© 2018 SPLUNK INC.

Life at Mars

The Day to Day Life of a Splunk Center of Excellence

Greg Poniatowski, Information Security Lead , Mars, Inc.

Doug Erkkila, Customer Success Manager , Splunk

October 2018 | Version 1.0

© 2018 SPLUNK INC.

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.

© 2018 SPLUNK INC.

Our Speakers

GREG PONIATOWSKI

Information Security Lead @ Mars, Inc.

DOUG ERKKILA

Customer Success Manager @ Splunk

© 2018 SPLUNK INC.

How did we get here?

And why am I in this hand basket?

© 2018 SPLUNK INC.

Our Start

This is where the subtitle goes

- Splunk Cloud and Enterprise Security purchased by the Mars security team
  - Originally only used by SOC analysts
- Security team wanted to get additional value from the existing data and let other IT Ops teams start to use it
  - New teams had no training and Security team didn't have time to train them
  - Also wanted new data sources added quickly
  - Ops even started a major project to improve Visibility across the enterprise!
- Additional data meant more hardware to handle the data flow
- And all the new users asking for data, or support, or training

- **All this being done by 1 person!**

Can you see where this is headed?

splunk> .conf18

© 2018 SPLUNK INC.

Nightmare Use Cases

“We have some data we need to onboard”

```
[tws:merge]
EXTRACT-000_tws_merge_fields = ^\d{2}:\d{2}:\d{2} \d{2}.\d{2}.\d{4}\|(?<message_source>[^:]+):(?<message>.*)$
EXTRACT-010_tws_merge_job_stream = JOB=(?<job_stream>[^\[]+) in message
EXTRACT-020_tws_merge_job = \[\(\d+\s\d{2}\/\d{2}\/\d{2}\)\,\([^\)]+\)\]\.(?<job>\S+(?:\s\([^\)]+\))) in message
EXTRACT-030_tws_merge_job_name_id = (?<job_name>\S+)\s\(#(?<job_id>[^\)]+)\) in job
EXTRACT-040_tws_merge_job_type = \s(?<job_type>\w{2}): in message
EXTRACT-050_tws_merge_job_stream = (?:(?:[Jj]ob stream )|(?:[Jj]ob )|(?:[Jj]obman streamed ))(?<job_stream>[^\[]+) in message
EXTRACT-051_tws_merge_job_workstation = ^(?<workstation>[^#]+) in job_stream
EXTRACT-052_tws_merge_job_stream_name = (?<job_stream_name>[^#]+)$ in job_stream
EXTRACT-060_tws_merge_job_status = (?:(?:status to)|(?:has completed))\s(?<job_status>\w+) in message
EXTRACT-070_tws_merge_command_workstation = Received command (?<command>\S+) for run number (?<run_number>\d+) (?:for workstation (?<recv_workstation>\S+) )?fr
om workstation (?<orig_workstation>[^\.]+) in message
EXTRACT-080_tws_merge_job_id = #(?<job_id>J\d+) in message
EXTRACT-090_tws_merge_job_name = JOBS\.(?<job_name>\S+) in message
EXTRACT-100_tws_merge_job_stream = [^(?:JOB=)](?<job_stream>\S+#[^\s\[)+) in message
EXTRACT-110_tws_merge_job_group = \[(?<job_group>\(\d+\s\S+\),\([^\)]+\))\] in message
EXTRACT-120_tws_merge_job_group_date_id = \((?<start_time>\d+)\s(?<start_date>[^\)]+)\),\((?<schedule_id>[^\)]+)\) in job_group
EXTRACT-130_tws_merge_level_data_arch = ^(?<log_level>[^:]+):(?<data>\S+), architecture type:(?<arch_type>.*?)$ in message
EXTRACT-140_tws_merge_operator_command = ^#(?<operator>[^\/]+)\/Operator command:\s(?<operator_command>\S+) in message
EXTRACT-150_tws_merge_state_change = changing from state (?<state_old>\d+) to new state (?<state_new>\d+)$ in message
EVAL-arch_type = lower(arch_type)
EVAL-status = lower(status)
```

© 2018 SPLUNK INC.

Nightmare Use Cases

”We want to create Incidents in Service Now”

Project

- Splunk_TA_ServiceNow ~/Documents/Gitlab/Splun
  - appserver
  - bin
    - certifi
    - chardet
    - idna
    - requests
    - servicenow
      - drivers
      - __init__.py
      - Connection.py
      - ServiceNow.py
      - Utils.py
    - splunk_ta_servicenow
      - cloudconnectlib
      - functools32
      - httplib2
      - jinja2
      - jsl
      - jsonpath_rw
      - jsonschema
      - mako
      - markupsafe
      - modinput_wrapper
      - munch
      - ply
      - requests
      - solnlib
      - sortedcontainers

ServiceNow Incident

Remove

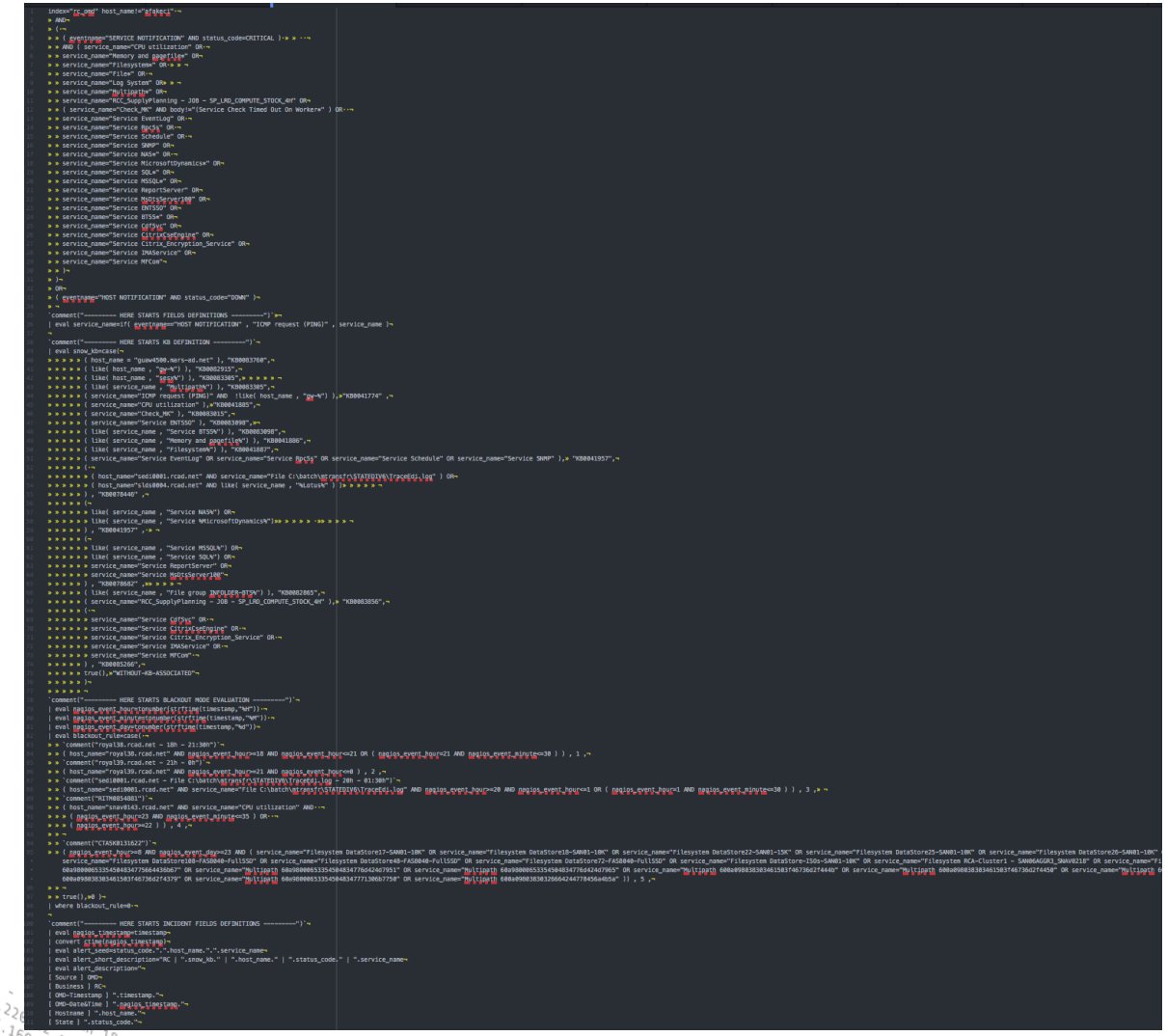
Account *	marsdev2	
Assignment Group *	OPS-SERVICEDESK-ART	
Category-Sub-category *	Linux SAP File System - SAP&BI Platf...	Value that maps to 'category' and 'subcategory' in ServiceNow.
CMDB CI *	$host_name	Value that maps to 'cmdb_ci' in ServiceNow. Prepend '$' to use value of field provided.
Description	$alert_description	Value that maps to 'description' in ServiceNow. Prepend '$' to use value of field provided.
Impact *	2 - Medium	

splunk> .conf18

© 2018 SPLUNK INC.

Nightmare Use Cases

“I need help with this search”



111 Line SPL Query

© 2018 SPLUNK INC.

Uh oh!

A bit off the rails

splunk> .conf18

© 2018 SPLUNK INC.

How can we get better?

© 2018 SPLUNK INC.

Address Staffing Shortage

What if Greg were hit by a bus?

- Short Term: Staff augmentation from Splunk Professional Services
  - Highly trained people right away to take over some of the load.
  - PS consultant roll over leads to recurring ramp up time that is wasted.
  - Not scalable.
  - Not Sustainable.
- Long Term: Contract staffing through a Splunk trained partner
  - Highly scalable.
  - Sustainable.
  - Slow to implement as contracts have to go through a lengthy process.
  - Shared service provided by the partner enables a networking effect that improves service quality.

© 2018 SPLUNK INC.

Phase 1: Clean Up

Paying down Critical Technical Debt : 3 to 6 months of work

- Splunk Professional Services was brought in to help clean up
  - Remove unused apps.
  - Properly configure some data sources.
    - Some data sources had changed formats since their initial onboarding and needed to be updated.
  - Rebuilt a search head since it had been managed so poorly before and was performing poorly.

- Also took some of the support load
  - Freed up Greg’s time to re-architect areas he didn’t have time to earlier.
  - Worked with automation team to implement Add-ons.
  - Helped build a new process to use Docker to run test environments as well as collect data.

splunk> .conf18

© 2018 SPLUNK INC.

Phase 2: Staff On-Boarding

On-going and iterative process

- On-boarding new staff is difficult
- Even more difficult when you don't have any documentation
  - R-syslog
  - Docker
  - HA-Proxy
  - GitLab

- Initial task for team contractors was to document EVERYTHING!
  - On-prem infrastructure
  - Data types

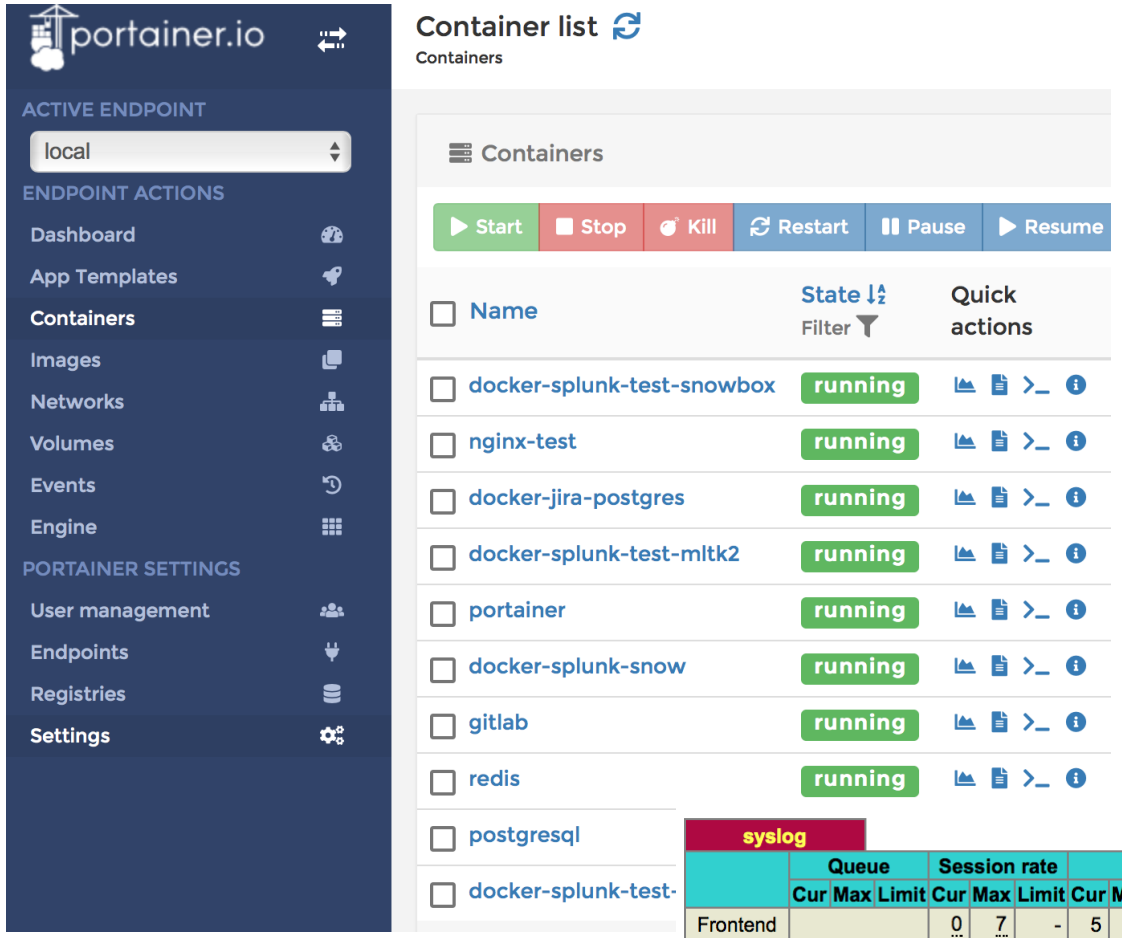
But how do you run this new team?

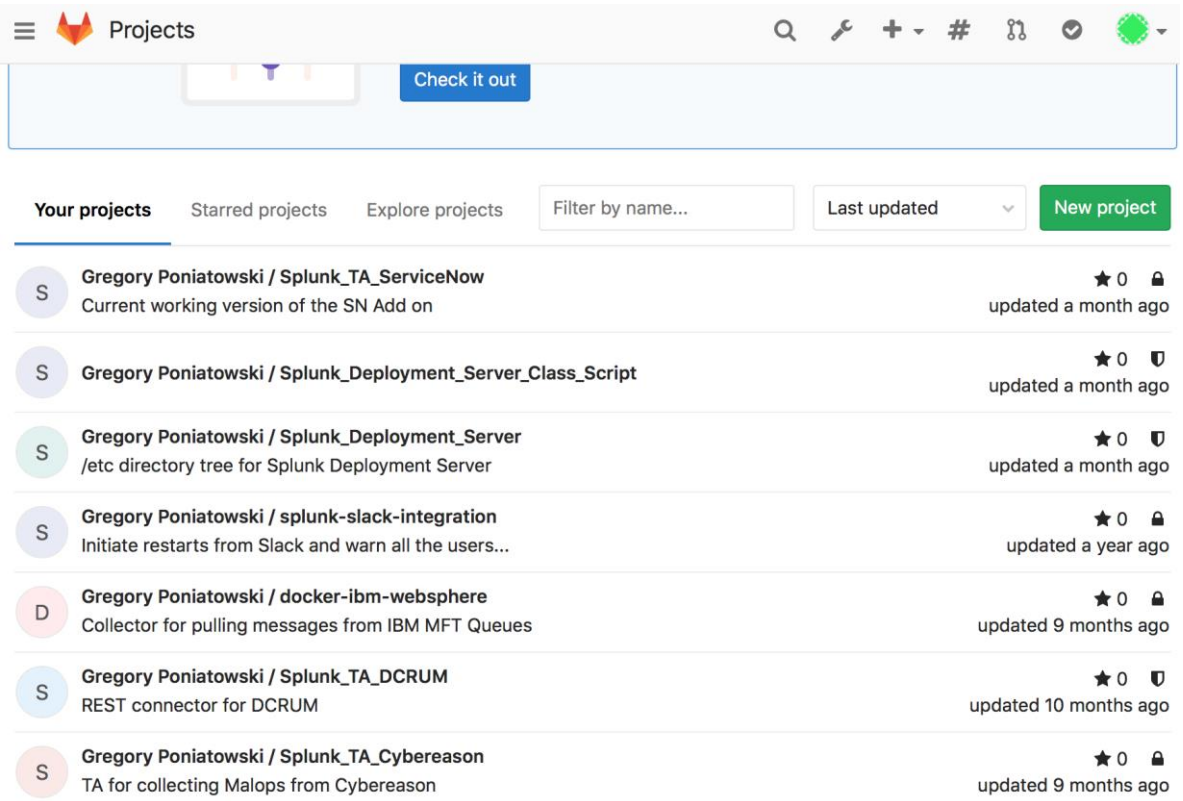
splunk> .conf18

© 2018 SPLUNK INC.

Additional Technology

A bit off the rails





syslog

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status
Frontend				0	7	-	5	9	2 000	55 696			177 446 598	0	0	0	0					OPEN
vmwl5350	0	0	-	0	3		1	5	-	17 879	17 879	19s	53 137 021	0		0		0	0	0	0	6d18h UP
vmwl5351	0	0	-	0	3		2	5	-	17 878	17 878	29s	58 343 905	0		0		0	0	0	0	6d18h UP
vmwl6013	0	0	-	0	3		1	5	-	17 864	17 855	2s	58 957 534	0		0		2	0	9	0	21h51m UP
vmwl6017	0	0	-	0	2		1	4	-	2 084	2 084	33s	7 008 138	0		0		0	0	0	0	1d1h UP
Backend	0	0		0	7		5	9	200	55 696	55 696	2s	177 446 598	0	0	0		2	0	9	0	6d18h UP

splunk> .conf18

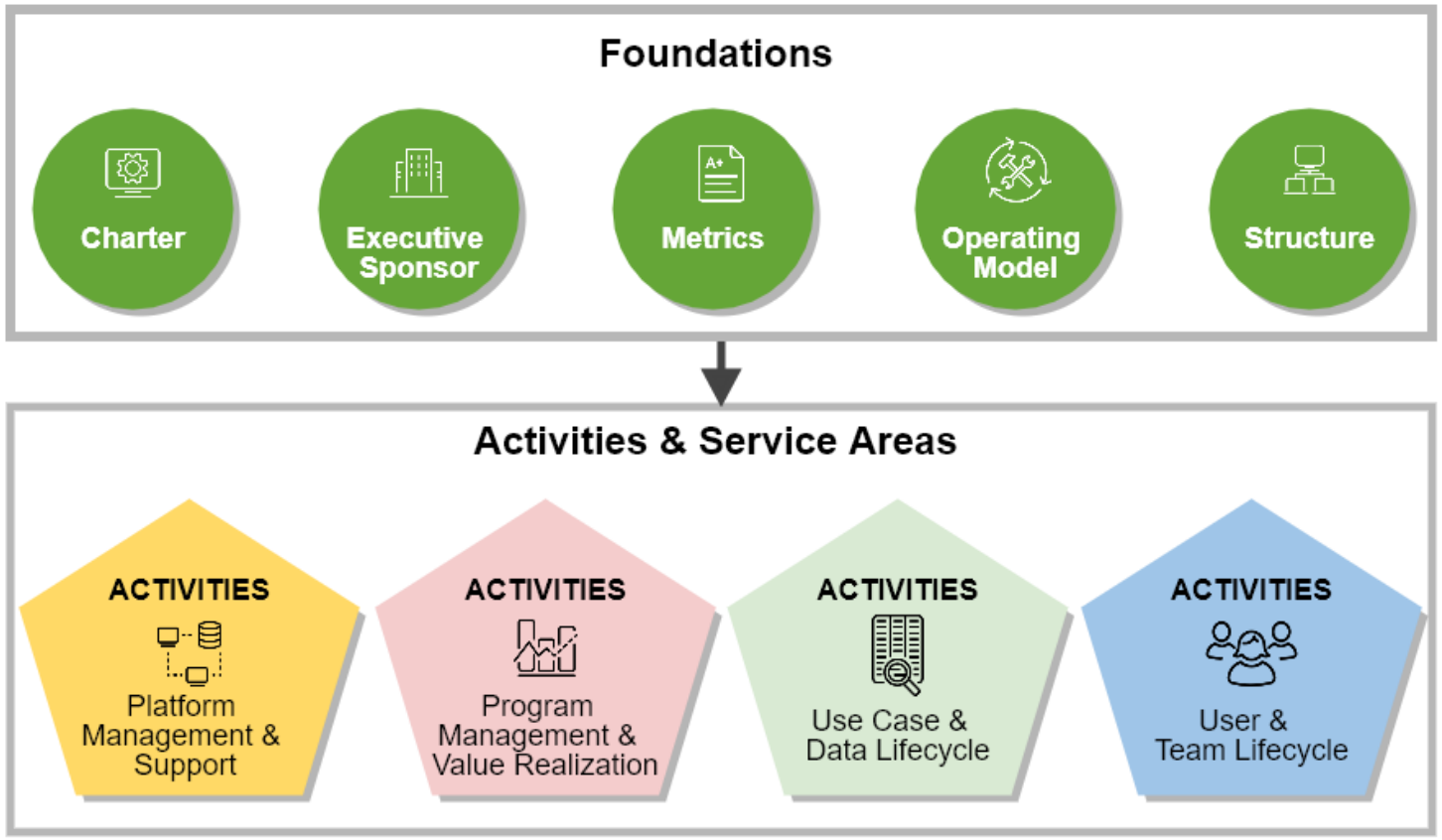
© 2018 SPLUNK INC.

A Splunk Center of Excellence

splunk> .conf18

© 2018 SPLUNK INC.

What is a Center of Excellence



- A set of best practices provided by Splunk
- A framework for translating those best practices to individual companies

© 2018 SPLUNK INC.

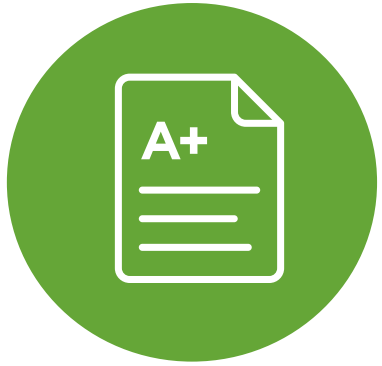
CoE Foundations

Executive Sponsor

Structure

Operating Model

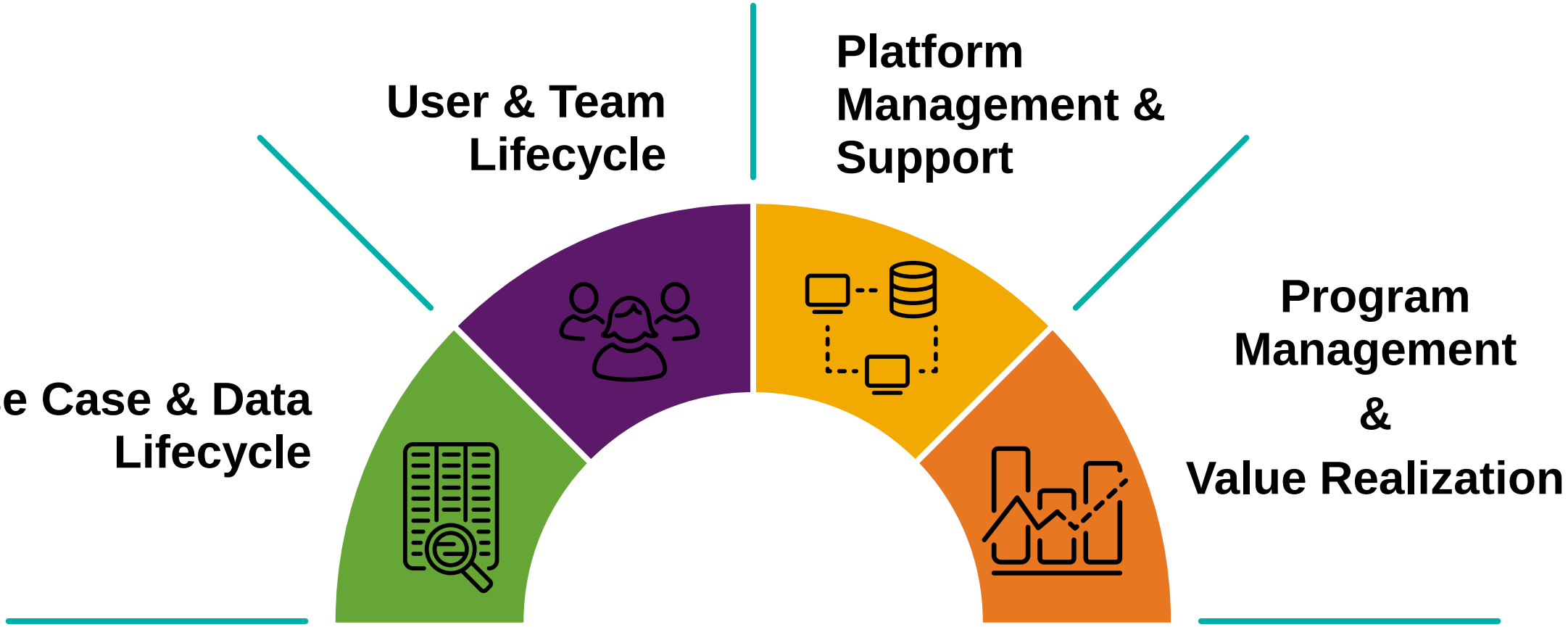
Charter



Metrics

© 2018 SPLUNK INC.

CoE Activities & Service Areas

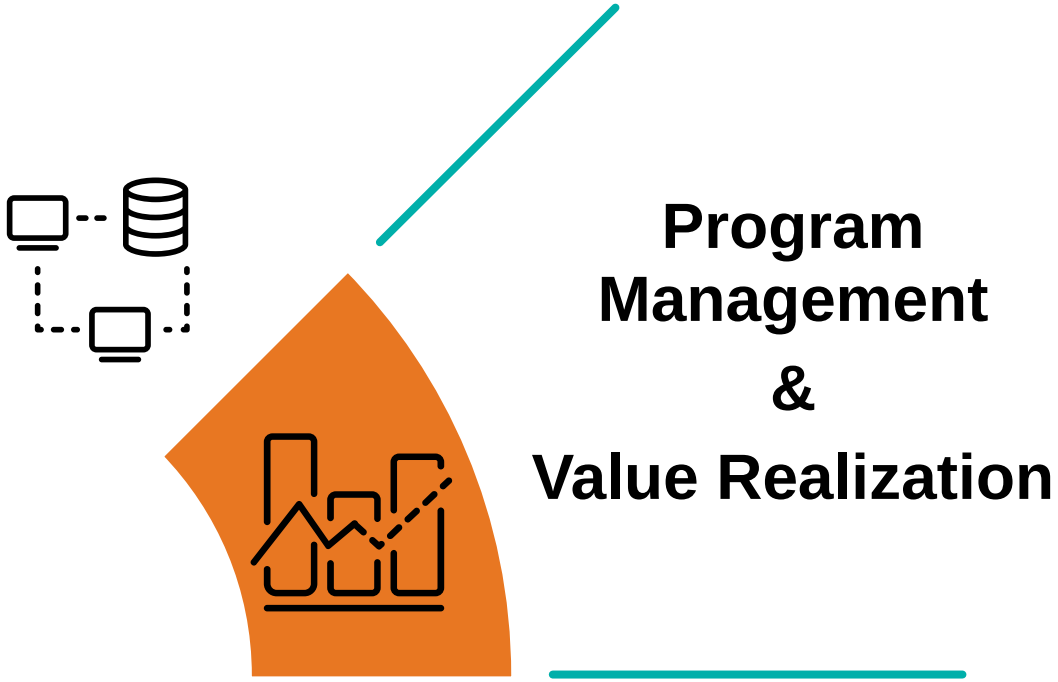


© 2018 SPLUNK INC.

CoE Activities & Service Areas

Program Management Example

- Success Planning
- Workshops
- Program Resources
- Executive Alignment



© 2018 SPLUNK INC.

Mars Differences

- Focused on certain areas rather than the whole CoE Program
  - Focused on Platform and Program Management Service Areas
- Used a Steering Group instead of having a single CoE lead or Program Manager
  - Subtle difference but has a large impact on flow of new work
  - Priority is established by subject matter experts

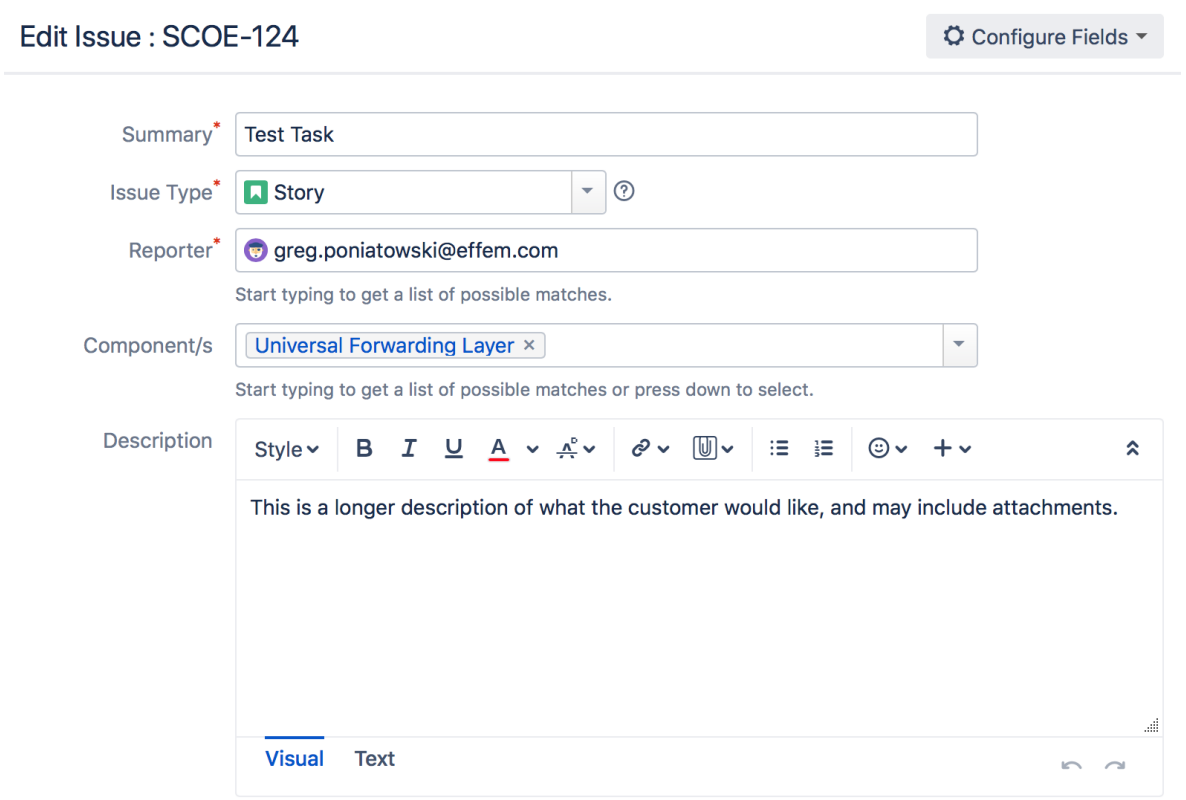
© 2018 SPLUNK INC.

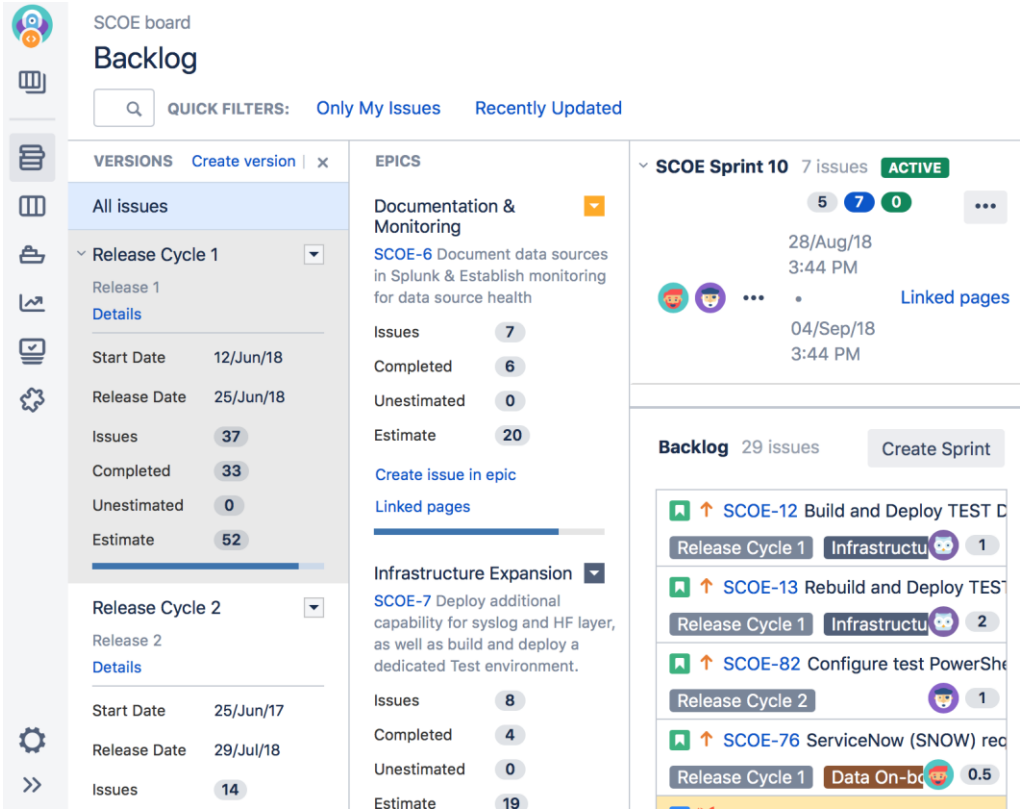
Where are we now?

© 2018 SPLUNK INC.

Today

- Team has grown from 2 people to 6
- Put a new processes to funnel and prioritize demand (screenshot below)





© 2018 SPLUNK INC.

Baseline Comparison

	Initial Baseline	Current State
Gap	6	0
Good	12	9
Better	1	7
Best	2	5

No more identified gaps!

© 2018 SPLUNK INC.

Lessons Learned

- What could we have done better?
  - We could have addressed the problem before it became critical
  - Gotten leadership buy in for additional resourcing sooner
  - Anticipated better the workload that additional demand would bring
  - The amount of time it would take to educate and inform users

© 2018 SPLUNK INC.

Staffing

What if Greg got hit by a bus?

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Seventh level is for paragraphs with no bullets, 24pt

Eighth level is for paragraphs with no bullets, 20pt

Ninth level is for paragraphs with no bullets, 16pt

© 2018 SPLUNK INC.

Two Column Text Layouts

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

© 2018 SPLUNK INC.

Comparison

This is where the subtitle goes

Title, 24pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Title, 24pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

© 2018 SPLUNK INC.

Comparison

This is where the subtitle goes

Title, 24pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Title, 24pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

© 2018 SPLUNK INC.

Three Column Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

© 2018 SPLUNK INC.

Three Column Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

© 2018 SPLUNK INC.

Bullets and Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

© 2018 SPLUNK INC.

Bullets and Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

© 2018 SPLUNK INC.

Three Column Quotes

This is where the subtitle goes

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

splunk> .conf18

© 2018 SPLUNK INC.

Three Column Quotes

This is where the subtitle goes

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

splunk> .conf18

© 2018 SPLUNK INC.

Title and Subtitle Only

This is where the subtitle goes

© 2018 SPLUNK INC.

Title and Subtitle Only

This is where the subtitle goes

splunk> .conf18

© 2018 SPLUNK INC.

Title and Subtitle with No Footer Graphic

This is where the subtitle goes

© 2018 SPLUNK INC.

Title and Subtitle with No Footer Graphic

This is where the subtitle goes

© 2018 SPLUNK INC.

“Quotes are more impactful when you selectively highlight key terms.”

Source information here

© 2018 SPLUNK INC.

Screenshot and Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

© 2018 SPLUNK INC.

Screenshot and Content

This is where the subtitle goes

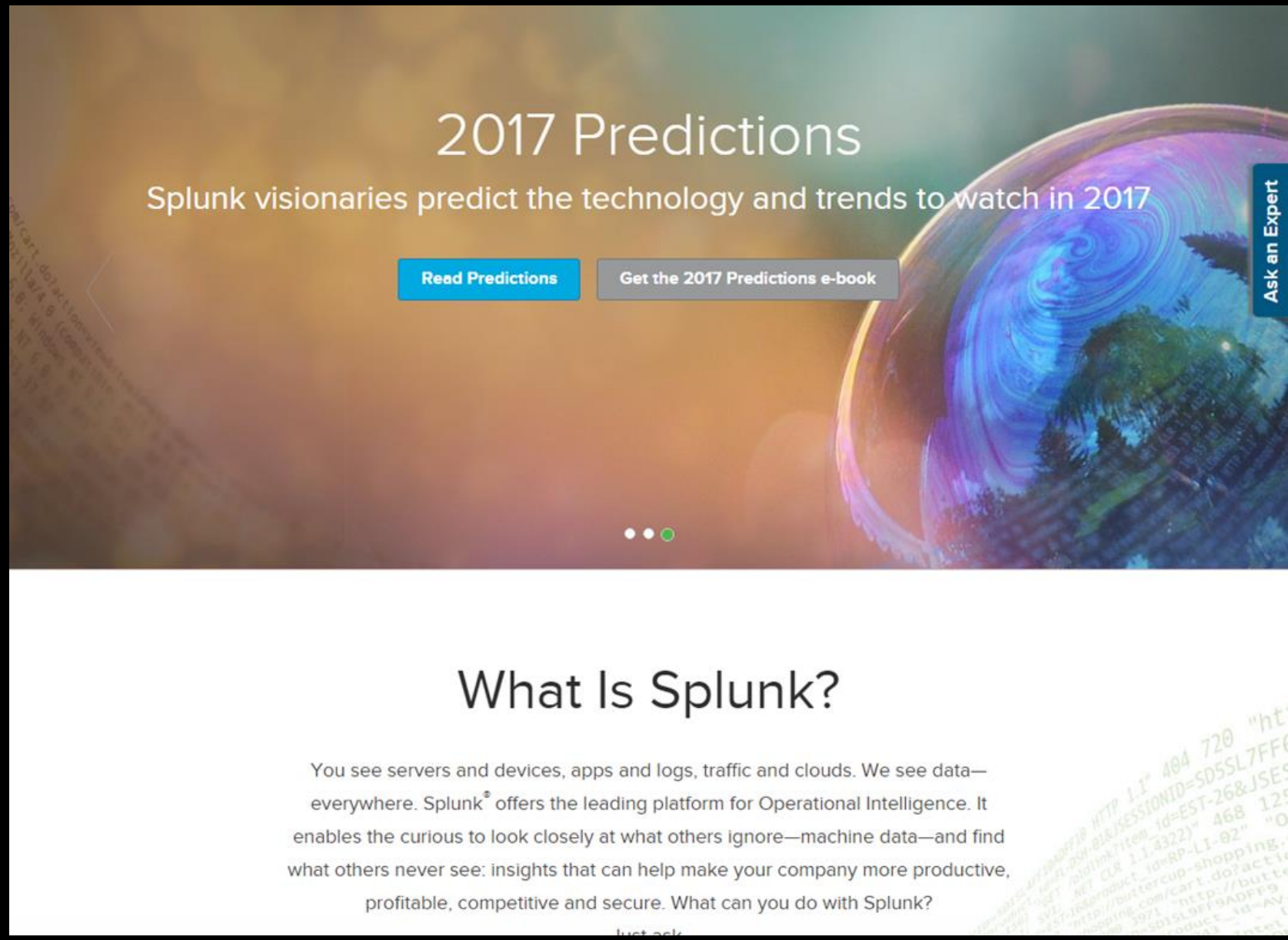
- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

splunk> .conf18

© 2018 SPLUNK INC.

Screenshot and Title

This is where the subtitle goes



© 2018 SPLUNK INC.

Screenshot and Title

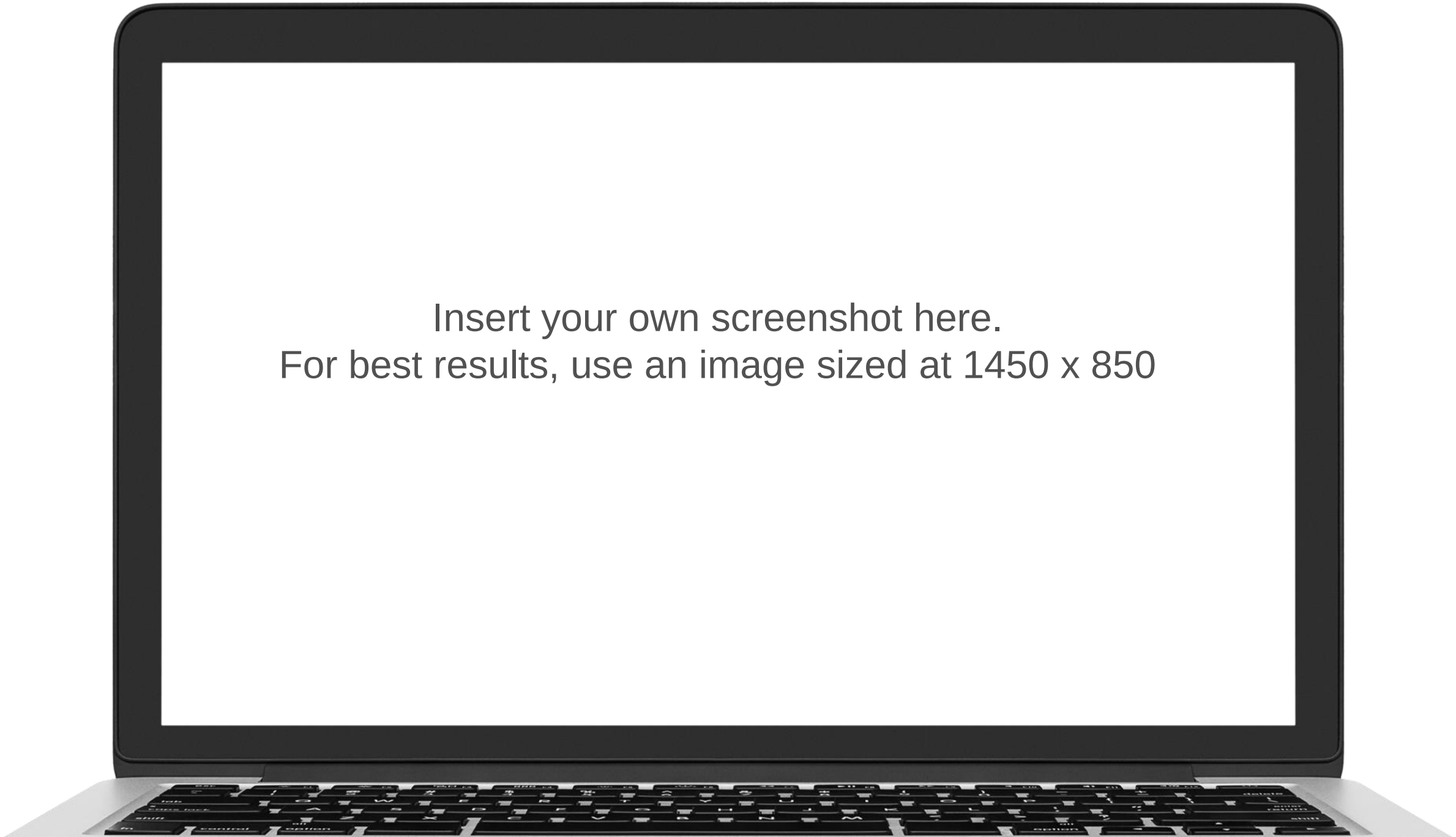
This is where the subtitle goes

What Is Splunk?

You see servers and devices, apps and logs, traffic and clouds. We see data—everywhere. Splunk® offers the leading platform for Operational Intelligence. It enables the curious to look closely at what others ignore—machine data—and find what others never see: insights that can help make your company more productive, profitable, competitive and secure. What can you do with Splunk?

Just ask.

© 2018 SPLUNK INC.



© 2018 SPLUNK INC.

Big Stats and Supporting Text

This is where the subtitle goes

#

This layout is used for large statistics

#

If you have fewer than five stats to display

#

Simply click on the extra circles and text boxes

#

Choose delete

#

Delete one more time to remove the placeholder s

© 2018 SPLUNK INC.

Big Stats and Supporting Text

This is where the subtitle goes

#

This layout is used for large statistics

#

If you have fewer than five stats to display

#

Simply click on the extra circles and text boxes

#

Choose delete

#

Delete one more time to remove the placeholder s

splunk> .conf18

© 2018 SPLUNK INC.

Three Icons with Supporting Text

This is where the subtitle goes

Title, 24pt

Title, 24pt

Title, 24pt

© 2018 SPLUNK INC.

Three Icons with Supporting Text

This is where the subtitle goes

Title, 24pt

Title, 24pt

Title, 24pt

© 2018 SPLUNK INC.

Four Icons with Supporting Text

This is where the subtitle goes

Title, 24pt

Title, 24pt

Title, 24pt

Title, 24pt

© 2018 SPLUNK INC.

Four Icons with Supporting Text

This is where the subtitle goes

Title, 24pt

Title, 24pt

Title, 24pt

Title, 24pt

© 2018 SPLUNK INC.

Five Icons with Supporting Text

This is where the subtitle goes

Title, 24pt

Title, 24pt

Title, 24pt

Title, 24pt

Title, 24pt

© 2018 SPLUNK INC.

Five Icons with Supporting Text

This is where the subtitle goes

Title, 24pt

Title, 24pt

Title, 24pt

Title, 24pt

Title, 24pt

Making machine data accessible, usable and valuable to everyone.

© 2018 SPLUNK INC.

© 2018 SPLUNK INC.

Key Takeaways

This is where the subtitle goes

1. First level bullets should be sentence case, 28pt
2. First level bullets should be sentence case, 28pt
3. First level bullets should be sentence case, 28pt

© 2018 SPLUNK INC.

Thank You

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

.conf18

splunk>

© 2018 SPLUNK INC.

Tracks and Sessions

New to Splunk	**11:15 – 12:15**	Splunk Overview	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Getting Started with Splunk Enterprise **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	Data Onboarding	**Presenter Name**, Senior Sales Engineer, Splunk
IT Ops	**11:15 – 12:15**	Happy Apps, Happy Users: Using Splunk APM	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Splunk Enterprise for IT Troubleshooting **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	How to Design, Build and Map IT and Business Services in Splunk	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
Security	**11:15 – 12:15**	Build a Security Portfolio That Strengthens Your Security Posture	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Building an Analytics Driven Security Operation Center using Splunk Enterprise Security	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	An End-To-End Approach: Detect via Behavior and Orchestrate via SIEM	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
Advanced	**11:15 – 12:15**	The Power of SPL	**Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Advanced Analytics and Machine Learning in Splunk	**Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	Ransomware Investigation and Prevention Strategies **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk

© 2018 SPLUNK INC.

BUTTERCUP SPLUNKER

Mascot, Internal Mischief

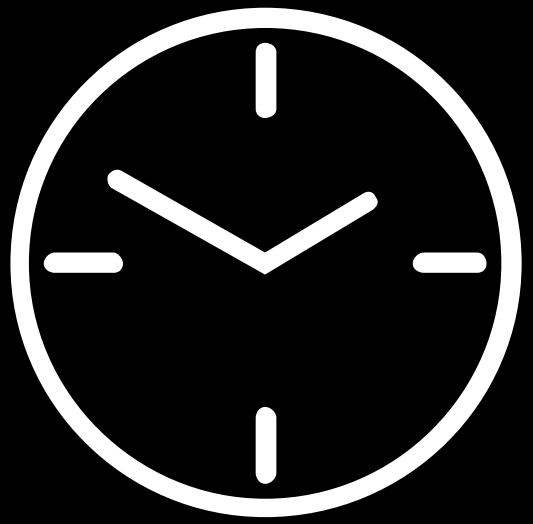
© 2018 SPLUNK INC.

Splunk Demo

Presented by Buttercup Splunker

splunk> .conf18

© 2018 SPLUNK INC.



BREAK

15 MINUTES

splunk> .conf18

© 2018 SPLUNK INC.

Customer Logo Here

Please use an all-white image on a transparent background, like this Splunk logo: splunk>

splunk> .conf18

© 2018 SPLUNK INC.

Join the Pony Poll

ponypoll.com/***

Join us at Splunk .conf18

October 1–4, 2018

Walt Disney World Swan and Dolphin Resort in Orlando

8,750+ Splunk Enthusiasts

300+ Sessions

100+ Customer Speakers

Plus Splunk University:

Three Days: September 29-October 1, 2018

Get CPE credits for CISSP, CAP, SSCP

Register now at conf.splunk.com

.conf18

splunk>

© 2018 SPLUNK INC.

Q&A

Participant name | Role

Participant name | Role

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Corporate Logo

Copy/paste these graphics to use in your own presentation

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

© 2018 SPLUNK INC.

Splunk Corporate Logo

Copy/paste these graphics to use in your own presentation

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

© 2018 SPLUNK INC.

Splunk Corporate Logo: One Color

Copy/paste these graphics to use in your own presentation

splunk>®

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

© 2018 SPLUNK INC.

Splunk Corporate Logo: One Color

Copy/paste these graphics to use in your own presentation

splunk>®

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Product Logo: Two Color

Copy/paste these graphics to use in your own presentation

Note: The Splunk product logo should be used whenever you are referencing the product or its capabilities.

© 2018 SPLUNK INC.

Splunk Product Logo: Two Color

Copy/paste these graphics to use in your own presentation

Note: The Splunk product logo should be used whenever you are referencing the product or its capabilities.

© 2018 SPLUNK INC.

Premium Solutions Logos

Copy/paste these graphics to use in your own presentation

Splunk User Behavior Analytics™

Splunk User Behavior Analytics™

Splunk IT Service Intelligence™

Splunk IT Service Intelligence™

Splunk Enterprise Security™

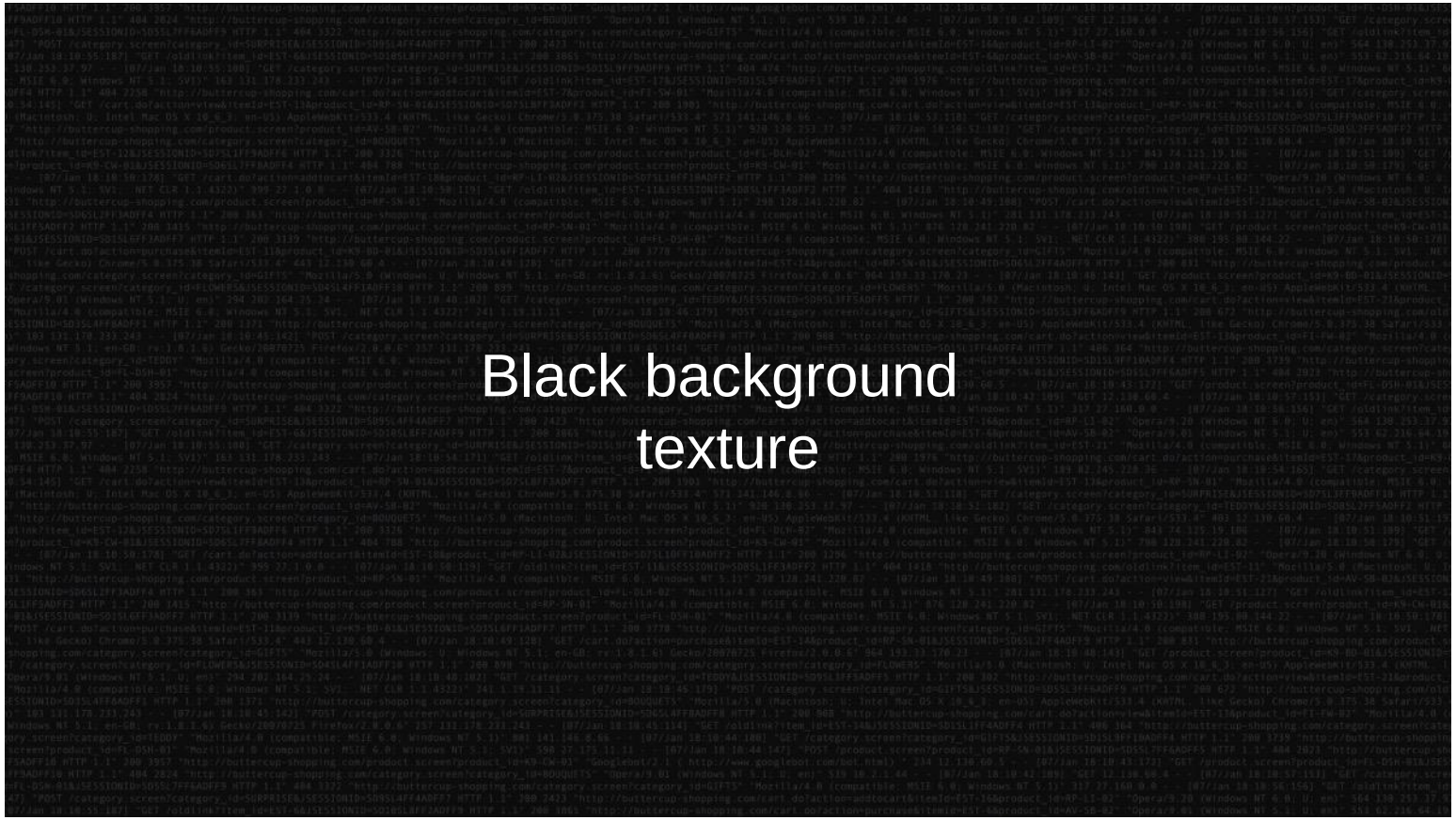
Splunk Enterprise Security™

splunk> .conf18

© 2018 SPLUNK INC.

Line and Shape Assets

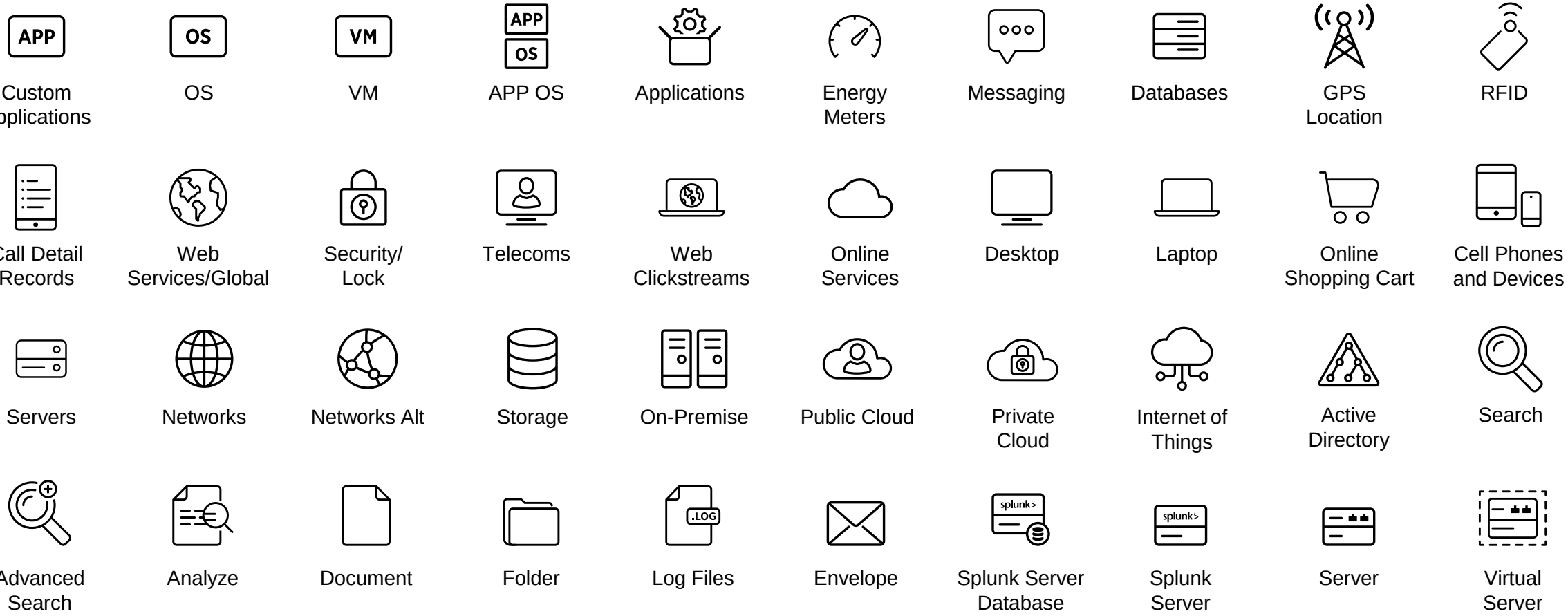
Copy/paste this graphic to use in your own presentations



© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

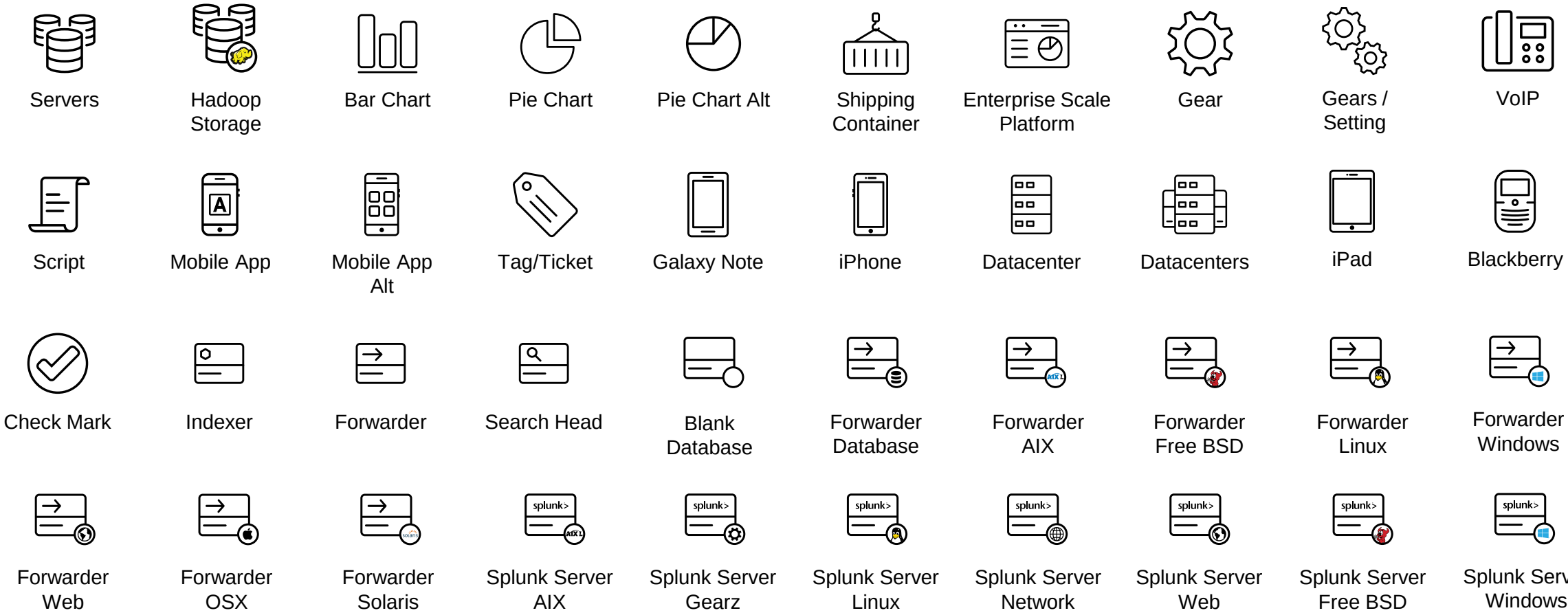


splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations



© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Splunk Server Solaris
Splunk Server OSX
Splunk Server Search
Failed Splunk Server
Failed Server
Server License
Tools
Clock
RSS
Send Arrow

Android
Network Switch
Router
Cloud Services Monitoring
Telephone
Facebook
Facebook Color
Twitter
Twitter Color
LinkedIn

LinkedIn Color
YouTube
YouTube Color
Healthcare
Info
Stop
Calendar
Alert
Hospital
Office Building

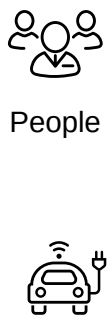
Process Analytics
Universal Collection
Wire Data
Load Balancing
Cycle
Customer Support
Customer Support Alt
Male
Female
Stacked Document/ Documents

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


People

People Alt

Splunk People

Splunk Male

Splunk Female

Meter

Signature Capture

POS Card Reader

EMV Card Reader

Factory

Electric Car

Shield

Footsteps

Malware Document

Malware

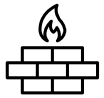
Malware Packaged

Security Server

Security Badge

Virus

Key


Firewall

Botnet

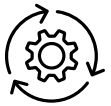
Attacker General

Attacker Insider

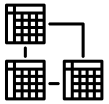
Attacker Nation/State

Real Time Monitoring

Detect Unknown Threats


Asset Lifecycle Management

Instant Pivot


Data Model

Fraud Detection

Product Analytics/ Custom Dashboard

Host/ Activity/Security

Operational Efficiency

Shield Revised

Waste Reduction

Monitoring

Environmental and Industrial

House

Innovate

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Mission Operations

Facilities and Assets

Warfighter

Vehicle Fleet

Vehicle Fleet Cloud

Share with Mission Partners

Collaboration

Data Management

Device Usage Analytics

DHCP/DNS

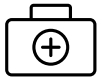
Disaster Relief

Campus Experience

Learning Management System

Machine learning

Learning Management


Emergency Management

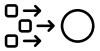
Shared Services

Consolidation

Grades

Admissions

Admissions and Registratio


Consolidation and Modernization

Consolidation and Modernization

Situational Awareness

Infrastructure

Public Services

IT Infrastructure

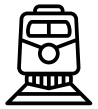
Campus Housing

Connected Campus + Smart Campus

Control Fraud Waste and Abuse

Dispatch Systems

Subway


Locomotive

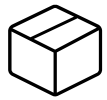
Energy

Water

Vulnerability Scans

Transportation

Threat Intelligence


Package

Business Analytics

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Badge/Pass

Tailored

Hourglass

Predictive Analytics

Satellite

Intrusion Prevention

Application Management

DevOps/ Application Deployment

IT Operations

Adaptive Response

Automation or Operational Efficiency

Preventative Maintenance

Splunk Enterprise License

Aviation

New Developer Resources

Data Prep & Analysis

Filter Results

Parallel Processing

Scalable

Kiosk

Value Assurance

Trading Systems

Flexible

Platform

Hypervisor

Heart

Patient Generated Data

Healthcare App

CMDB

Service Monitoring

Cost Savings

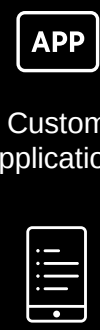
Education

Threat PDF Stealing

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Custom Applications

OS

VM

APP OS

Applications

Energy Meters

Messaging

Databases

GPS Location

RFID

Call Detail Records

Web Services/Global

Security/ Lock

Telecoms

Web Clickstreams

Online Services

Desktop

Laptop

Online Shopping Cart

Cell Phones and Devices

Servers

Networks

Networks Alt

Storage

On-Premise

Public Cloud

Private Cloud

Internet of Things

Active Directory

Search

Advanced Search

Analyze

Document

Folder

Log Files

Envelope

Splunk Server Database

Splunk Server

Server

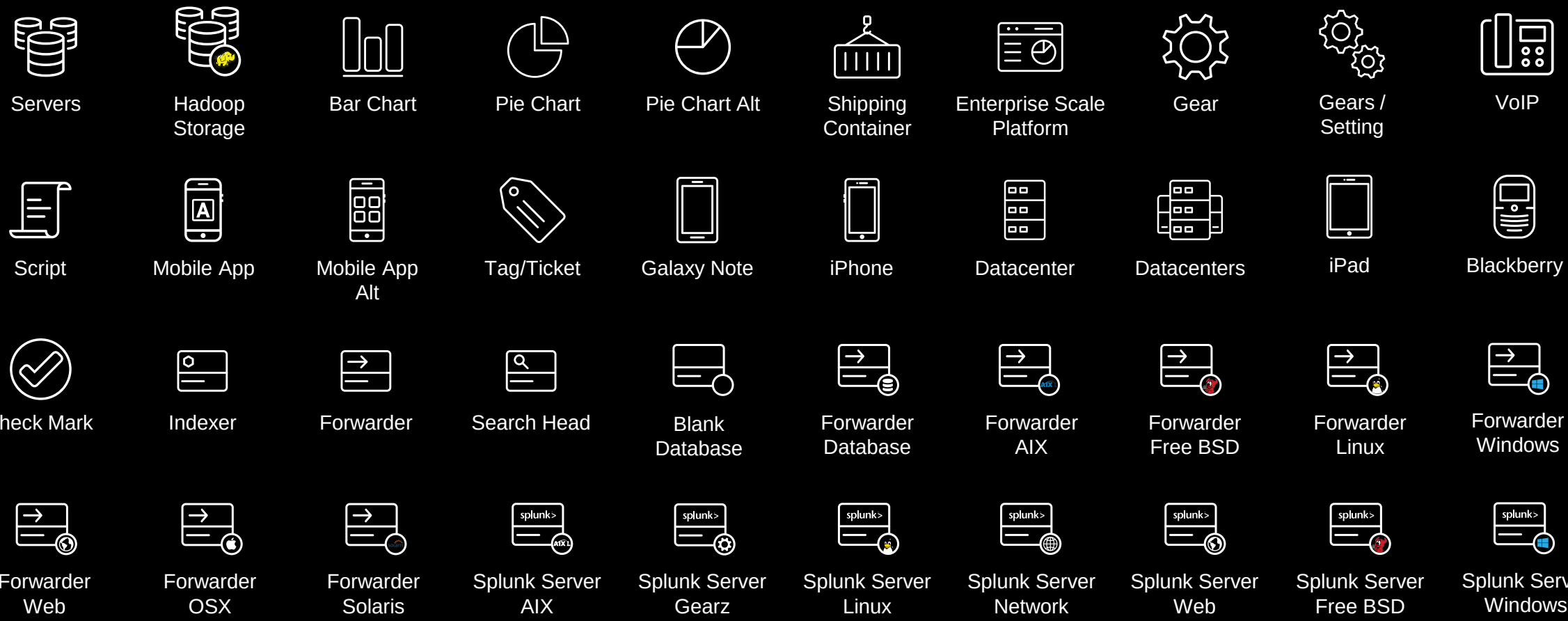
Virtual Server

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations



splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Splunk Server Solaris
Splunk Server OSX
Splunk Server Search
Failed Splunk Server
Failed Server
Server License
Tools
Clock
RSS
Send Arrow

Android
Network Switch
Router
Cloud Services Monitoring
Telephone
Facebook
Facebook Color
Twitter
Twitter Color
LinkedIn

LinkedIn Color
YouTube
YouTube Color
Healthcare
Info
Stop
Calendar
Alert
Hospital
Office Building

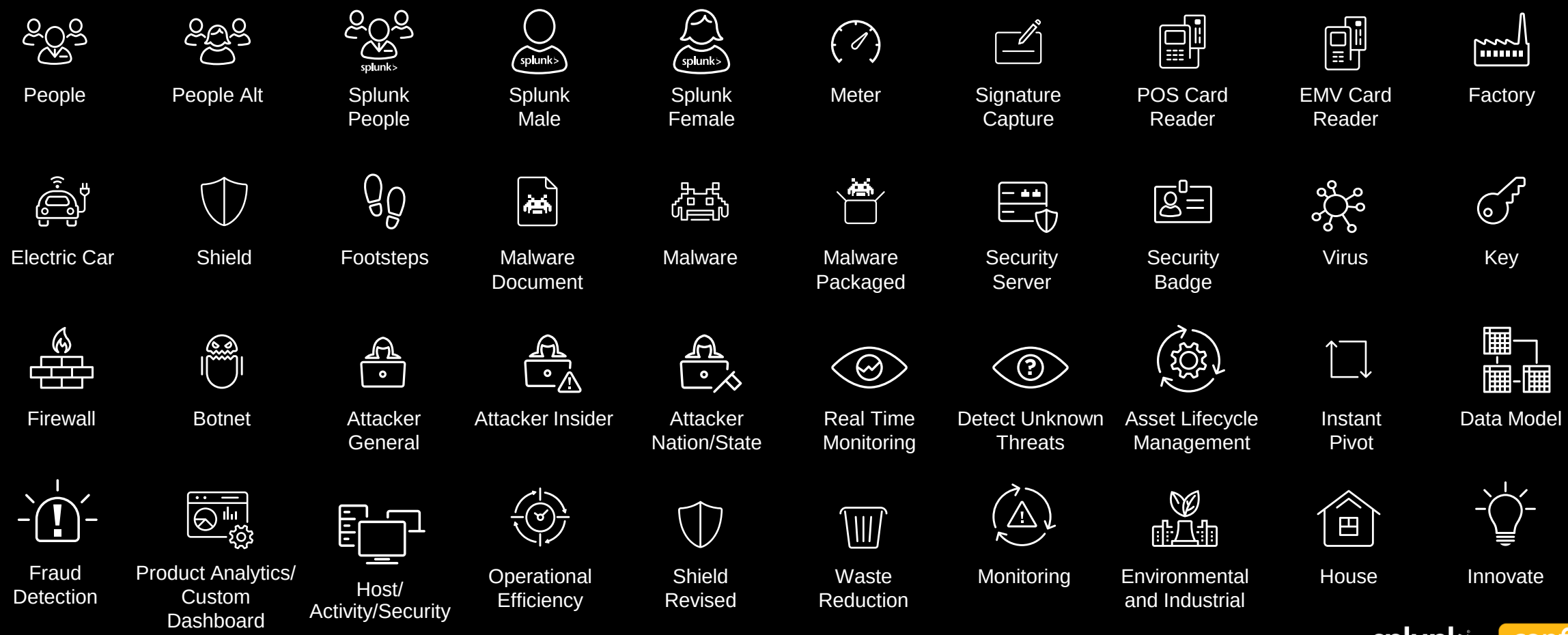
Process Analytics
Universal Collection
Wire Data
Load Balancing
Cycle
Customer Support
Customer Support Alt
Male
Female
Stacked Document/ Documents

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations



splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Mission Operations
Facilities and Assets
Warfighter
Vehicle Fleet
Vehicle Fleet Cloud
Share with Mission Partners
Collaboration
Data Management
Device Usage Analytics
DHCP/DNS

Disaster Relief
Campus Experience
Learning Management System
Machine learning
Learning Management
Emergency Management
Shared Services
Consolidation
Grades
Admissions

Admissions and Registration
Consolidation and Modernization
Consolidation and Modernization
Situational Awareness
Infrastructure
Public Services
IT Infrastructure
Campus Housing
Connected Campus + Smart Campus
Control Fraud Waste and Abuse

Dispatch Systems
Subway
Locomotive
Energy
Water
Vulnerability Scans
Transportation
Threat Intelligence
Package
Business Analytics

splunk> .conf18

© 2018 SPLUNK INC.

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Badge/Pass

Tailored

Hourglass

Predictive Analytics

Satellite

Intrusion Prevention

Application Management

DevOps/ Application Deployment

IT Operations

Adaptive Response

Automation or Operational Efficiency

Preventative Maintenance

Splunk Enterprise License

Aviation

New Developer Resources

Data Prep & Analysis

Filter Results

Parallel Processing

Scalable

Kiosk

Value Assurance

Trading Systems

Flexible

Platform

Hypervisor

Heart

Patient Generated Data

Healthcare App

CMDB

Service Monitoring

Cost Savings

Education

Threat PDF Stealing