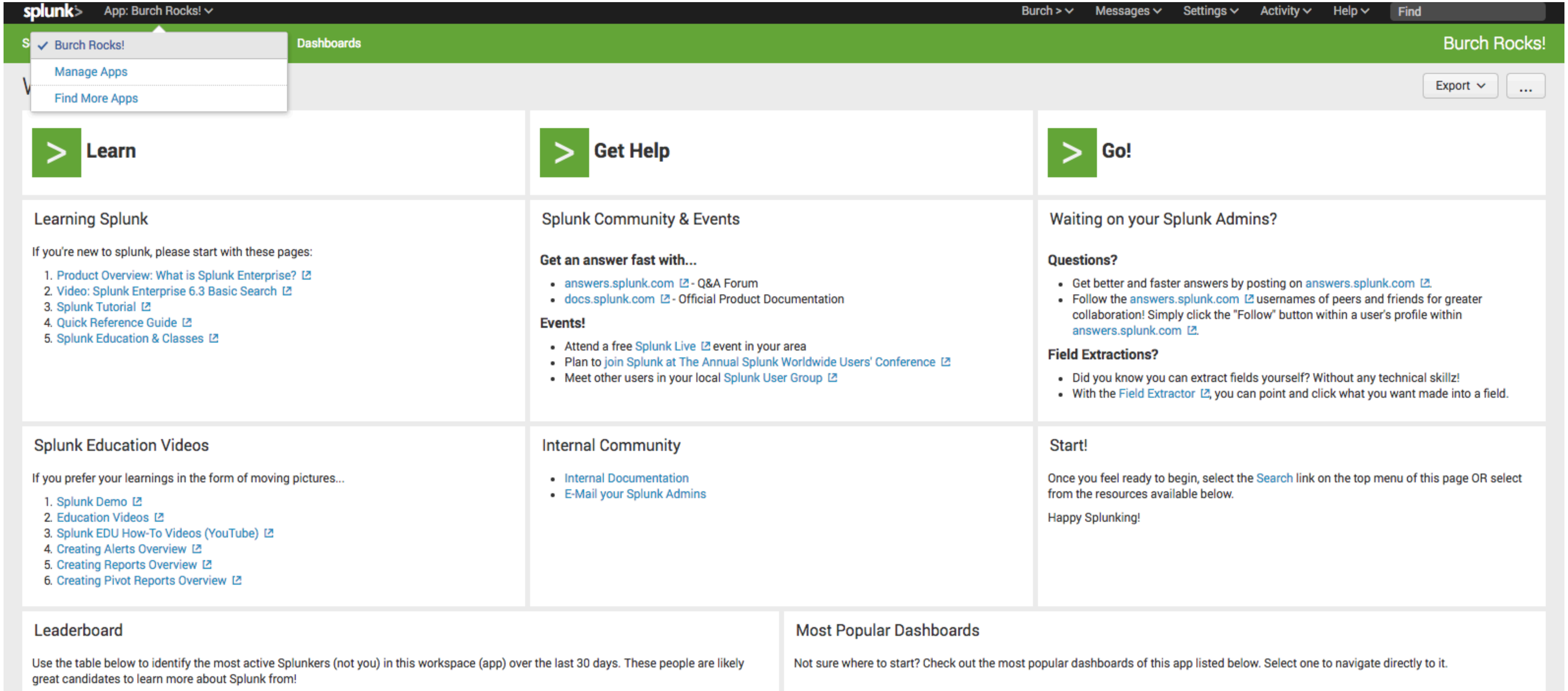
25 Dashboards

i	Title	Actions	Owner	App	Sharing
>	Data Model Audit	Edit	nobody	Splunk_SA_CIM	Global
>	Detect Journal Clearing	Edit	nobody	Splunk_Security_Essenti...	Global
>	Detect Lateral Movement With WMI	Edit	nobody	Splunk_Security_Essenti...	Global
>	Detect Log Clearing With wevtutil	Edit	nobody	Splunk_Security_Essenti...	Global
>	Error Details	Edit	nobody	Splunk_TA_aws	Global
>	Fake Windows Processes	Edit	nobody	Splunk_Security_Essenti...	Global
>	Health Overview	Edit	nobody	Splunk_TA_aws	Global
>	Introduction	Edit	nobody	Splunk_Security_Essenti...	Global
>	Malicious Command Line Executions	Edit	nobody	Splunk_Security_Essenti...	Global
>	Monitor AutoRun Registry Keys	Edit	nobody	Splunk_Security_Essenti...	Global
>	Monitor Successful Backups	Edit	nobody	Splunk_Security_Essenti...	Global
>	Monitor Successful Windows Updates	Edit	nobody	Splunk_Security_Essenti...	Global
>	Monitor Unsuccessful Backups	Edit	nobody	Splunk_Security_Essenti...	Global
>	Monitor Unsuccessful Windows Updates	Edit	nobody	Splunk_Security_Essenti...	Global
>	Predictive Analytics	Edit	nobody	Splunk_SA_CIM	Global
>	Ransomware Extensions	Edit	nobody	Splunk_Security_Essenti...	Global
>	Ransomware Note Files	Edit	nobody	Splunk_Security_Essenti...	Global

© 2017 SPLUNK INC.

App as a Workspaces

Dedicated to one team/group/purpose



> Learn

> Get Help

> Go!

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

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

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 skillz!
- With the Field Extractor, you can point and click what you want made into a field.

Splunk Education Videos

If you prefer your learnings in the form of moving pictures...

1. Splunk Demo
2. Education Videos
3. Splunk EDU How-To Videos (YouTube)
4. Creating Alerts Overview
5. Creating Reports Overview
6. Creating Pivot Reports Overview

Internal Community

- Internal Documentation
- E-Mail your Splunk Admins

Start!

Once you feel ready to begin, select the Search link on the top menu of this page OR select from the resources available below.

Happy Splunking!

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!

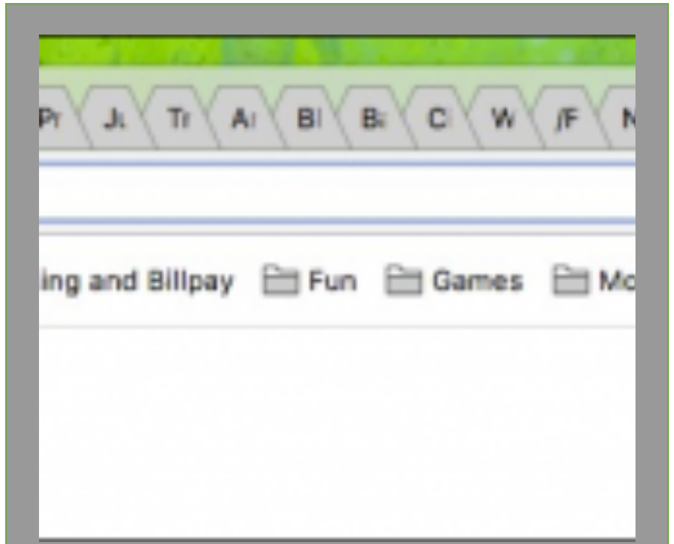
Most Popular Dashboards

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

© 2017 SPLUNK INC.

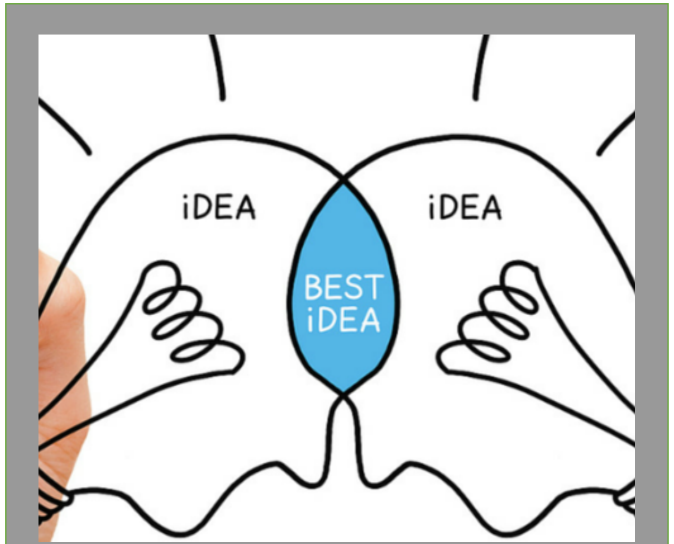
Benefits

Increases in…



Safety

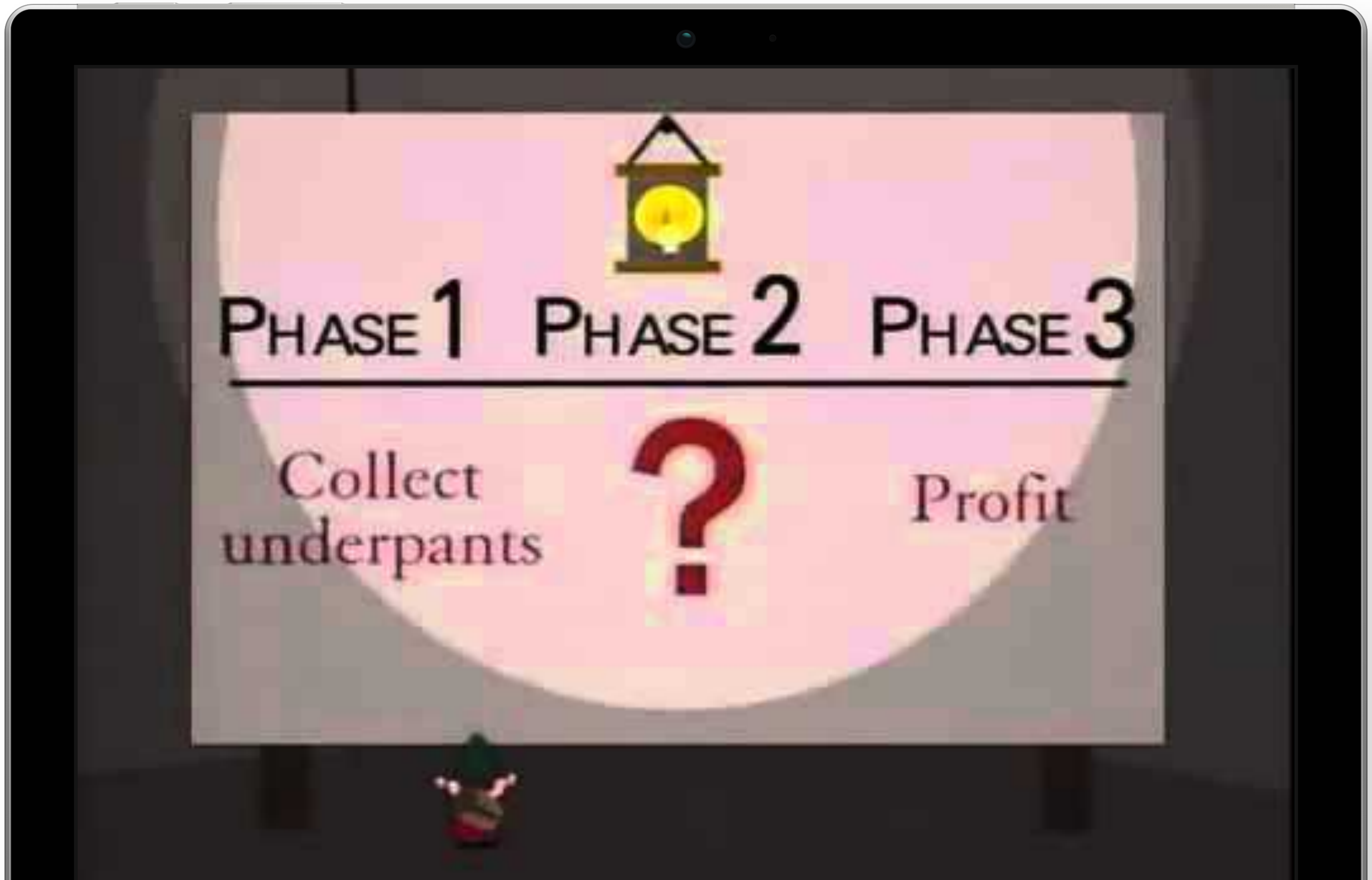
Risk led learning



Discovery led collaboration

© 2017 SPLUNK INC.

Implementation

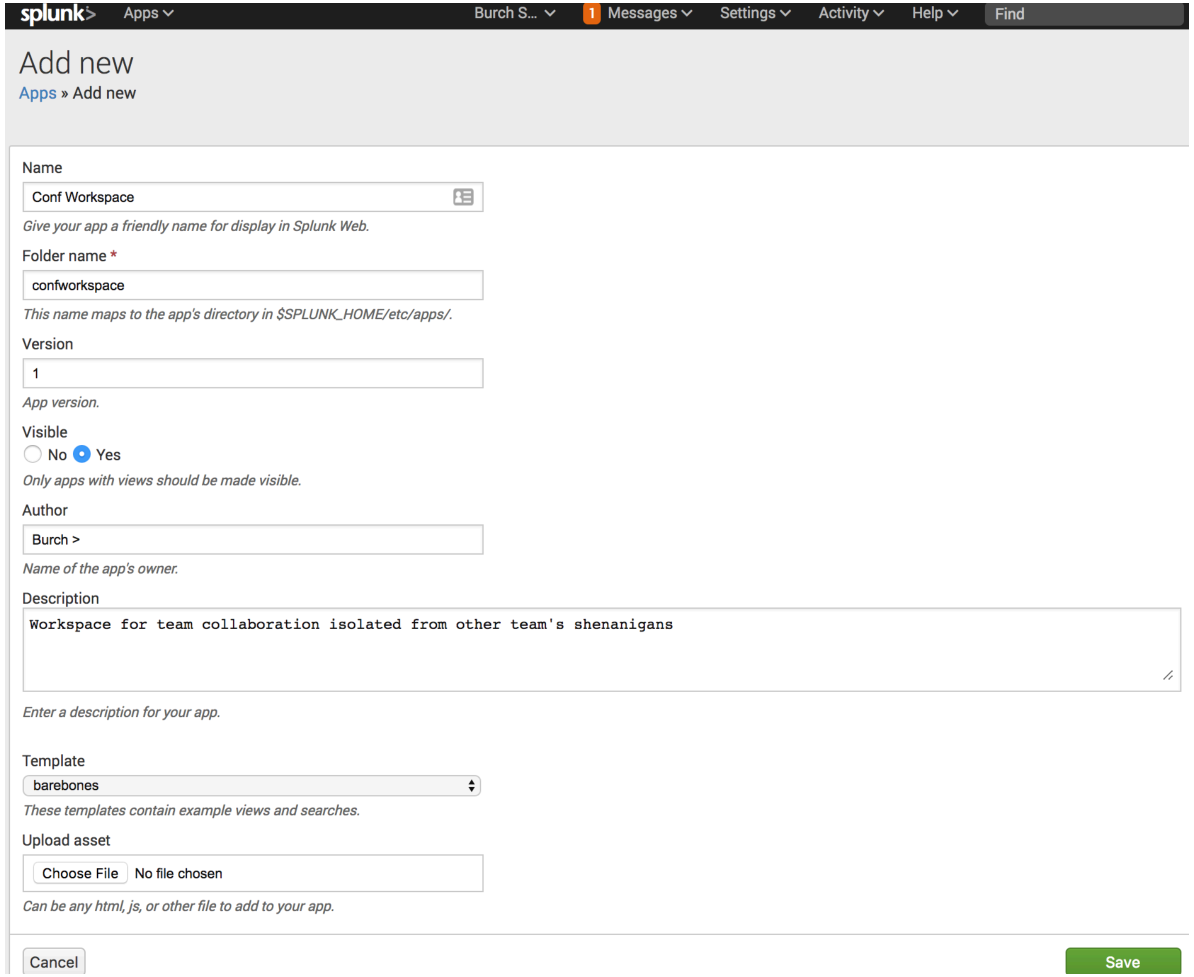


1. Create an app
2. Set permissions
3. Set as role default
4. Profit

© 2017 SPLUNK INC.

Step 1: Create an app

http://dev.splunk.com/view/SP-CAAAEUC



Add new

Apps » Add new

Name
Conf Workspace
Give your app a friendly name for display in Splunk Web.

Folder name *
confworkspace
This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.

Version
1
App version.

Visible
○ No ● Yes
Only apps with views should be made visible.

Author
Burch >
Name of the app's owner.

Description
```
Workspace for team collaboration isolated from other team's shenanigans
```
Enter a description for your app.

Template
barebones
These templates contain example views and searches.

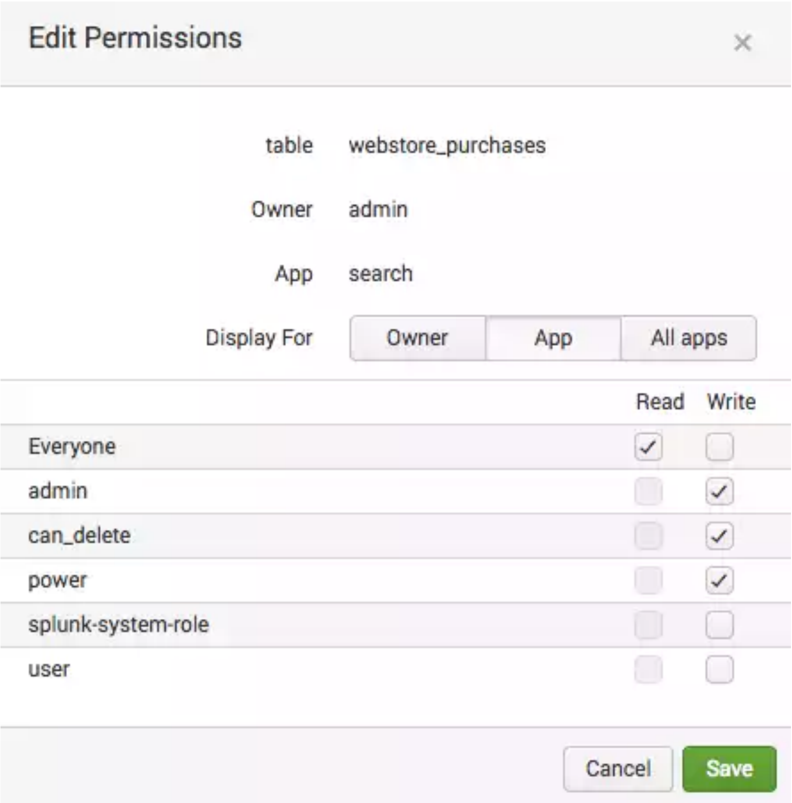
Upload asset
Choose File No file chosen
Can be any html, js, or other file to add to your app.

splunk> .conf2017

© 2017 SPLUNK INC.

Step 2: Set Permissions

Apps -> Manage Apps



Edit Permissions ×

table	webstore_purchases
Owner	admin
App	search
Display For	Owner / App / All apps

	Read	Write
Everyone	☑	☐
admin	☐	☑
can_delete	☐	☑
power	☐	☑
splunk-system-role	☐	☐
user	☐	☐

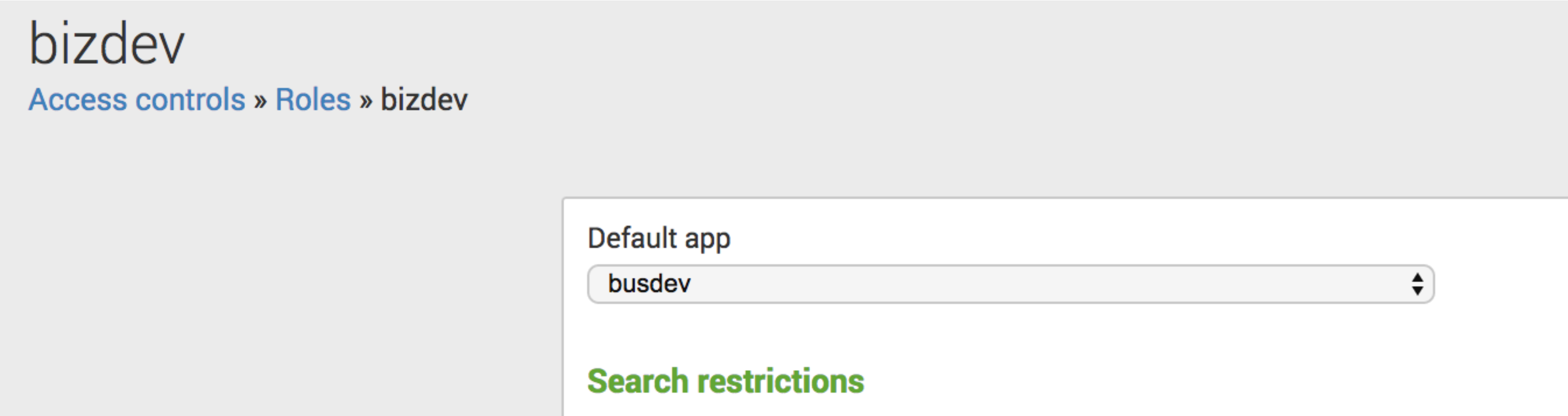
- “Hide” extraneous apps/workspaces:
  - Remove role’s read permissions
  - `app.conf`

```
[ui]
  ~~is_visible = false~~
  show_in_nav = false
```

© 2017 SPLUNK INC.

Step 3: Set Role Default

Bypasses launcher. Guides user to workspace.



bizdev

Access controls » Roles » bizdev

Default app: busdev

Search restrictions

appname/local/user-prefs.conf

```
[role_capability_admin]
        default_namespace = workspace_app
```

appname/metadata/local.meta

```
[ui-prefs]
        export = system
```

© 2017 SPLUNK INC.

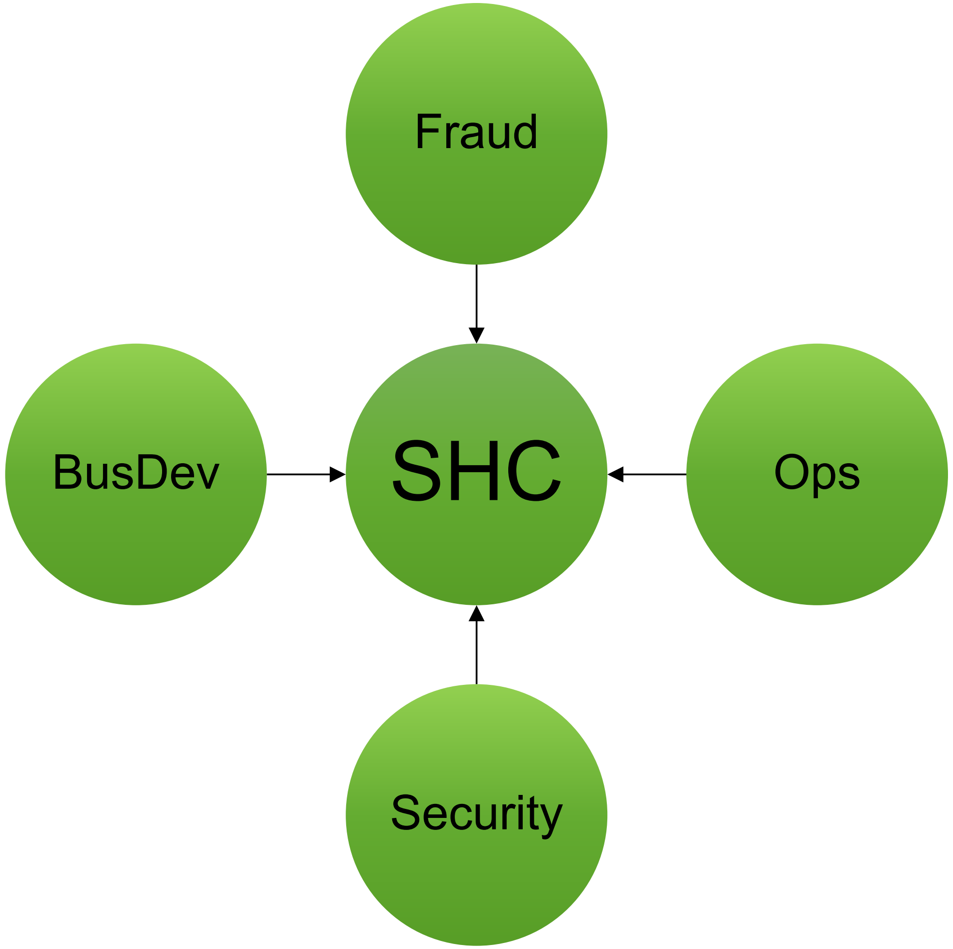
Step 4: Profit

$$ Everyone get a search head $$

© 2017 SPLUNK INC.

Step 4: Profit

Collapsing Search Heads



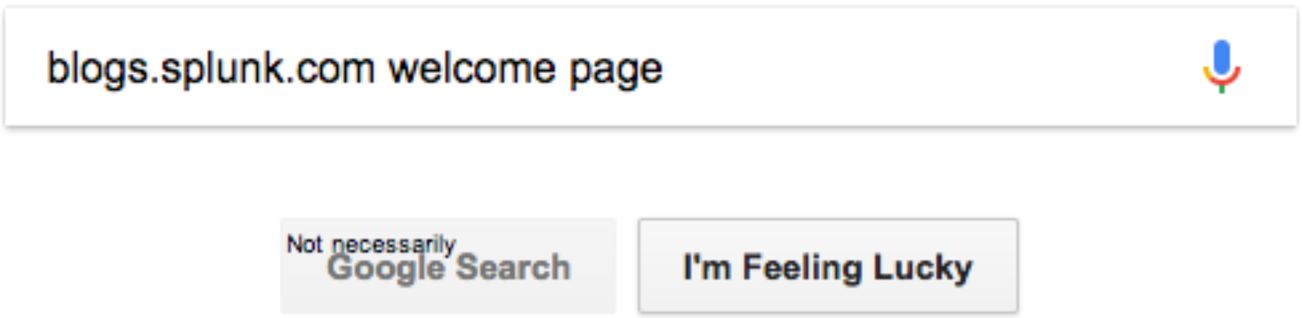
- Users still navigate to their FQDN
- DNS directs to SHC
  - Not dedicated SH
- Same experience as before
  - default app
  - hiding other workspaces

splunk> .conf2017

© 2017 SPLUNK INC.

Welcome Page

Concept II of III



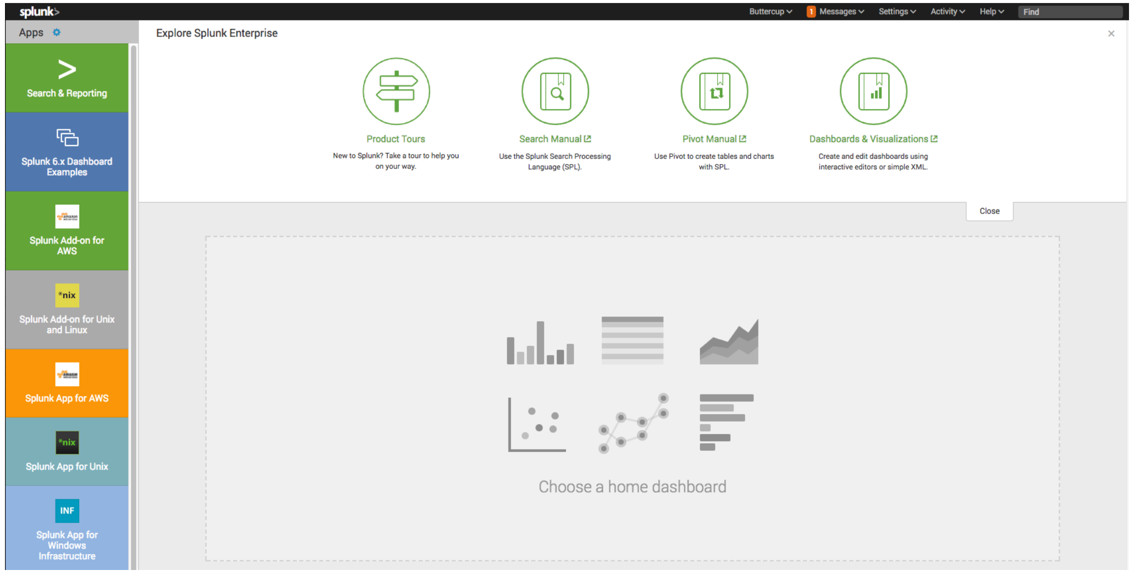
blogs.splunk.com welcome page

Not necessarily

© 2017 SPLUNK INC.

Oh, the Places You’ll Go

Too many options!

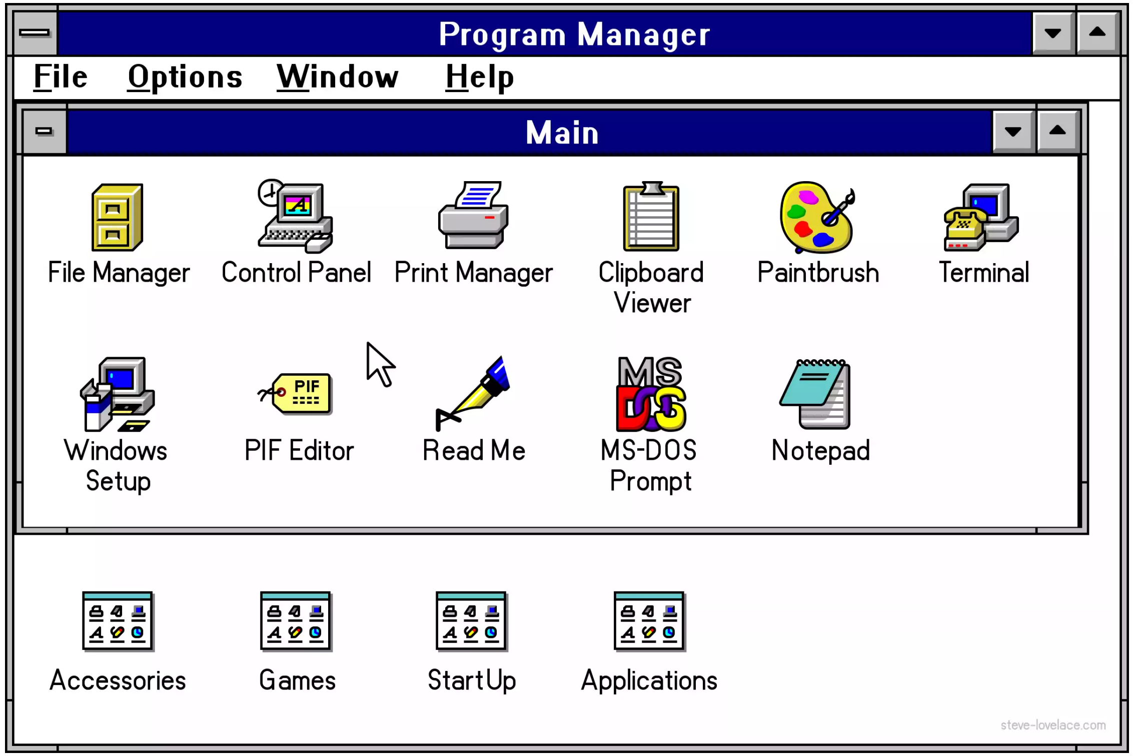


New to Splunk? Take a tour to help you on your way.

Use the Splunk Search Processing Language (SPL).

Use Pivot to create tables and charts with SPL.

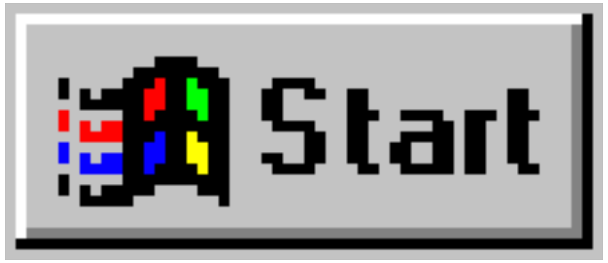
Create and edit dashboards using interactive editors or simple XML.



© 2017 SPLUNK INC.

Same Challenge. Different Platforms.

What did this button do for user design?

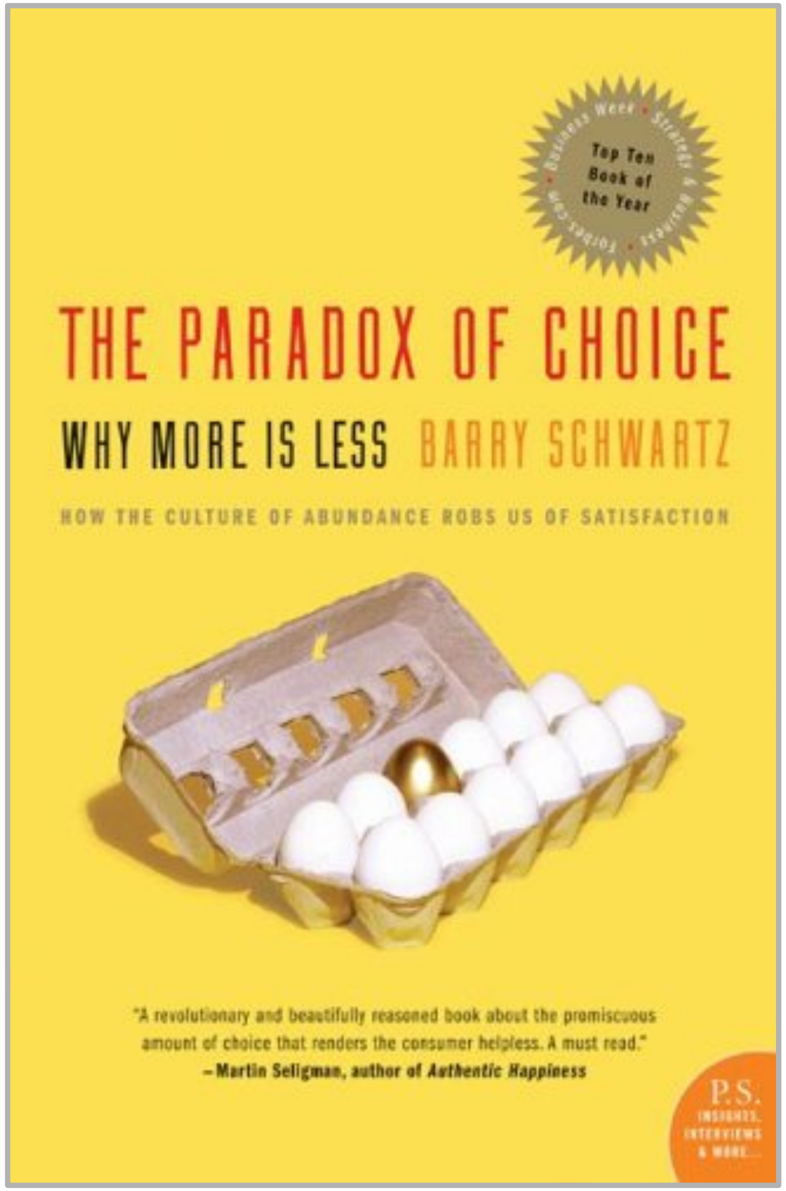


- Mislead?
- Restrict?
- Guidance!
- Confidence!
- Comfort!

© 2017 SPLUNK INC.

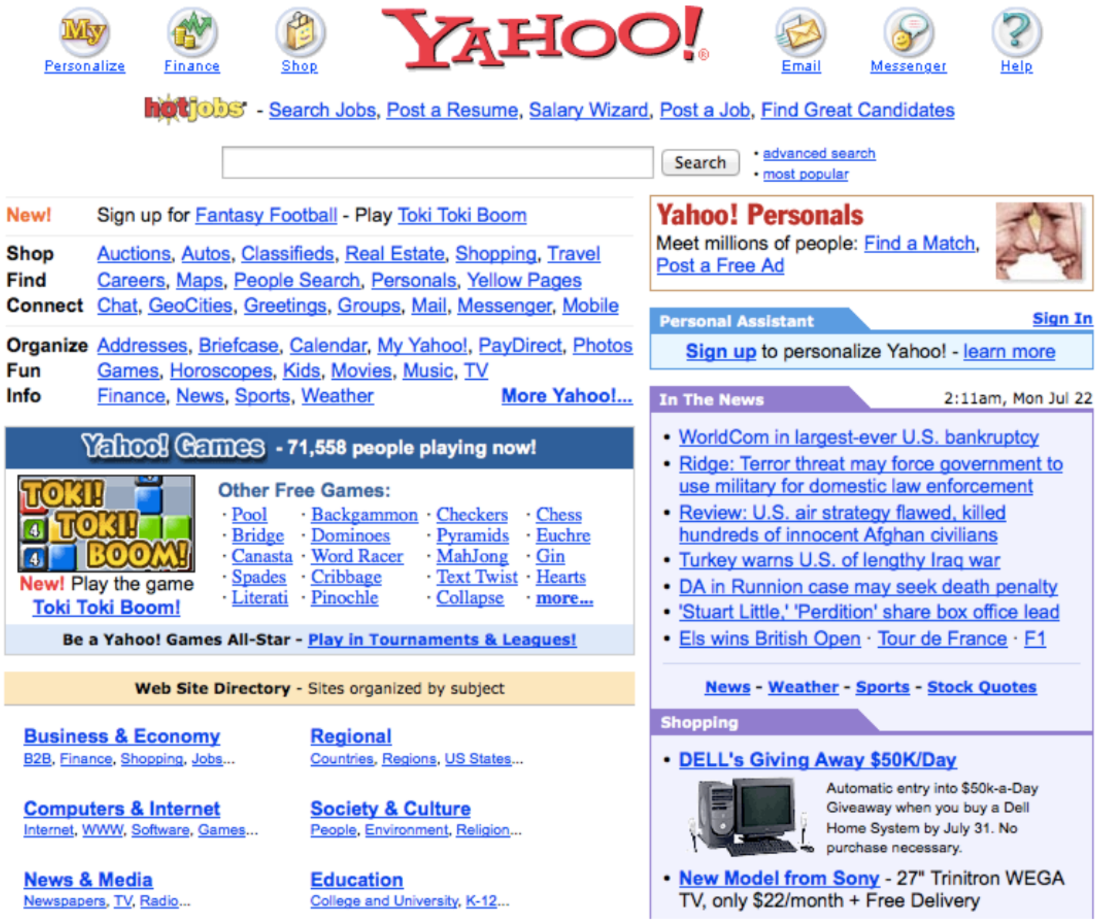
The Paradox of Choice

“eliminating consumer choices can greatly reduce anxiety”


Business Week • Strategy & Business • Forbes.com
Top Ten Book of the Year
THE PARADOX OF CHOICE
WHY MORE IS LESS
BARRY SCHWARTZ
HOW THE CULTURE OF ABUNDANCE ROBS US OF SATISFACTION
"A revolutionary and beautifully reasoned book about the promiscuous amount of choice that renders the consumer helpless. A must read."
—Martin Seligman, author of Authentic Happiness
P.S.
INSIGHTS, INTERVIEWS & MORE...

© 2017 SPLUNK INC.

Same Challenge. Different Platforms.



hotjobs - Search Jobs, Post a Resume, Salary Wizard, Post a Job, Find Great Candidates

Search · advanced search · most popular

New! Sign up for Fantasy Football - Play Toki Toki Boom

Shop Auctions, Autos, Classifieds, Real Estate, Shopping, Travel
Find Careers, Maps, People Search, Personals, Yellow Pages
Connect Chat, GeoCities, Greetings, Groups, Mail, Messenger, Mobile

Organize Addresses, Briefcase, Calendar, My Yahoo!, PayDirect, Photos
Fun Games, Horoscopes, Kids, Movies, Music, TV
Info Finance, News, Sports, Weather More Yahoo!...

Yahoo! Games - 71,558 people playing now!

TOKI! TOKI! BOOM!

New! Play the game Toki Toki Boom!

Other Free Games:
· Pool · Backgammon · Checkers · Chess
· Bridge · Dominoes · Pyramids · Euchre
· Canasta · Word Racer · MahJong · Gin
· Spades · Cribbage · Text Twist · Hearts
· Literati · Pinochle · Collapse · more...

Be a Yahoo! Games All-Star - Play in Tournaments & Leagues!

Web Site Directory - Sites organized by subject

Business & Economy
B2B, Finance, Shopping, Jobs...

Regional
Countries, Regions, US States...

Computers & Internet
Internet, WWW, Software, Games...

Society & Culture
People, Environment, Religion...

News & Media
Newspapers, TV, Radio...

Education
College and University, K-12...

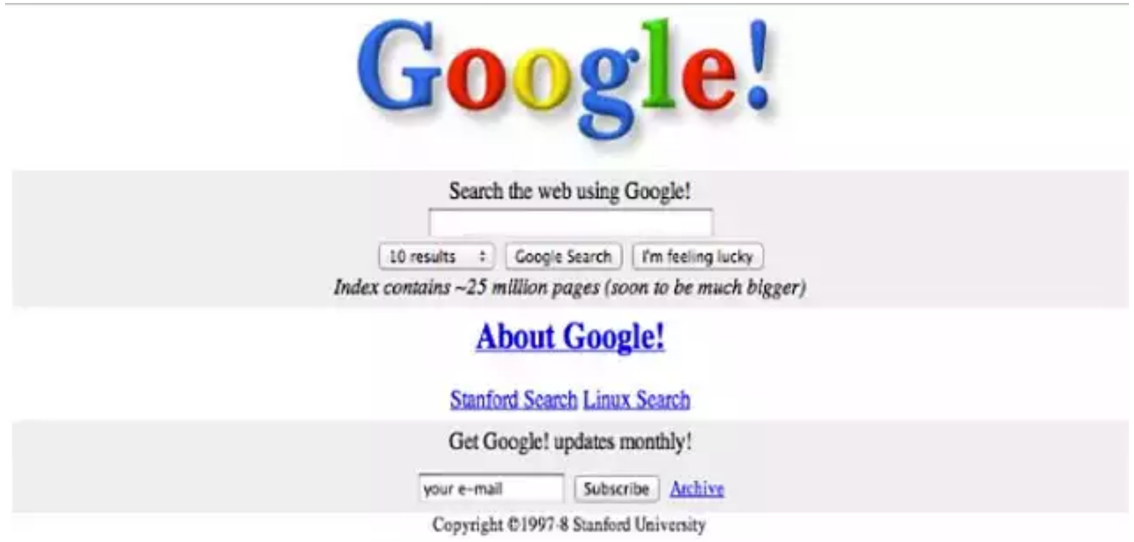
Yahoo! Personals
Meet millions of people: Find a Match, Post a Free Ad

Personal Assistant Sign In
Sign up to personalize Yahoo! - learn more

In The News 2:11am, Mon Jul 22
- WorldCom in largest-ever U.S. bankruptcy
- Ridge: Terror threat may force government to use military for domestic law enforcement
- Review: U.S. air strategy flawed, killed hundreds of innocent Afghan civilians
- Turkey warns U.S. of lengthy Iraq war
- DA in Runnion case may seek death penalty
- 'Stuart Little,' 'Perdition' share box office lead
- Els wins British Open · Tour de France · F1

News - Weather - Sports - Stock Quotes

Shopping
- DELL's Giving Away $50K/Day
Automatic entry into $50k-a-Day Giveaway when you buy a Dell Home System by July 31. No purchase necessary.
- New Model from Sony - 27" Trinitron WEGA TV, only $22/month + Free Delivery



Search the web using Google!

10 results Google Search I'm feeling lucky

Index contains ~25 million pages (soon to be much bigger)

About Google!

Stanford Search Linux Search

Get Google! updates monthly!

your e-mail Subscribe Archive

Copyright ©1997-8 Stanford University

© 2017 SPLUNK INC.

Burch’s Experience

Same questions and confusions over and over

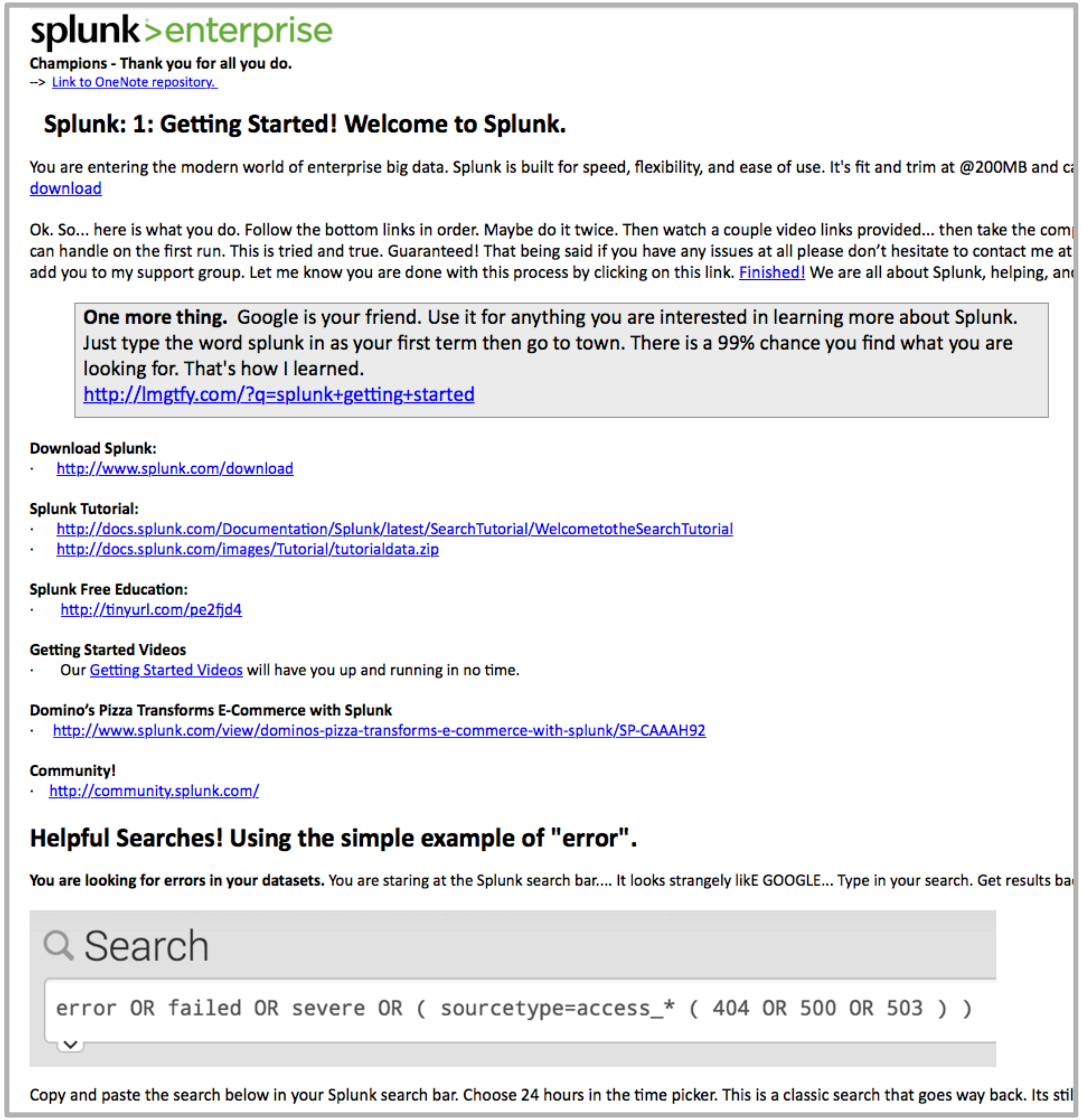
- What is Splunk?
- What report/dashboard to use?
- What data available?
- Want to learn more!

© 2017 SPLUNK INC.

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, 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://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

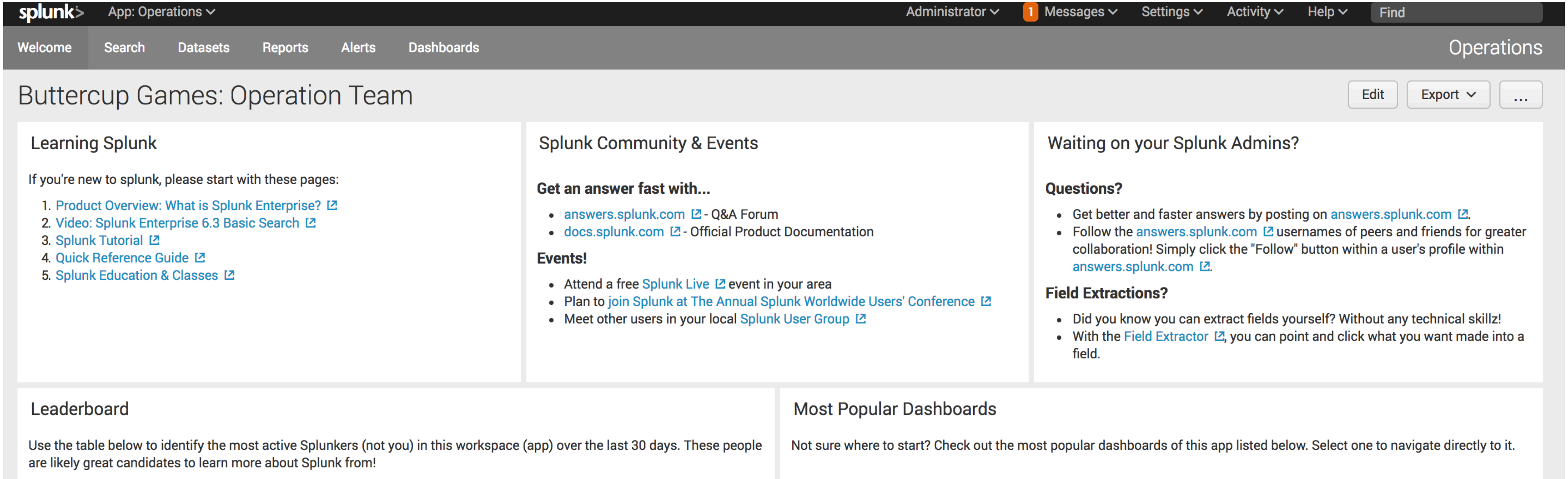
```
error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503 ) )
```

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

© 2017 SPLUNK INC.

Eureka! Welcome Page!

Effective material presented at every log in



Buttercup Games: Operation Team

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

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

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 skillz!
- 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.

© 2017 SPLUNK INC.

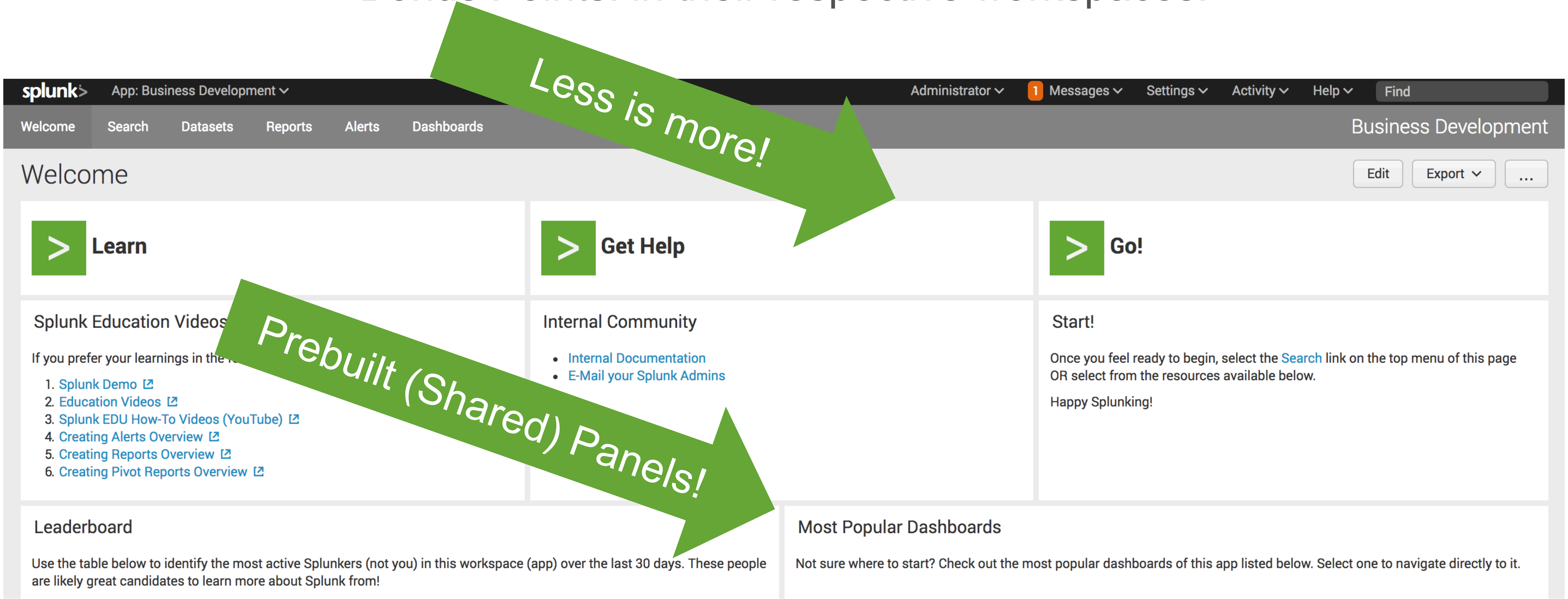
Different Technical Competencies

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

© 2017 SPLUNK INC.

And for BizDev!

Bonus Points: in their respective workspaces!



Less is more!

Prebuilt (Shared) Panels!

Welcome

Learn

Get Help

Go!

Splunk Education Videos

If you prefer your learnings in the

1. Splunk Demo
2. Education Videos
3. Splunk EDU How-To Videos (YouTube)
4. Creating Alerts Overview
5. Creating Reports Overview
6. Creating Pivot Reports Overview

Internal Community

- Internal Documentation
- E-Mail your Splunk Admins

Start!

Once you feel ready to begin, select the Search link on the top menu of this page OR select from the resources available below.

Happy Splunking!

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.

© 2017 SPLUNK INC.

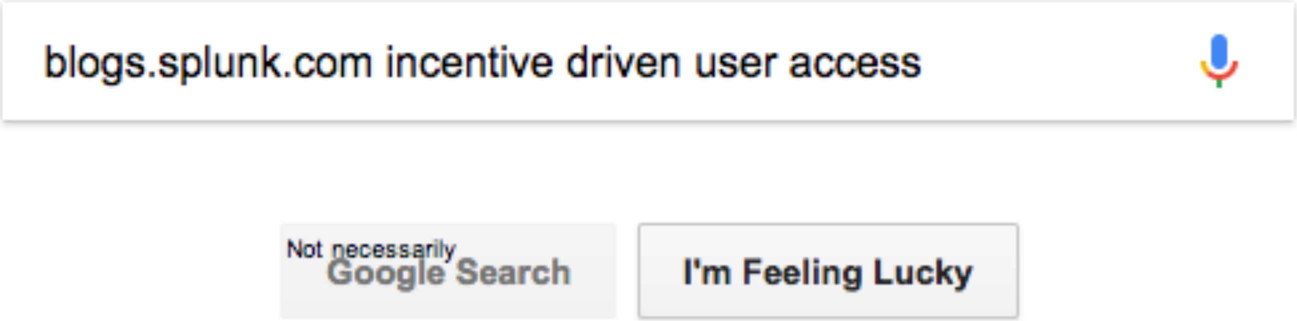
Workspaces + Welcome Pages = Awesomesauce

- Create a workspace template
  - Load it with a Welcome page
- Encourage users to own and edit their welcome page
- HTML panels to direct to other apps when needed
  - Minimized lost users
- Hands on Lab @ .conf2017-> Welcome Page Creator

© 2017 SPLUNK INC.

Incentive Driven User Onboarding

Concept III of III



blogs.splunk.com incentive driven user access

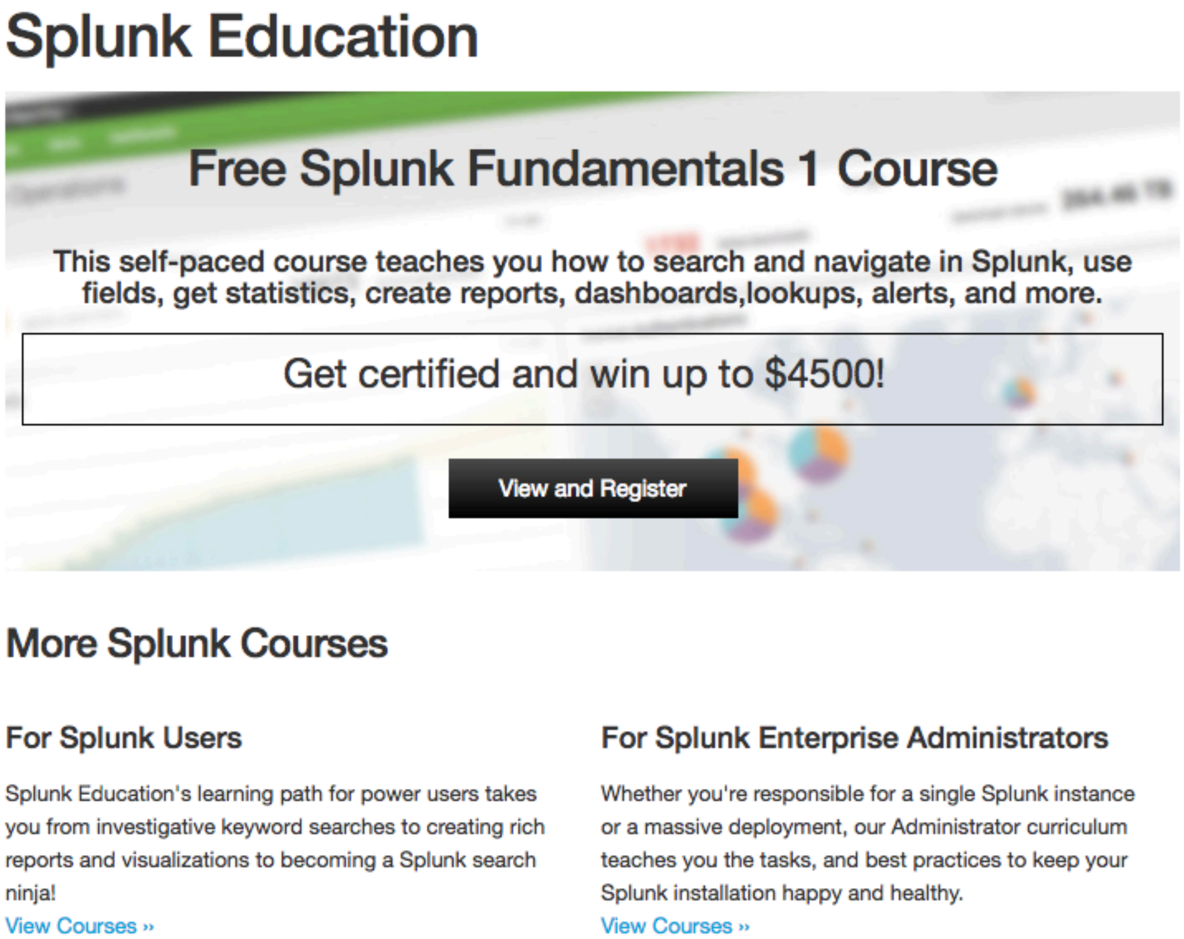
© 2017 SPLUNK INC.

Incentives

vs.

© 2017 SPLUNK INC.

Is EDU Required?



Splunk Education

Free Splunk Fundamentals 1 Course

This self-paced course teaches you how to search and navigate in Splunk, use fields, get statistics, create reports, dashboards,lookups, alerts, and more.

Get certified and win up to $4500!

More Splunk Courses

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 »

© 2017 SPLUNK INC.

“Yea, I took education”

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

© 2017 SPLUNK INC.

Alternative Approach: No Requirements

But limited impact…

You can't stop splunk-thusiasm…

©2010 FreeBigPictures.com

…so shape it in your favor!

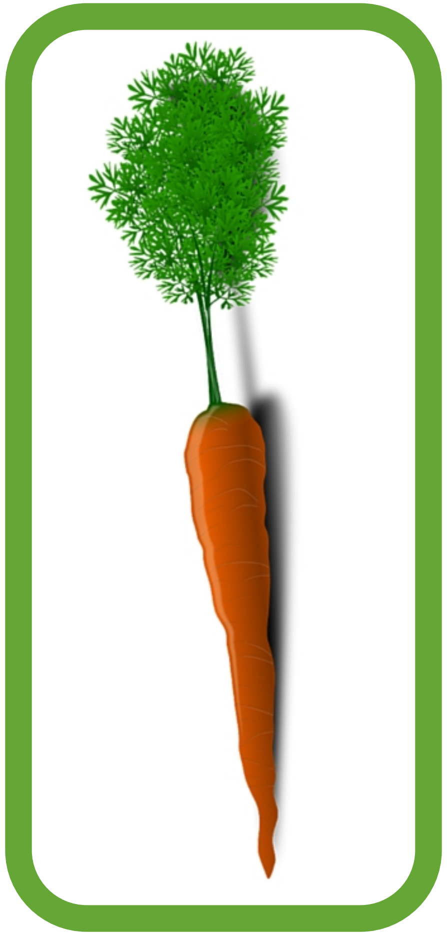
© 2017 SPLUNK INC.

Result

Curiosity and exploration

NASA/JPL-CALTECH

Incentives



vs.

© 2017 SPLUNK INC.

Brace Yourself!

© 2017 SPLUNK INC.

Incentive Driven User Onboarding

- Limit capabilities and risk to the platform for new users
- Generate curiosity and desire through those limitations
- Grant more capabilities through objective progress
- Users have a point & purpose to self-educate
- Positive reinforcement encourages positive behavior

© 2017 SPLUNK INC.

Rinse & Repeat

Admin Teachers Power User

Power User Teaches User

© 2017 SPLUNK INC.

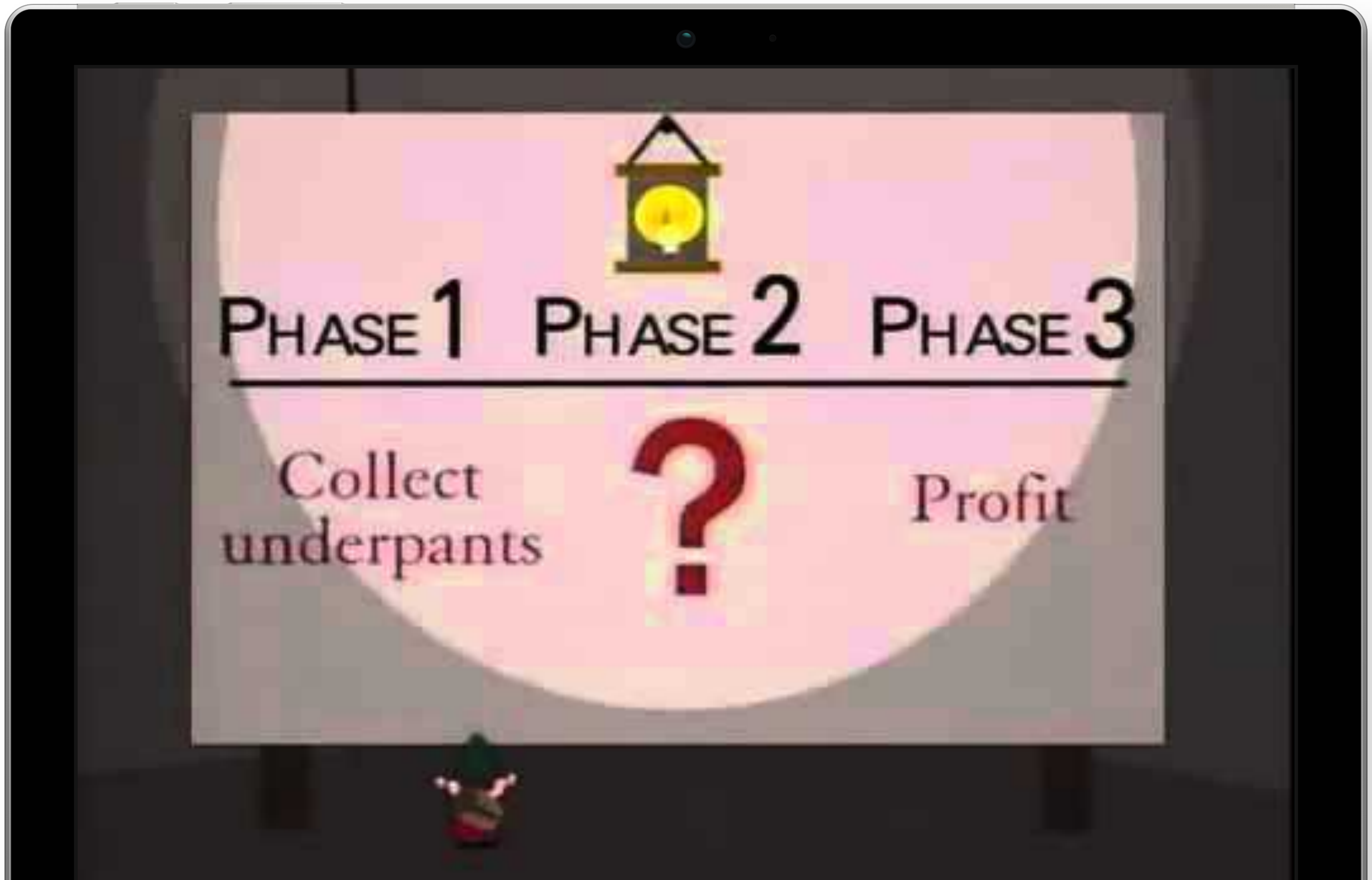
Result

At first, more questions. Later, more disciples.

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

© 2017 SPLUNK INC.

Implementation



1. Define new Splunk roles
2. Identify Power Users
   - > one per team
   - EDU from Account Team
3. Communicate & Publish Changes
4. Profit

splunk> .conf2017

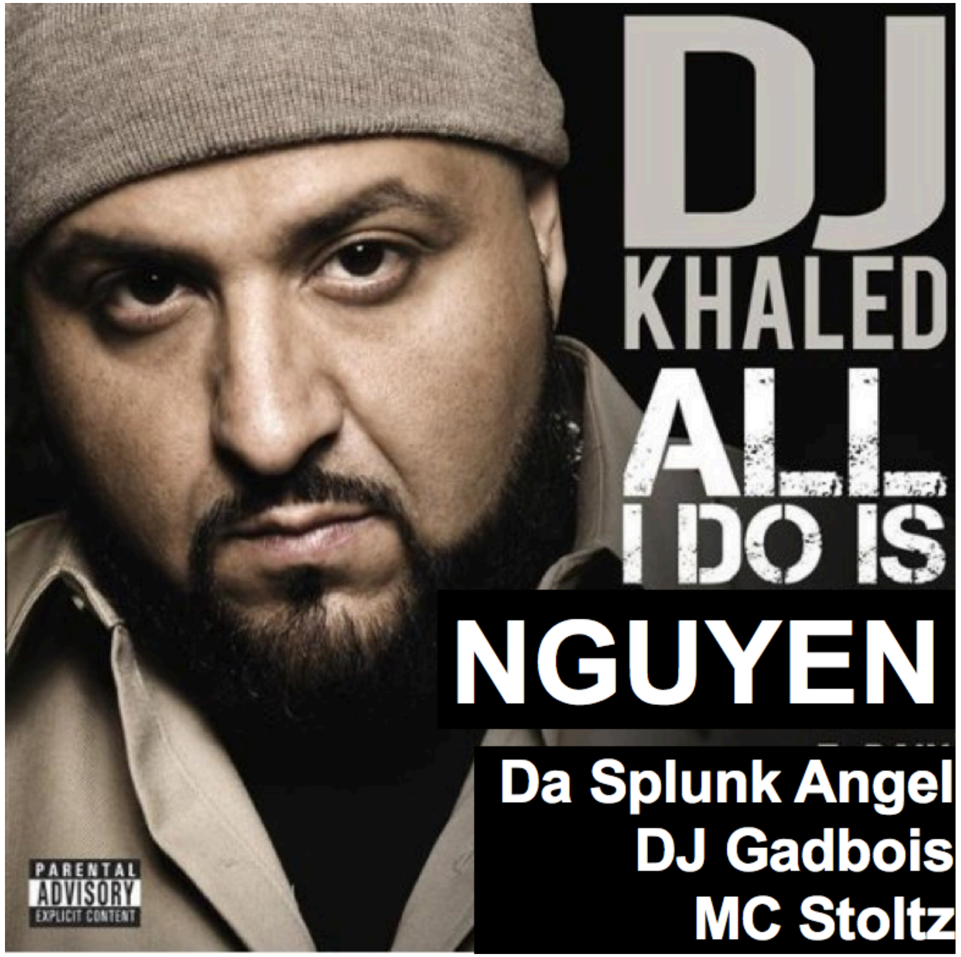
© 2017 SPLUNK INC.

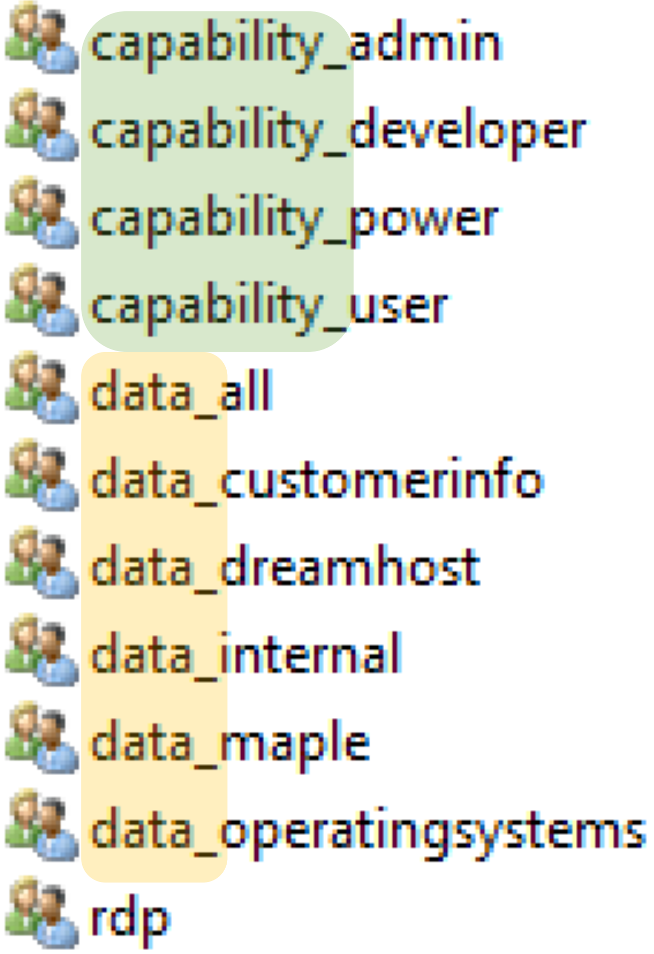
Hold Up!

© 2017 SPLUNK INC.

Sub-Concept: For The Nguyen (FTN)

Separate Roles & Capabilities & Groups





- capability_admin
- capability_developer
- capability_power
- capability_user
- data_all
- data_customerinfo
- data_dreamhost
- data_internal
- data_maple
- data_operatingsystems
- rdp

© 2017 SPLUNK INC.

Regarding data…

- Separate because team members have different skill sets
- Data access control for security
- Scalable with wildcards

```
[role_data_operatingsystems]
srchIndexesAllowed = os;perfmon;windows;wineventlog;winevents;unix_summary;msad;linux

[role_data_internal]
srchIndexesAllowed = _*

[role_data_prod]
srchIndexesAllowed = *_prod

[role_data_nonprod]
srchIndexesAllowed = *_nonprod

[role_data_all]
srchIndexesAllowed = *;_*
```

© 2017 SPLUNK INC.

© 2017 SPLUNK INC.

Step 1: Define New Splunk Roles

Ask Yourself

- How can the absence or limitation of a given capability be used to incentivize a user into learning more?
- What capability can be used as rewards for demonstrating Splunk proficiency?
- Will this capability **impact** the Splunk deployment when the user is **NOT logged in**?

© 2017 SPLUNK INC.

Selection of Impacting Capabilities

http://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities

Group	Capabilities	Why
Accelerations	• accelerate_datamodel • accelerate_search • output_file	• Compute & Storage costs • Rarely cleaned up
Scheduled Searches	• schedule_search • schedule_rtsearch	• Compute and concurrent load • Rarely cleaned up
Real Time Searches	• rtsearch • schedule_rtsearch	• Rarely necessary • Impact on SH + ALL Indexers • Proliferation to dashboards
Search Limits	• srchJobsQuota • srchMaxTime • srchTimeWin • srchDiskQuota • rtSrchJobsQuota	• Boundaries Careful, could be annoying

© 2017 SPLUNK INC.

Which Conf File?!

Before you edit the wrong one…

authentication.conf

- “Who are you?”
- LDAP system connection details
- LDAP -> Splunk role mapping

authorization.conf

- “Are you allowed?”
- feature and data access definition
- Tip: Inherit OOTB roles
  - Can override
  - Use of existing role names deflects errors

© 2017 SPLUNK INC.

Step 3: Communicate & Publish Changes

- What’s changing?
- How to earn capabilities?
- Who to contact?
  - Who are power users on their team?
- essentially, wh*

© 2017 SPLUNK INC.

Political Support

Make sure management is on board

- Outline Problem
  - Quantify
    - projected hardware cost savings
    - load/outage impact
- Outline Solution
  - Timeline + steps
  - Communication plan
  - Expected end results

© 2017 SPLUNK INC.

Step 4: Profit

Your future.

I DID ABSOLUTELY NOTHING TODAY
AND IT WAS EVERYTHING I THOUGHT IT COULD BE

© 2017 SPLUNK INC.

Reset

© 2017 SPLUNK INC.

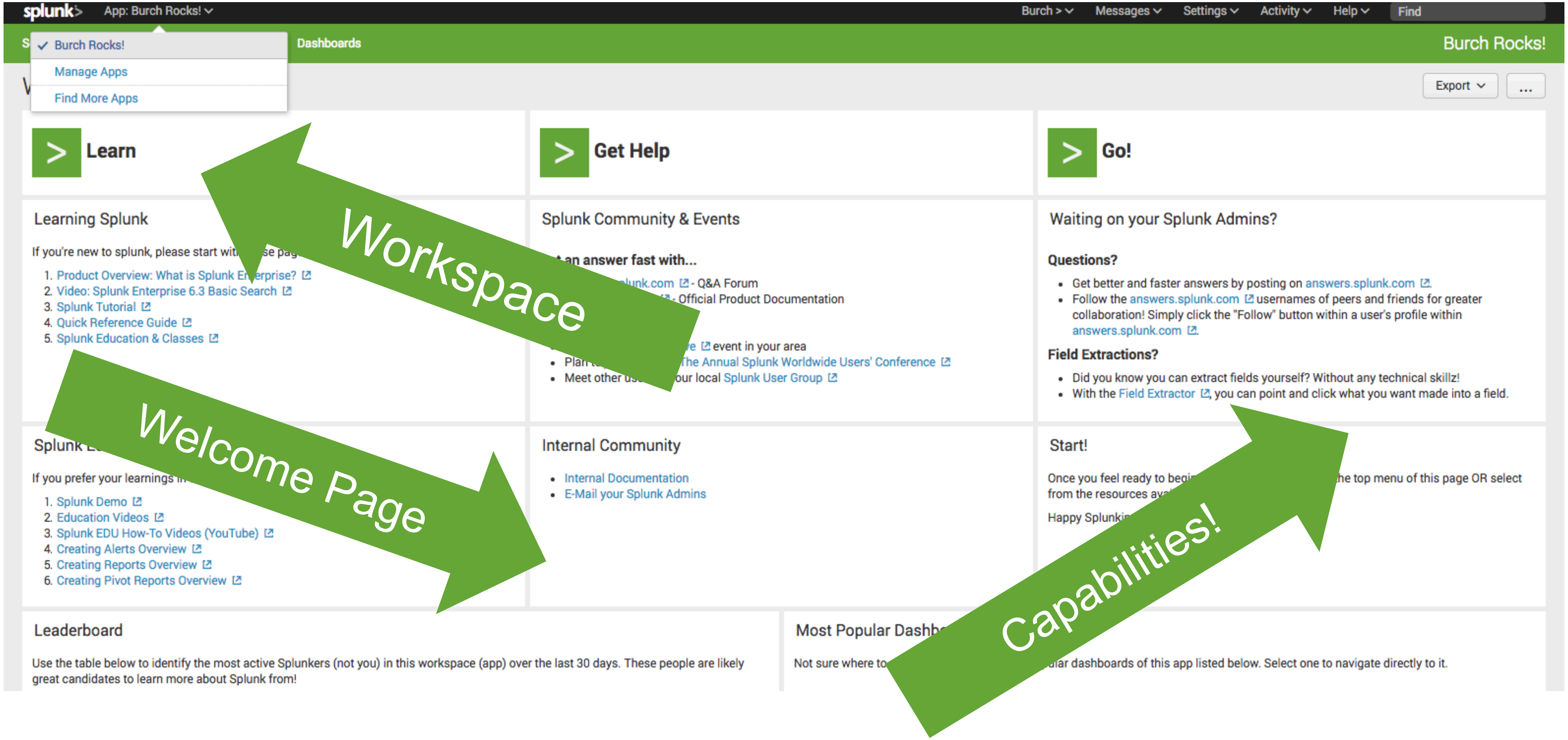
Scenario

- New employee at Buttercup Games
- Responsibilities include Data Driven Decisions
- 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!
- Just got Splunk access and you log in to see…

© 2017 SPLUNK INC.

…only what you need

With clear information on where to go/learn next



> Learn

Learning Splunk

If you're new to splunk, please start wit… se pag…

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

Splunk E…

If you prefer your learnings i…

1. Splunk Demo
2. Education Videos
3. Splunk EDU How-To Videos (YouTube)
4. Creating Alerts Overview
5. Creating Reports Overview
6. Creating Pivot Reports Overview

> Get Help

Splunk Community & Events

…an answer fast with...

- …lunk.com - Q&A Forum
- … - Official Product Documentation
- …e event in your area
- Plan … The Annual Splunk Worldwide Users' Conference
- Meet other us… your local Splunk User Group

Internal Community

- Internal Documentation
- E-Mail your Splunk Admins

> 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 skillz!
- With the Field Extractor, you can point and click what you want made into a field.

Start!

Once you feel ready to begi… he top menu of this page OR select from the resources av…

Happy Splunki…

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!

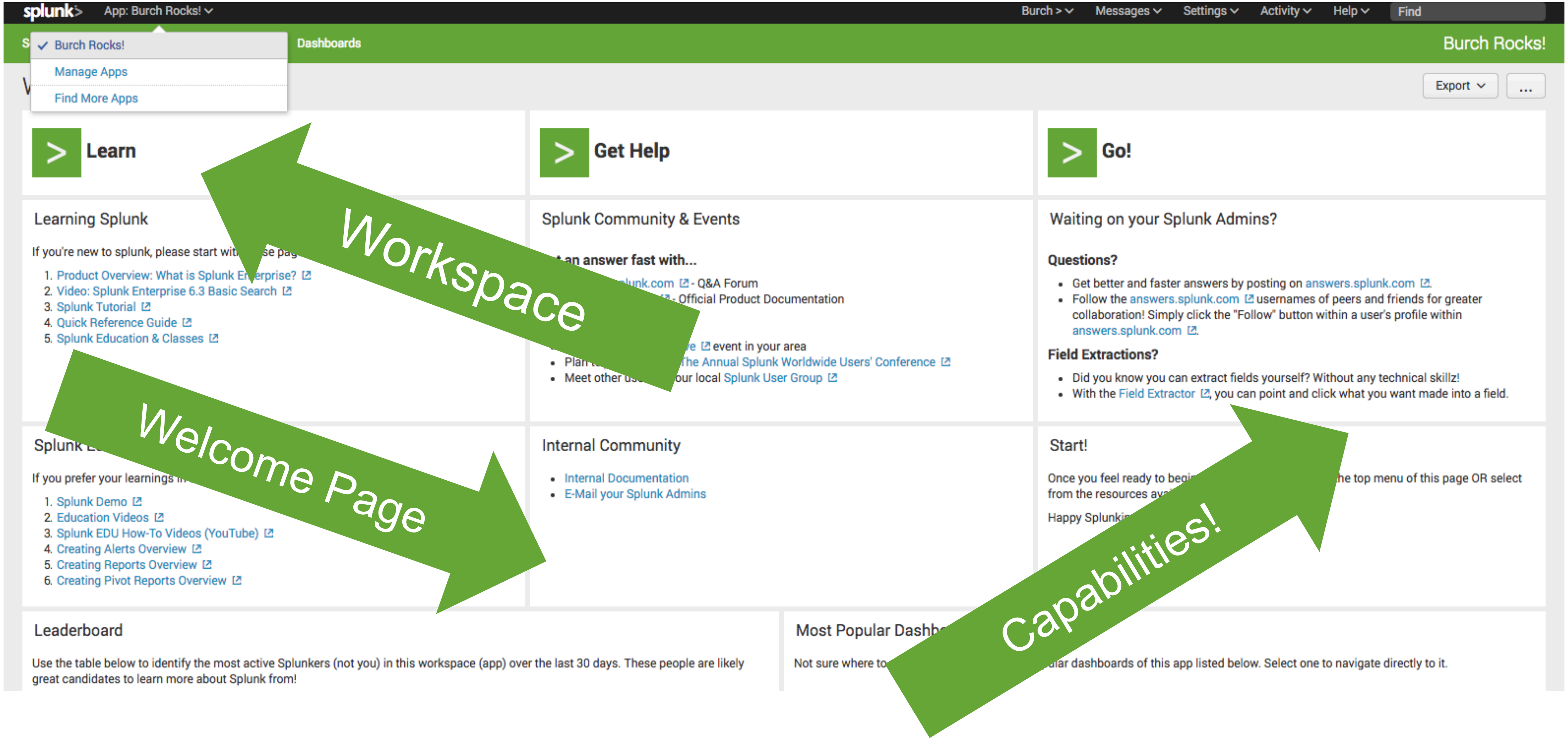
Most Popular Dashb…

Not sure where to … lar dashboards of this app listed below. Select one to navigate directly to it.

© 2017 SPLUNK INC.

Blueprints for Onboarding Teams

"Hey! That's the name of the session!"



> Learn

Learning Splunk

If you're new to splunk, please start wit… …se pag…

1. Product Overview: What is Splunk Er…erprise?
2. Video: Splunk Enterprise 6.3 Basic Search
3. Splunk Tutorial
4. Quick Reference Guide
5. Splunk Education & Classes

Splunk E…

If you prefer your learnings i…

1. Splunk Demo
2. Education Videos
3. Splunk EDU How-To Videos (YouTube)
4. Creating Alerts Overview
5. Creating Reports Overview
6. Creating Pivot Reports Overview

> Get Help

Splunk Community & Events

…an answer fast with...

- …plunk.com - Q&A Forum
- … - Official Product Documentation
- …e event in your area
- Plan… …The Annual Splunk Worldwide Users' Conference
- Meet other us… …our local Splunk User Group

Internal Community

- Internal Documentation
- E-Mail your Splunk Admins

> 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 skillz!
- With the Field Extractor, you can point and click what you want made into a field.

Start!

Once you feel ready to begi… …he top menu of this page OR select from the resources av…

Happy Splunki…

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 Dashb…

Not sure where to… …ular dashboards of this app listed below. Select one to navigate directly to it.

© 2017 SPLUNK INC.

What Now?

Related breakout sessions and activities…

8DEC0D

1. Rate this! (be honest)
2. Collaborate: #success
   - Sign Up @ http://splk.it/slack
3. Customer Success Studio
4. More talks, search for
   - Blueprints
   - Burch
   - Champagne
   - Delaney
   - Optimization
   - Best Practices
   - Veuve

© 2017 SPLUNK INC.

Questions & Discussion?

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017