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 --------------------------------------->
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.
Right Session?

Mo Teams, Mo Problems.
Clutter clutter everywhere…
Not yo’ Splunk on fleek.
Admins got you all...

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

STOP HITTING YOURSELF

@JAZMINREDUX
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.
Domains-o-Discussion

tots kewl to bounce

STOP HITTING YOURSELF

@JAZMINREDUX
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
“Scale customer success through the automation of adoption services and best practices”
Our World Today
Who wants to role play?
Choose Your Own Adventure!
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…
report on how popular splunk is

No results found. Try expanding the time range.
<table>
<thead>
<tr>
<th>i</th>
<th>Title</th>
<th>Actions</th>
<th>Owner</th>
<th>App</th>
<th>Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Model Audit</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Detect Journal Clearing</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Detect Lateral Movement With WMI</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Detect Log Clearing With wevtutil</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Error Details</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_TA_aws</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Fake Windows Processes</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Health Overview</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_TA_aws</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Malicious Command Line Executions</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Monitor AutoRun Registry Keys</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Monitor Successful Backups</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Monitor Successful Windows Updates</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Monitor Unsuccessful Backups</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Monitor Unsuccessful Windows Updates</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Predictive Analytics</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Ransomware Extensions</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td></td>
<td>Ransomware Note Files</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
</tbody>
</table>

Dashboards include searches, visualizations, and input controls that capture and present available data.
All the Dashboards!
UMMM, YES I HAVE A QUESTION...

WTF?
I deal with the god damn customers so the engineers don't have to
I DEAL WITH THE GOD DAMN CUSTOMERS

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

SO THE ENGINEERS DON'T HAVE TO
Splunk Admin
You
Grand Moff Tarkin
Your throat
Solution, you have?!
Three Concepts

Let’s pause and explore some new ideas
Workspaces

Concept I of III
Workspace

Do you keep everyone’s work on everyone’s desk?
...so why do we do that in Splunk?
App as a Workspaces
Dedicated to one team/group/purpose
Benefits
Increases in…

Safety

Risk led learning

Discovery led collaboration
Implementation

1. Create an app
2. Set permissions
3. Set as role default
4. Profit
Step 1: Create an app
http://dev.splunk.com/view/SP-CAAAEUC
Step 2: Set Permissions

Apps -> Manage Apps

“Hide” extraneous apps/workspaces:

- Remove role’s read permissions

- `app.conf`
  ```
  [ui]
  is_visible = false
  show_in_nav = false
  ```
Step 3: Set Role Default
Bypasses launcher. Guides user to workspace.

appname/local/user-prefs.conf
[role_capability_admin]
default_namespace = workspace_app

appname/metadata/local.meta
[ui-prefs]
export = system
Step 4: Profit

$$ Everyone get a search head $$

YOU GET ONE!

YOU GET ONE!

EVERYONE GETS ONE!
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
Welcome Page

Concept II of III

blogs.splunk.com welcome page

Not necessarily Google Search

I'm Feeling Lucky
Oh, the Places You’ll Go

Too many options!
Same Challenge. Different Platforms.
What did this button do for user design?

- Mislead?
- Restrict?
- Guidance!
- Confidence!
- Comfort!
“eliminating consumer choices can greatly reduce anxiety”
Same Challenge. Different Platforms.
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

---

Static == Ineffective

Lost in their mailbox...
Eureka! Welcome Page!
Effective material presented at every log in
Different Technical Competencies

I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."
And for BizDev!

Bonus Points: in their respective workspaces!

Less is more!

Prebuilt (Shared) Panels!
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
Incentive Driven User Onboarding

Concept III of III

blogs.splunk.com incentive driven user access
Incentives
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!

View and Register

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 »
“Yea, I took education”
“But I didn’t care, nor pay attention”
Alternative Approach: No Requirements
But limited impact...

You can’t stop splunk-thusiasm...  ...so shape it in your favor!
Result
Curiosity and exploration
Incentives
Brace Yourself!
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
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…
Implementation

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

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

```conf
[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 = *;__*
```
AND NOW BACK TO OUR REGULARLY SCHEDULED PROGRAMMING
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?
## Selection of Impacting Capabilities


<table>
<thead>
<tr>
<th>Group</th>
<th>Capabilities</th>
<th>Why</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accelerations</td>
<td>• accelerate_datamodel</td>
<td>• Compute &amp; Storage costs</td>
</tr>
<tr>
<td></td>
<td>• accelerate_search</td>
<td>• Rarely cleaned up</td>
</tr>
<tr>
<td></td>
<td>• output_file</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Searches</td>
<td>• schedule_search</td>
<td>• Compute and concurrent load</td>
</tr>
<tr>
<td></td>
<td>• schedule_rtsearch</td>
<td>• Rarely cleaned up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Time Searches</td>
<td>• rtsearch</td>
<td>• Rarely necessary</td>
</tr>
<tr>
<td></td>
<td>• schedule_rtsearch</td>
<td>• Impact on SH + ALL Indexers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Proliferation to dashboards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search Limits</td>
<td>• srchJobsQuota</td>
<td>• Boundaries</td>
</tr>
<tr>
<td></td>
<td>• srchMaxTime</td>
<td>Careful, could be annoying</td>
</tr>
<tr>
<td></td>
<td>• srchTimeWin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• srchTimeWin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• srchDiskQuota</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rtSrchJobsQuota</td>
<td></td>
</tr>
</tbody>
</table>
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
Step 3: Communicate & Publish Changes

- What’s changing?

- How to earn capabilities?

- Who to contact?
  - Who are power users on their team?

- essentially, wh*
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
Step 4: Profit

Your future.

I DID ABSOLUTELY NOTHING TODAY

AND IT WAS EVERYTHING I
THOUGHT IT COULD BE
Reset

LET'S SEE THAT

IN AN INSTANT REPLAY
• 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…
...only what you need

With clear information on where to go/learn next

Workspace

Welcome Page

Capabilities!
Blueprints for Onboarding Teams

“Hey! That’s the name of the session!”
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
Questions & Discussion?

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