Anatomy of a successful IT Service Intelligence Deployment

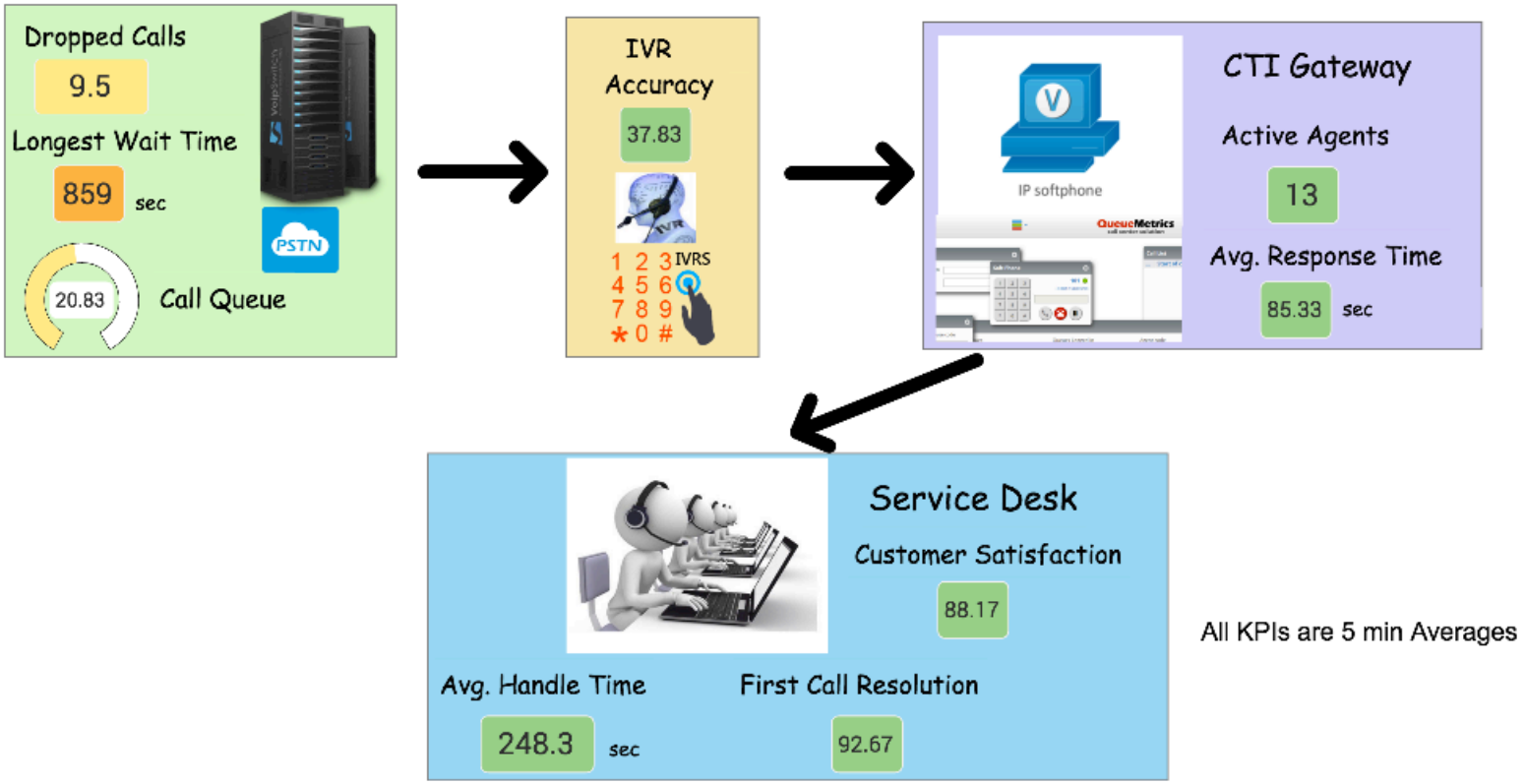
Martin Wiser (ITOA Practitioner, Splunk)

Bill Babilon (ITOA Solutions Architect, Splunk)

Agenda

- Why did your organization buy IT SI
- How do you get started
  - Pre-Reqs
  - Implementation Methodology
  - Deployment Pipeline – Keeping the Ball Moving
- Service Decomposition
- Lessons Learned & Best Practices

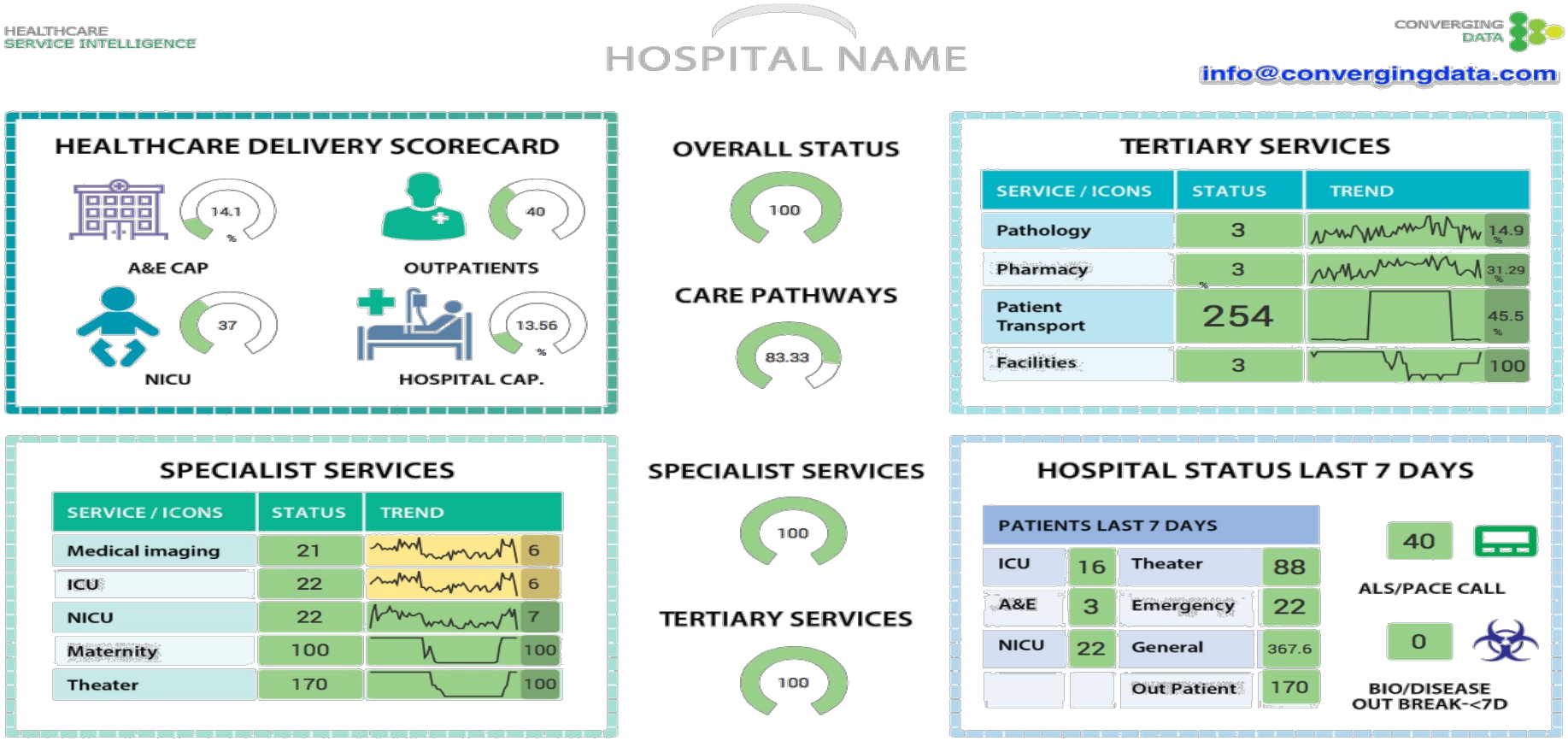
Why did you buy IT SI?



All KPIs are 5 min Averages

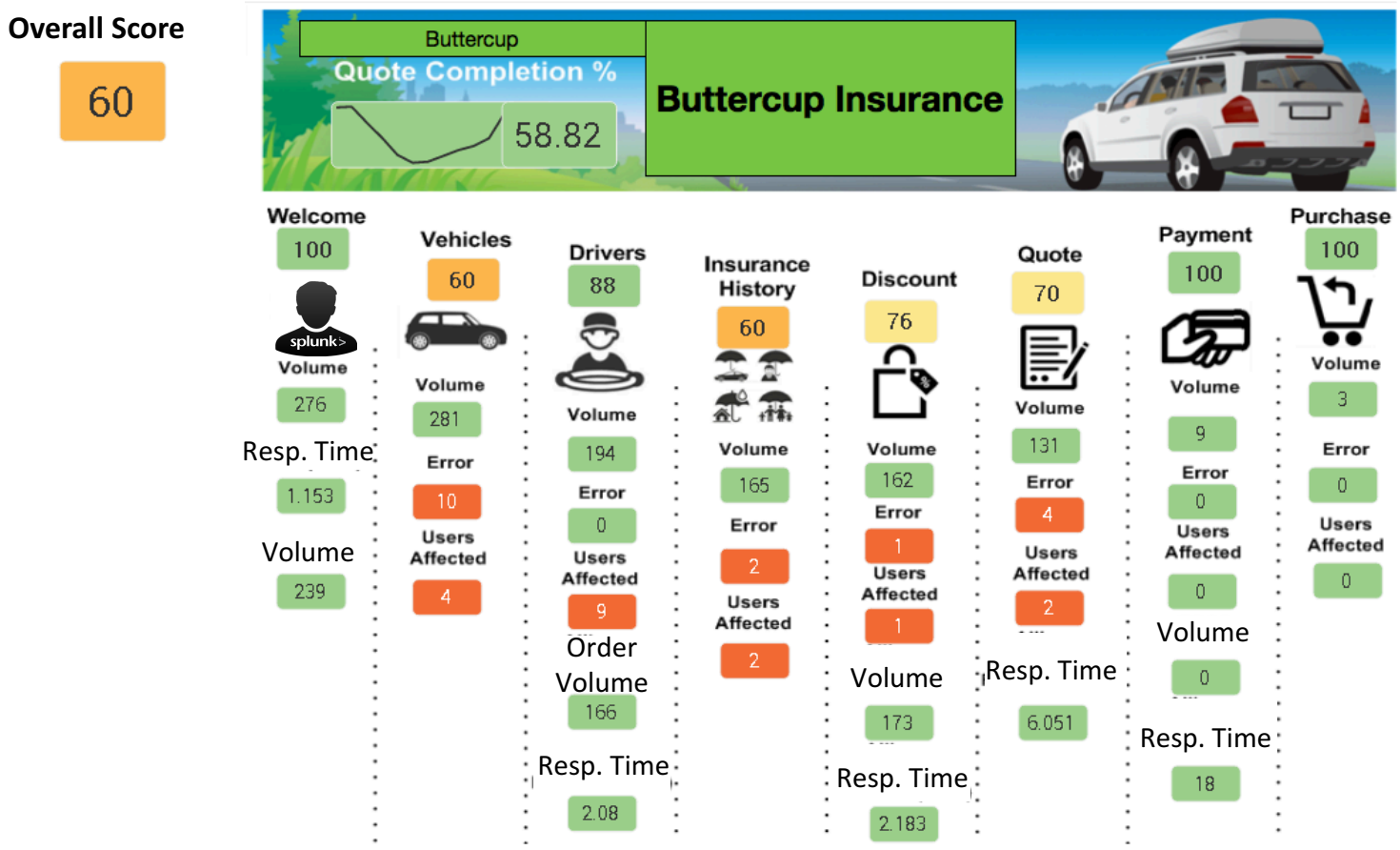
splunk> .conf2016

Why did you buy IT SI?

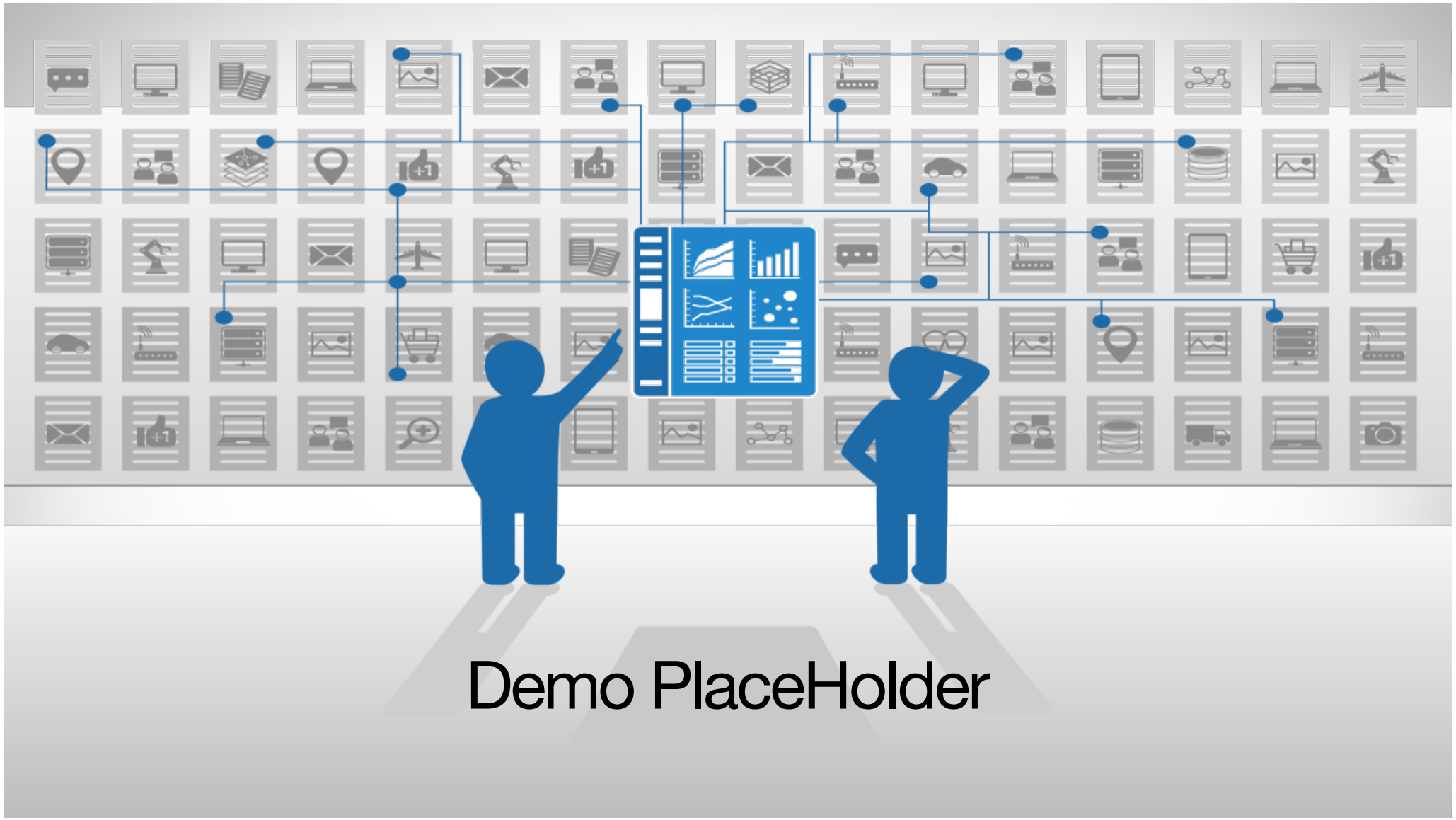


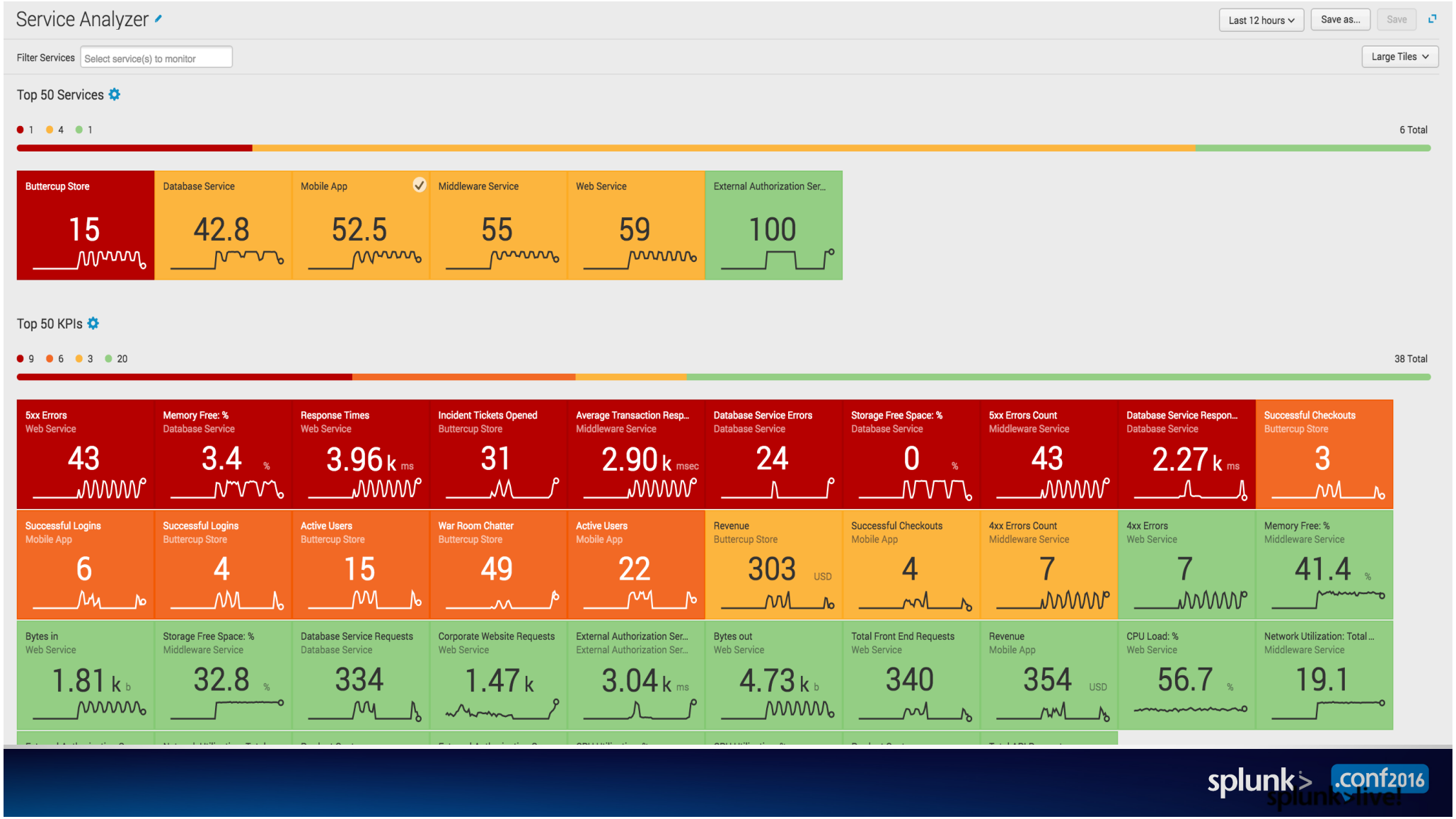
splunk> .conf2016

Why did you buy IT SI?

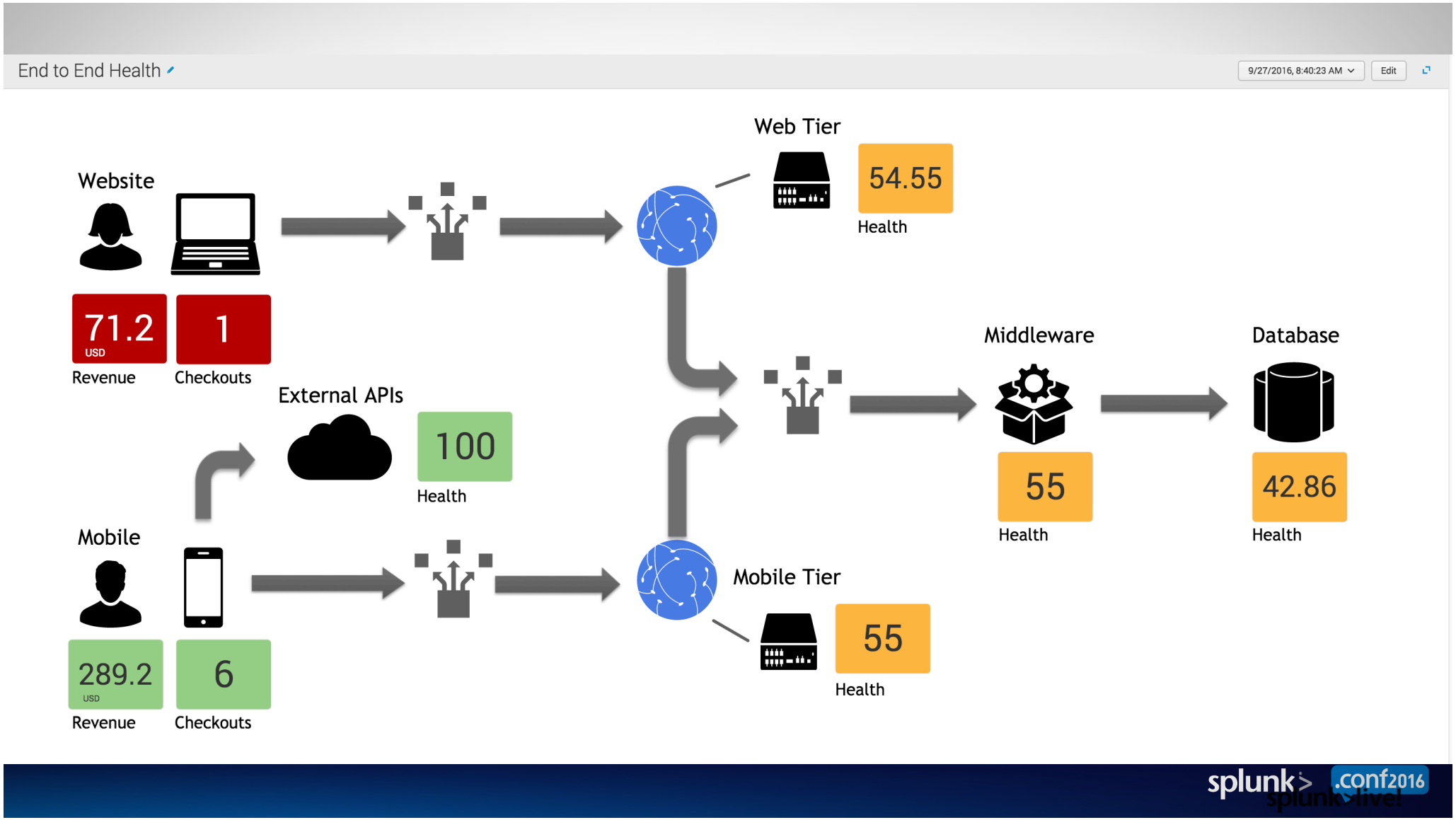


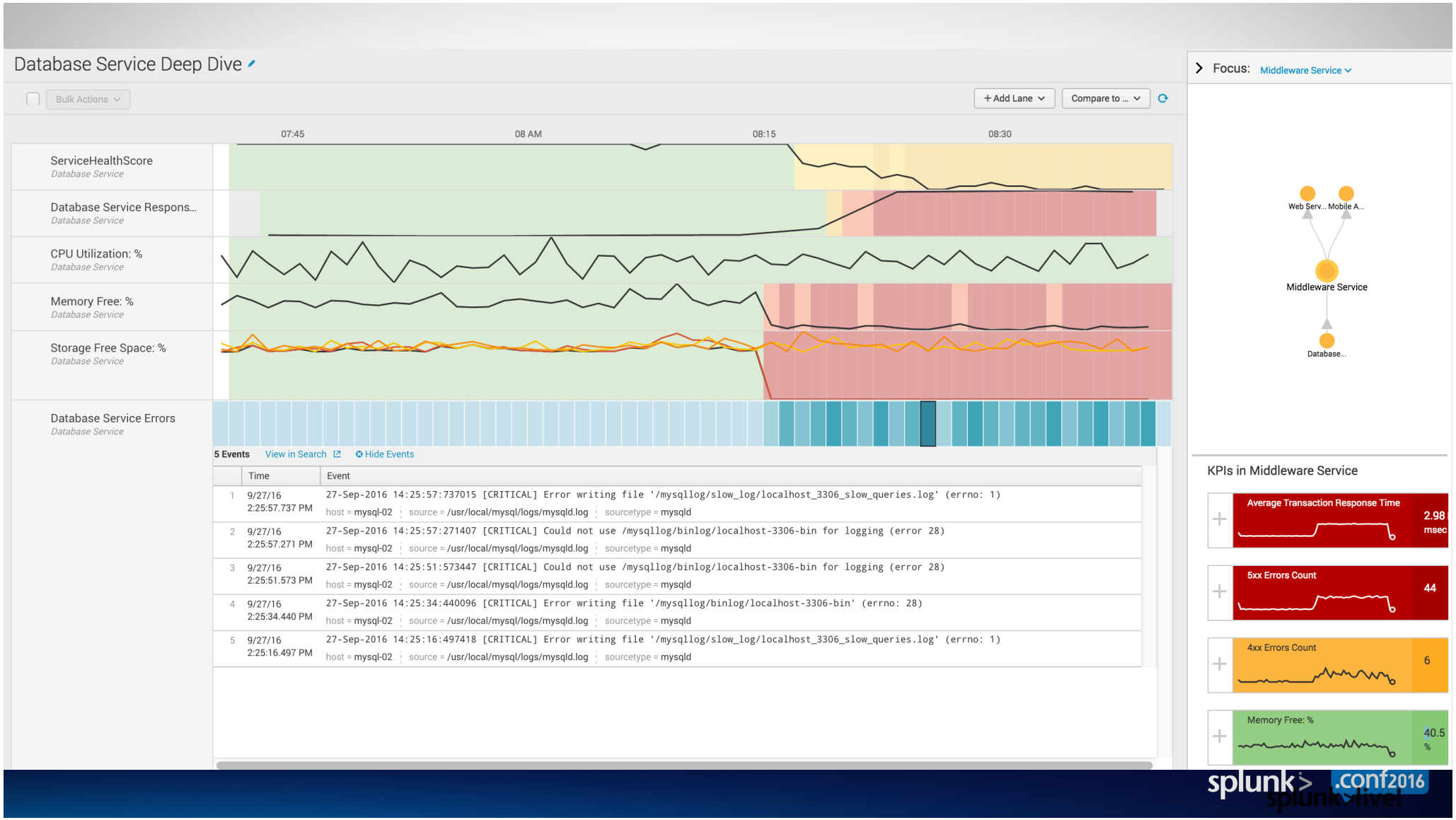
splunk> .conf2016


Demo PlaceHolder



splunk> .conf2016
splunk> live!


End to End Health
9/27/2016, 8:40:23 AM
Edit
Web Tier
54.55
Health
Website
71.2
USD
Revenue
1
Checkouts
External APIs
100
Health
Middleware
55
Health
Database
42.86
Health
Mobile
289.2
USD
Revenue
6
Checkouts
Mobile Tier
55
Health


Database Service Deep Dive
Bulk Actions
+ Add Lane
Compare to ...
07:45
08 AM
08:15
08:30
ServiceHealthScore
Database Service
Database Service Respons...
Database Service
CPU Utilization: %
Database Service
Memory Free: %
Database Service
Storage Free Space: %
Database Service
Database Service Errors
Database Service
5 Events
View in Search
Hide Events
Time
Event
1 9/27/16 2:25:57.737 PM
27-Sep-2016 14:25:57:737015 [CRITICAL] Error writing file '/mysqllog/slow_log/localhost_3306_slow_queries.log' (errno: 1)
host = mysql-02 source = /usr/local/mysql/logs/mysqld.log sourcetype = mysqld
2 9/27/16 2:25:57.271 PM
27-Sep-2016 14:25:57:271407 [CRITICAL] Could not use /mysqllog/binlog/localhost-3306-bin for logging (error 28)
host = mysql-02 source = /usr/local/mysql/logs/mysqld.log sourcetype = mysqld
3 9/27/16 2:25:51.573 PM
27-Sep-2016 14:25:51:573447 [CRITICAL] Could not use /mysqllog/binlog/localhost-3306-bin for logging (error 28)
host = mysql-02 source = /usr/local/mysql/logs/mysqld.log sourcetype = mysqld
4 9/27/16 2:25:34.440 PM
27-Sep-2016 14:25:34:440096 [CRITICAL] Error writing file '/mysqllog/binlog/localhost-3306-bin' (errno: 28)
host = mysql-02 source = /usr/local/mysql/logs/mysqld.log sourcetype = mysqld
5 9/27/16 2:25:16.497 PM
27-Sep-2016 14:25:16:497418 [CRITICAL] Error writing file '/mysqllog/slow_log/localhost_3306_slow_queries.log' (errno: 1)
host = mysql-02 source = /usr/local/mysql/logs/mysqld.log sourcetype = mysqld
Focus: Middleware Service
Web Serv...
Mobile A...
Middleware Service
Database...
KPIs in Middleware Service
Average Transaction Response Time
2.98
msec
5xx Errors Count
44
4xx Errors Count
6
Memory Free: %
40.5
%

Environment & Data Validation

How do I get started

- Make sure Environment is working
  - Validate Sizing (IDX & SH)
- Check Versions, index forwarding
- Multiple Environments?
  - Focus on Production
- **Nbr of Concurrent Searches**
  - **(ITSI triggers many small searches)**

How do I get started?

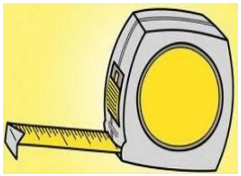
1

Start with a problem worth solving

2

Bring subject experts together

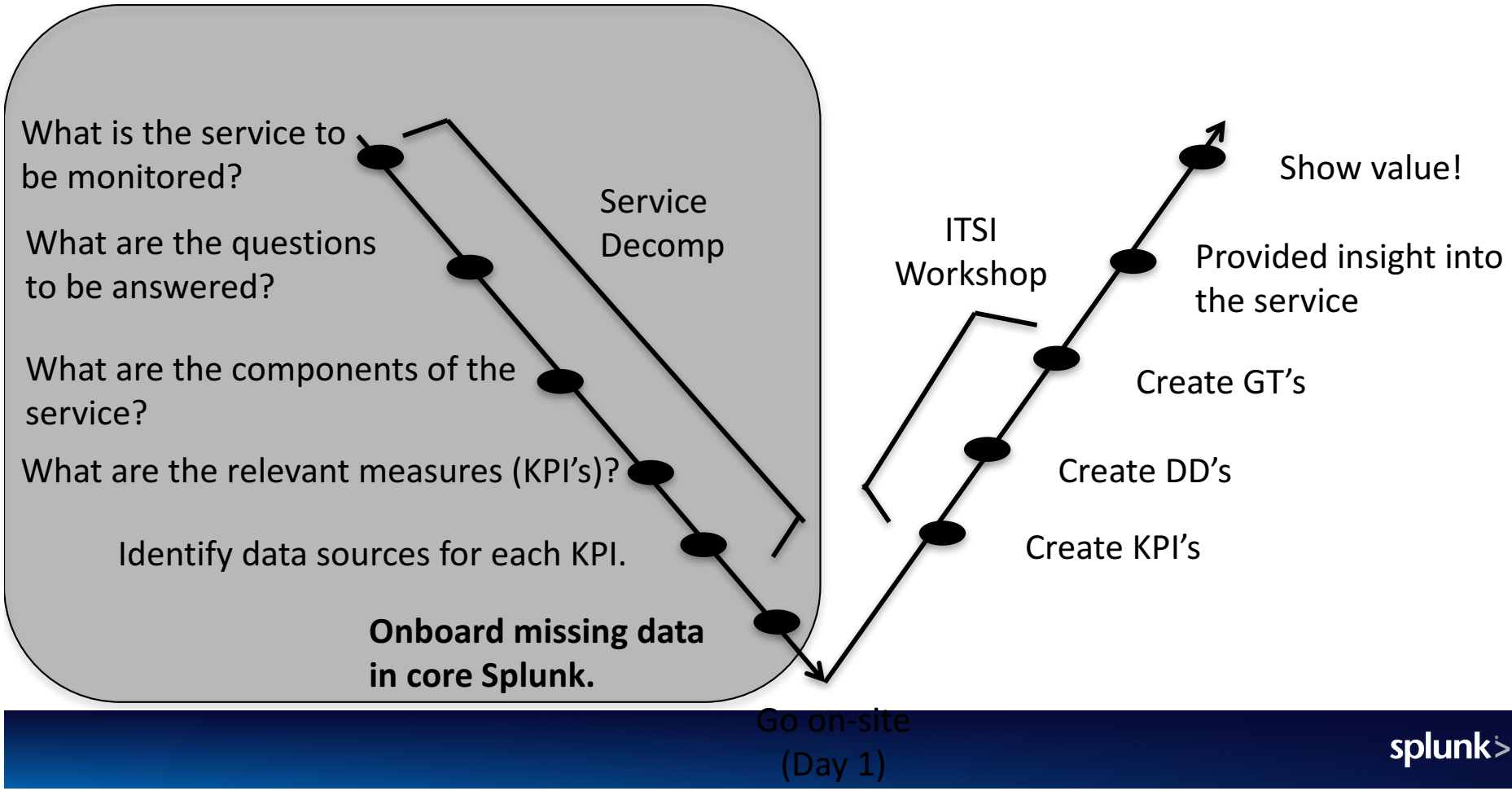
3



Decompose and design before configuring

splunk> .conf2016

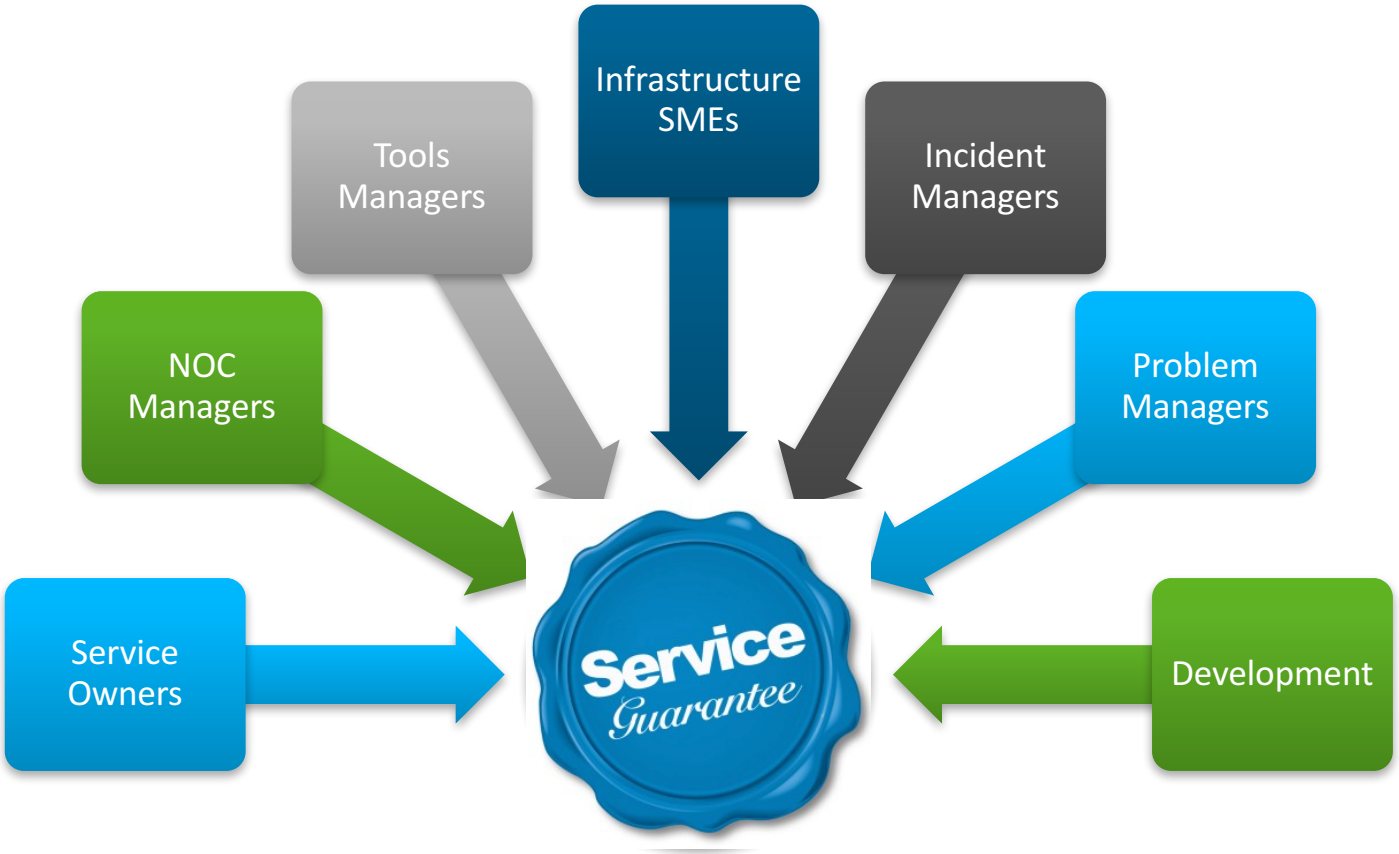
Top Down Approach to a Bottom Up Problem



Initial Kick Off

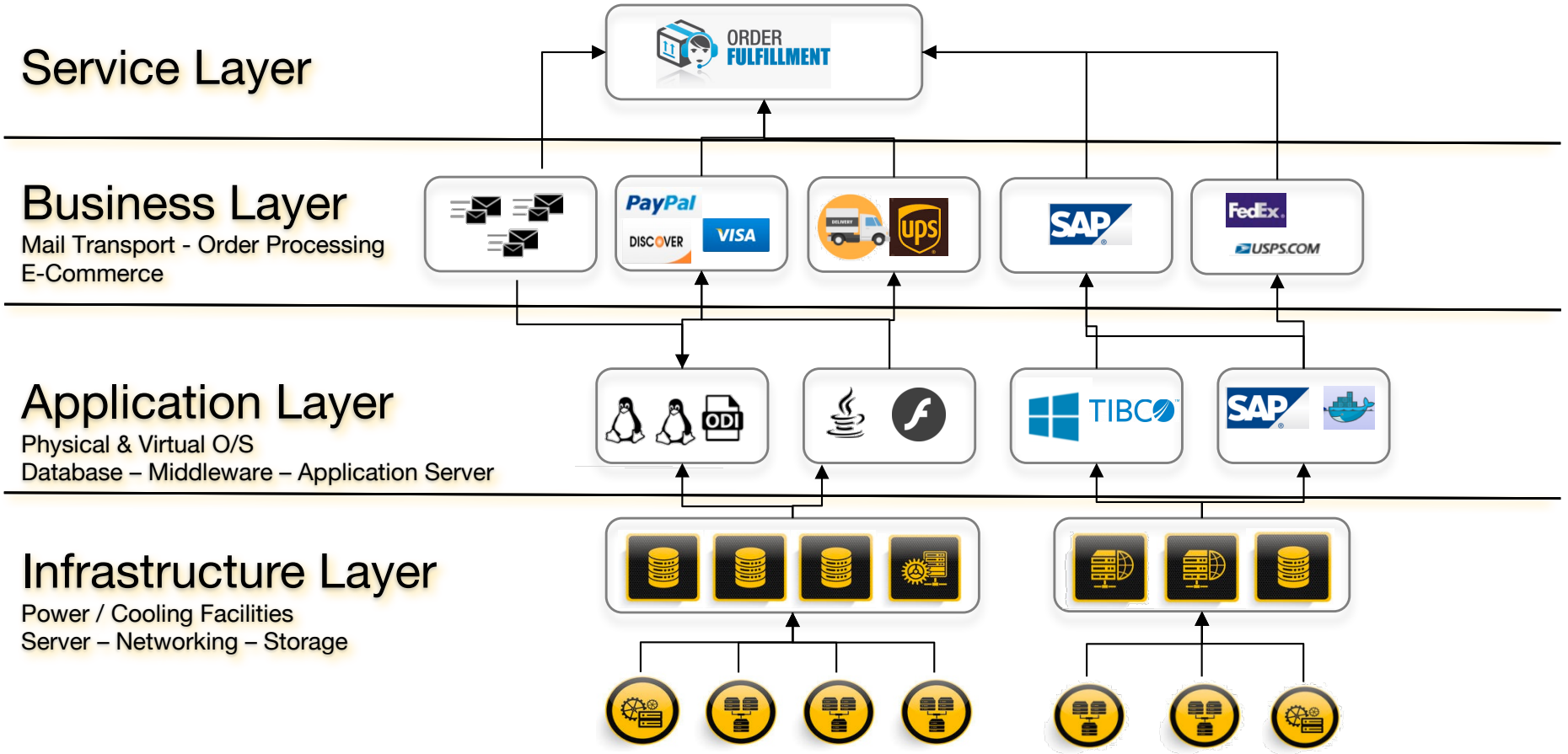
- Ensure you have stakeholders present
- Align Expectations
  - Monitoring/Apps/Opps Teams
- D E M O
  - Leverage Walk through to explain KPIs
- Facilitate Architecture/Data Flow Discussion and document KPIs (also schedule)
- Get KPI contact for follow up
- Get Group Agreement on KPIs (priority)

SMEs for Service Decomposition



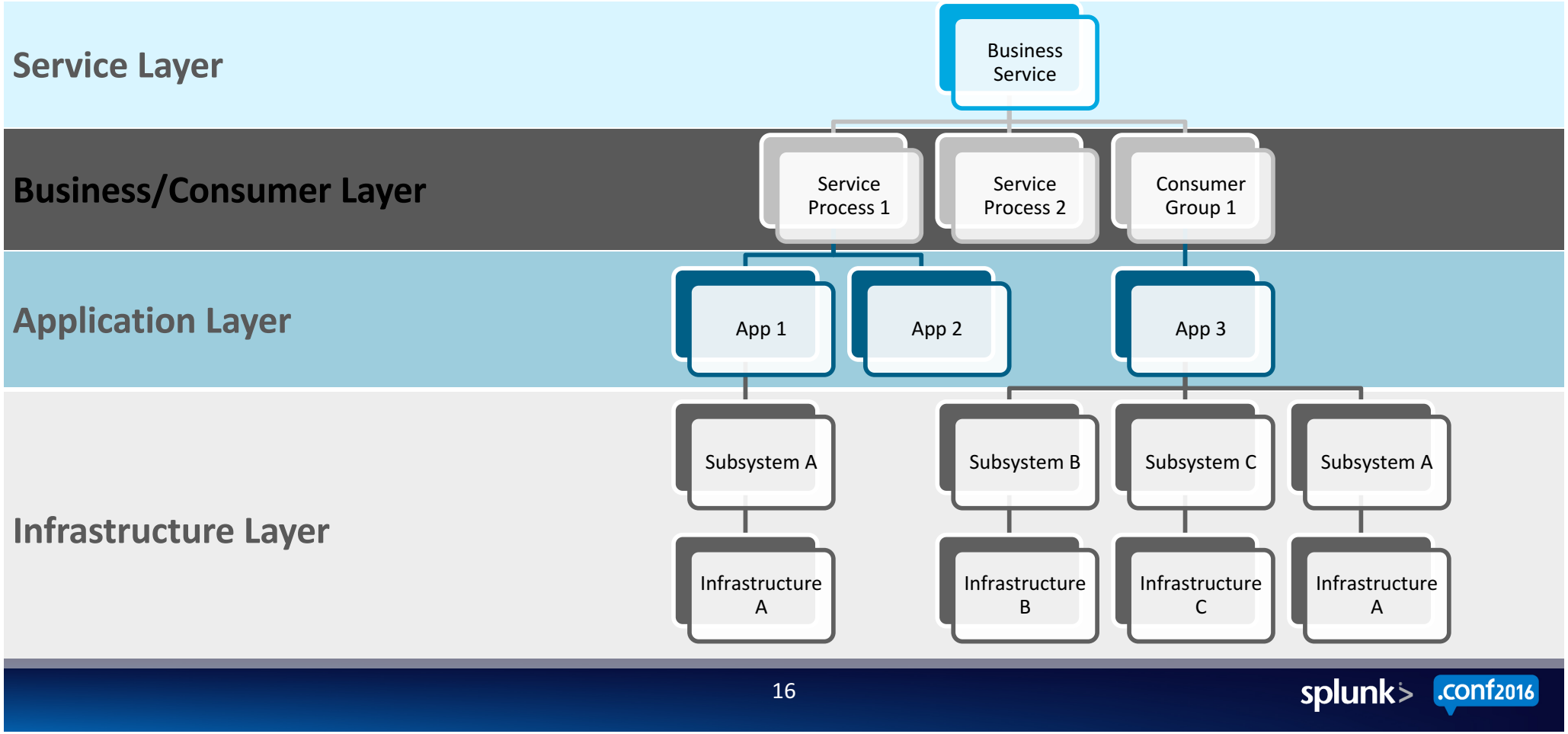
splunk> .conf2016

Expand The Mental Model with Service Decomposition



splunk> .conf2016

Expand the Mental Model with Service Decomposition



splunk> .conf2016

Ask your questions

1. **What is the Name, Description and business objective?**
2. **Who are the Service Owners and Stakeholders?**
3. **What is the business process flow?**
4. **What does the technical architecture look like?**
5. Are you an ITIL shop? What tools do you use for incident/problem and change processes?
6. What hosts make up the service?
7. **What are the existing or desired KPIs of the service? What business metrics map to these KPIs?**

Ask your questions II

8. What Splunk sourcetypes map to these KPIs?
9. What are some examples of critical incidents that have happened in the past with this service and what caused them?
10. **Who are the SMEs for these KPIs and sourcetypes?**
11. Are there **valid** asset stores (CMDB, SCOM, LDAP, VMWare, etc)?
12. What are some known ITSI entities? How many are there?
13. Will there be Notable Events Users -> Do you need to connect to your incident Management System?

Ask your questions III

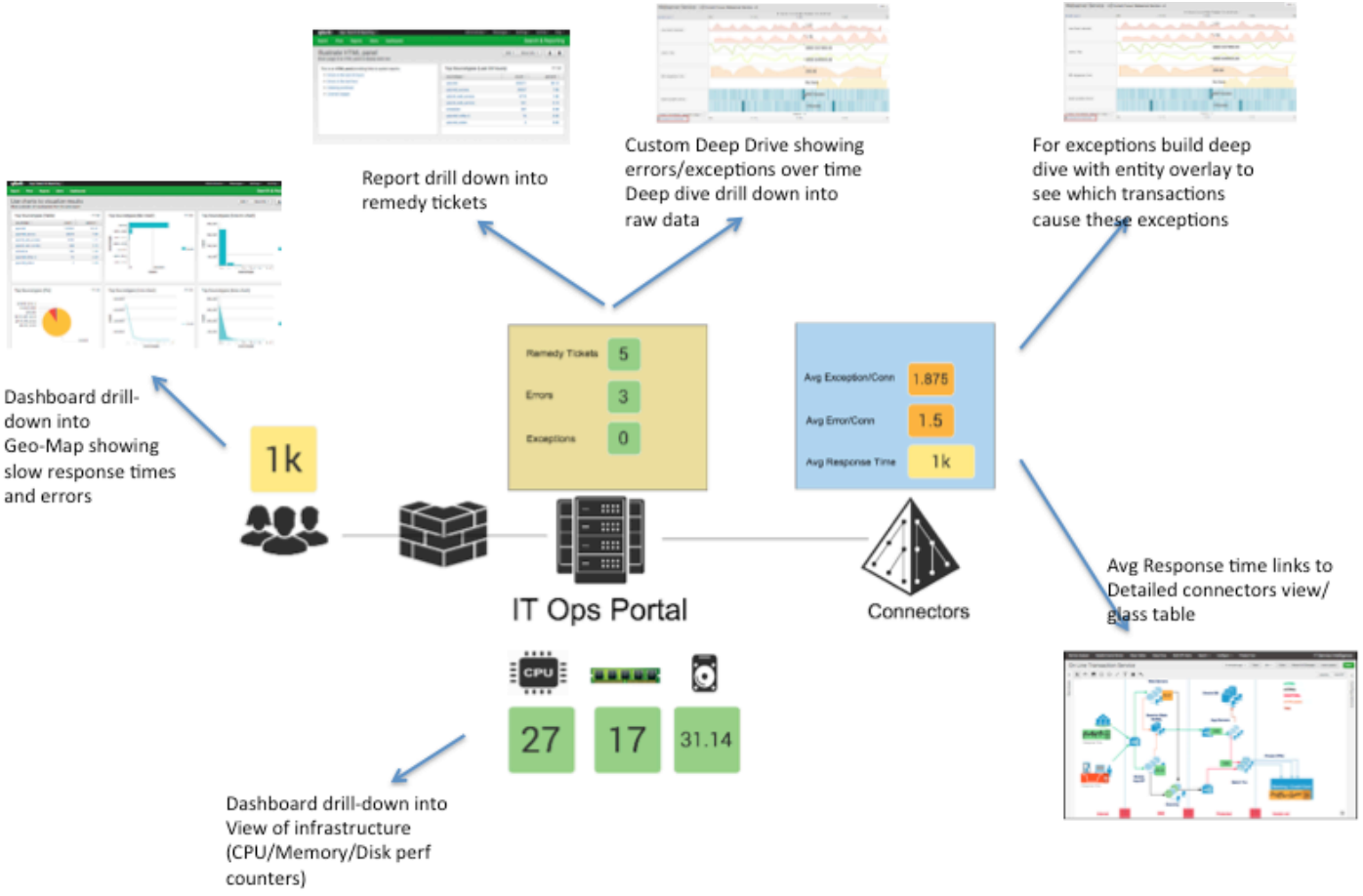
14. How are you going to leverage thresholds?
15. What type of Alerting you you expect?
16. What ITSI Modules do you plan to use?

Deliverable: List/Spreadsheet - **KPIs, Importance, Service, Frequency, SME/sourcetype**, Thresholds, Splunk Search, Notes & Next Steps

KPI Properties

- Good KPIs are Service Focused and allow for correlation
- Map easily to Vital Business Functions
  - **Velocity** -> # of Profile Creations/Updates/API & BackChannel Calls
  - **Response Time, Success Rate/Error Rate**
  - HackAttacks, Orders Processed, Logged In Users
- Bad KPIs are **only** infrastructure focused **without Application/Business Logic**
  - Memory/Disk Utilization
  - CPU Utilization

Environment Mock Up



- Sketch out what glass tables will look like
- Use data that makes sense but isn't overkill

splunk> .conf2016

Initial Service Review Meeting

- Show them the Mock Up/proto type
  - Use proto type to show entities, deep dives & drill downs
- Get agreement on storyboard and flow
- Re-Prioritize KPIs based on customer feedback and **Data availability**

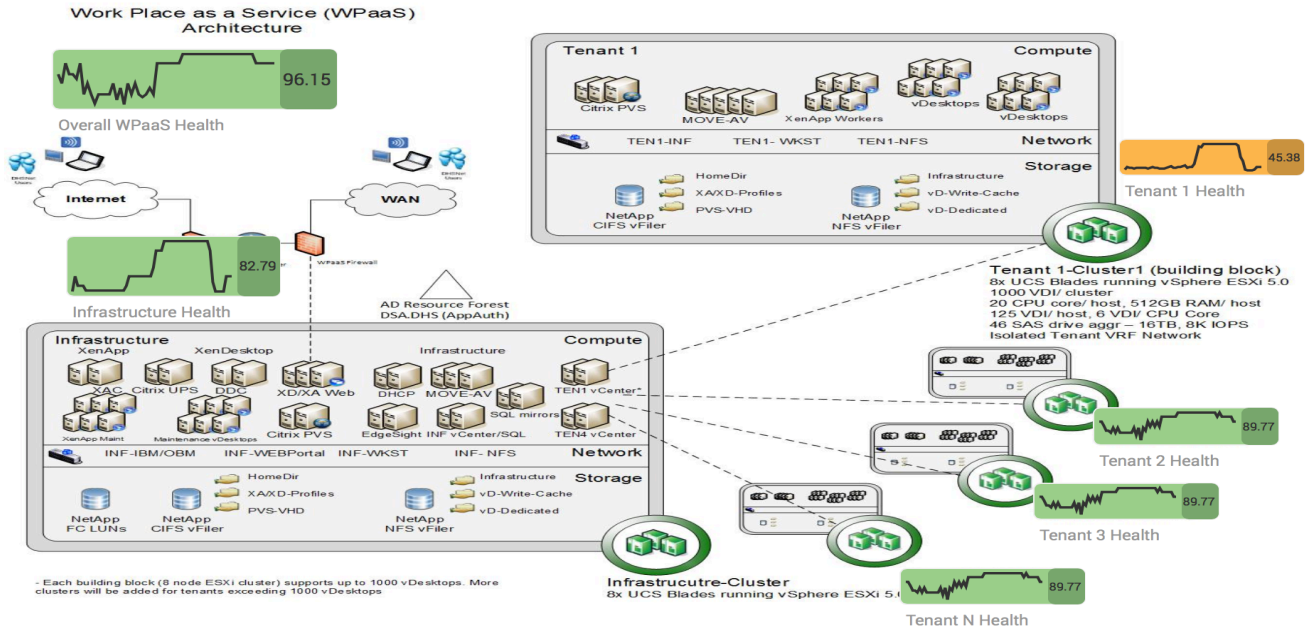
https prd-p-mqslwncv82dh.cloud.splunk.com/en-US/app/itsi/glass_table_editor?id=561b14933bd6902074264cd4&view=standard&owner=nobody — Glass Table Editor | Splunk

splunk> App: IT Service Intelligence | Messages | Settings | Activity | Find | Bill Babilon | My Splunk | Support & Services

Service Analyzer | Notable Events Review | Glass Tables | Deep Dives | Multi KPI Alerts | Search | Configure | Product Tour | IT Service Intelligence

WPaaS_Overall

Standard View | Now | Edit

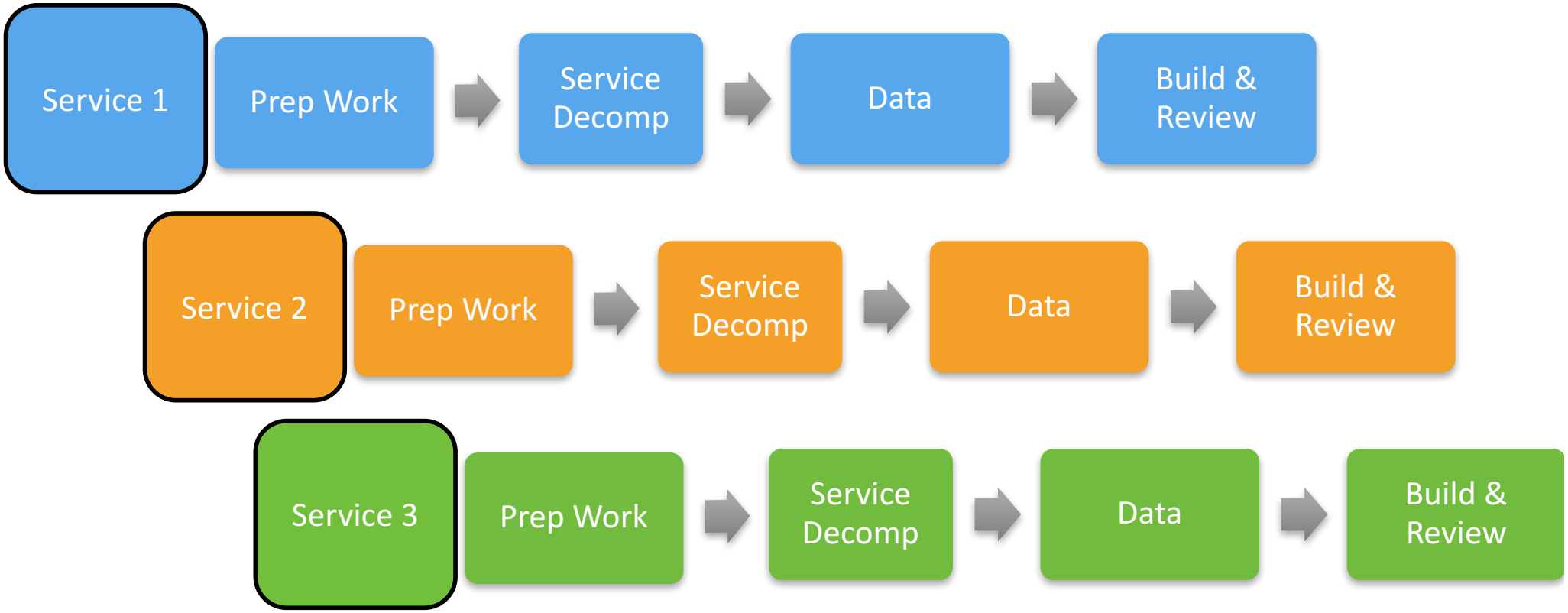


About | Support | File a Bug | Documentation | Privacy Policy

© 2005-2015 Splunk Inc. All rights reserved.

splunk> .conf2016

Deployment Pipeline



splunk> .conf2016

Environment & Data Validation

- Ensure data for KPIs is available
  - Cross reference Initial Kick Off list
    (Sit down with Data Owner)
  - If there are data gaps, identify data owner and onboarding times
    - (Red Tape aka. Process & Change Management)
- ITSI uses real time monitoring
  - (historical datasets or QA data is not adequate/exciting)

Data Challenges

- Customers can usually create CSVs easier and quicker than onboard data
  - Firewall/Account Creation/CAB meetings ….
- You can put CSV/Python onto Searchhead until Data is on-boarded
  - Not a permanent solution but it let's you focus on your core responsibility

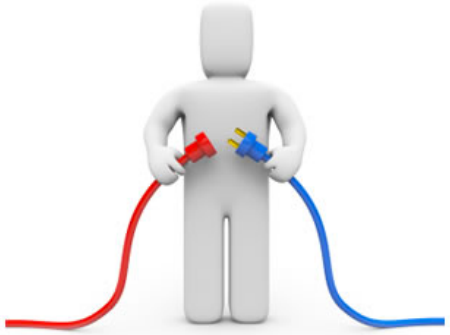
Tips and Tricks

Data Gaps

- Best Practice to show Glass Tables with rich set of information
- Use Glass tables and Deep Dives as selling tool to get new data
  - Get buy in to onboard data
- How can you work around missing data
  - Event Gen
  - Python
  - Random Number Generator
    - |eval randomnbr=random()
      |eval response_time=randomnbr%100

Now the real fun begins

- ITSI Install & Validation
  - Follow Best Practices (e.g. make you have backup)
  - Always go with latest & greatest from splunkbase
    - Remember ITSI is KV store heavy
  - Test Install – create KPI and Glass Table
    - Free tester app https://splunk.box.com/v/ITSI-Tester
- Start Building KPIs
  - Start Collecting Data
- **Rinse & Repeat**
- Don't go for perfection 80/20 rule



Checklist

- ❑ Environment Validation (Version & Capacity)
- ❑ Problem worth solving (Fails Often or has High Visibility)
- ❑ Data (Real time and On-boarded)
- ❑ Flow Diagrams/Agreed Outline
- ❑ Service Decomposition
- ❑ List of KPIs (and SMEs for follow Up)
- ❑ Service Review
- ❑ Incorporate Feedback & Schedule Production Deployment

splunk> .conf2016

Tips and Tricks

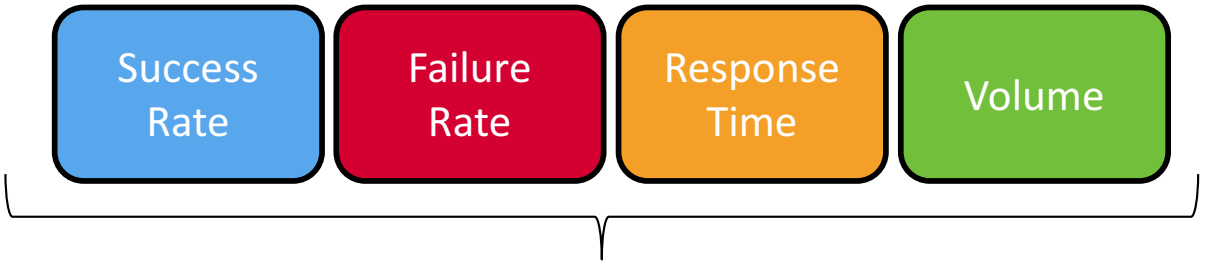
Backup and Migration Strategy

- ITSI Configurations are stored in KV store
  - Services, KPIs, Thresholds, Glass Tables, Deep Dives, Service Analyzers ….
- Exceptions
  - Config files for deep dives and Custom Notable Event Actions
- Perform File System Backup and KV Store Backup
  - http://docs.splunk.com/Documentation/ITSI/2.3.0/Configure/BackupandRestoreITSIconfig
- Partial Restores to Move Services from Dev/Test to Production

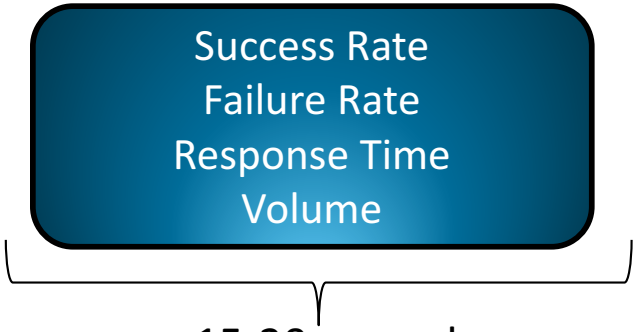
Tips and Tricks

Base Searches

- **BEST PRACTICE TO REDUCE RESOURCE UTILIZATION**
  - Use ANY TIME You can
  - Best Weapon to fight over-utilized Search Heads

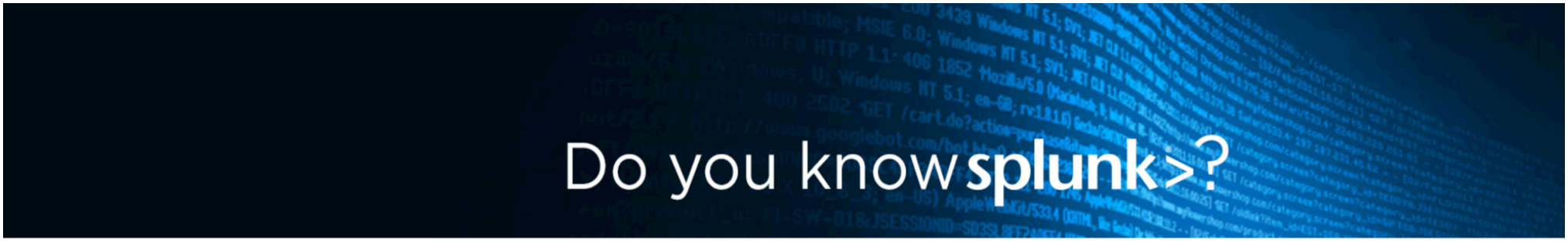


- 40 seconds



- 15-20 seconds

We Can Help You Get Started



UP NEXT

Workshops
Introduction to Splunk Search Party
Date: October 12, 2016
Time: 8:00am - 12:00pm
Click here for details

Introduction to Splunk Enterprise
Date: December 1, 2016
Time: 8:00am - 11:30am
Click here for details

DO YOU KNOW SPLUNK?

Do you know you can use Splunk to mitigate cybersecurity risk? How about to prevent fraud, waste, and abuse? Or did you know Splunk can help you improve the performance and reliability of your mobile apps? Are you aware it can help rapidly explore, analyze, and visualize data in Hadoop? Splunk uses for your organization are limited only by your imagination.

This online series will provide tips and tricks to help you optimize your Splunk environments. Plus, get introduced to new ideas on how Splunk can help increase visibility and intelligence of all your data types regardless of source, location, and device

SPLUNK WORKSHOPS

Experience the Splunk platform firsthand by attending our workshops. Led by Splunk experts, these hands-on workshops will introduce you to Splunk's uses, machine data concepts, and the Splunk user interface.

The workshops are complimentary and seating is limited

WORKSHOP OVERVIEW

These workshops are tailored for beginner users that are new to Splunk and have not used it before.

- October 12: Introduction to Splunk Search Party
- December 1: Introduction to Splunk Enterprise
- December 14: Introduction to Splunk IT Troubleshooting
- January 11: Introduction to Splunk Enterprise Security
- January 25: Introduction to Splunk IT Service Intelligence

WEBCAST REPLAYS

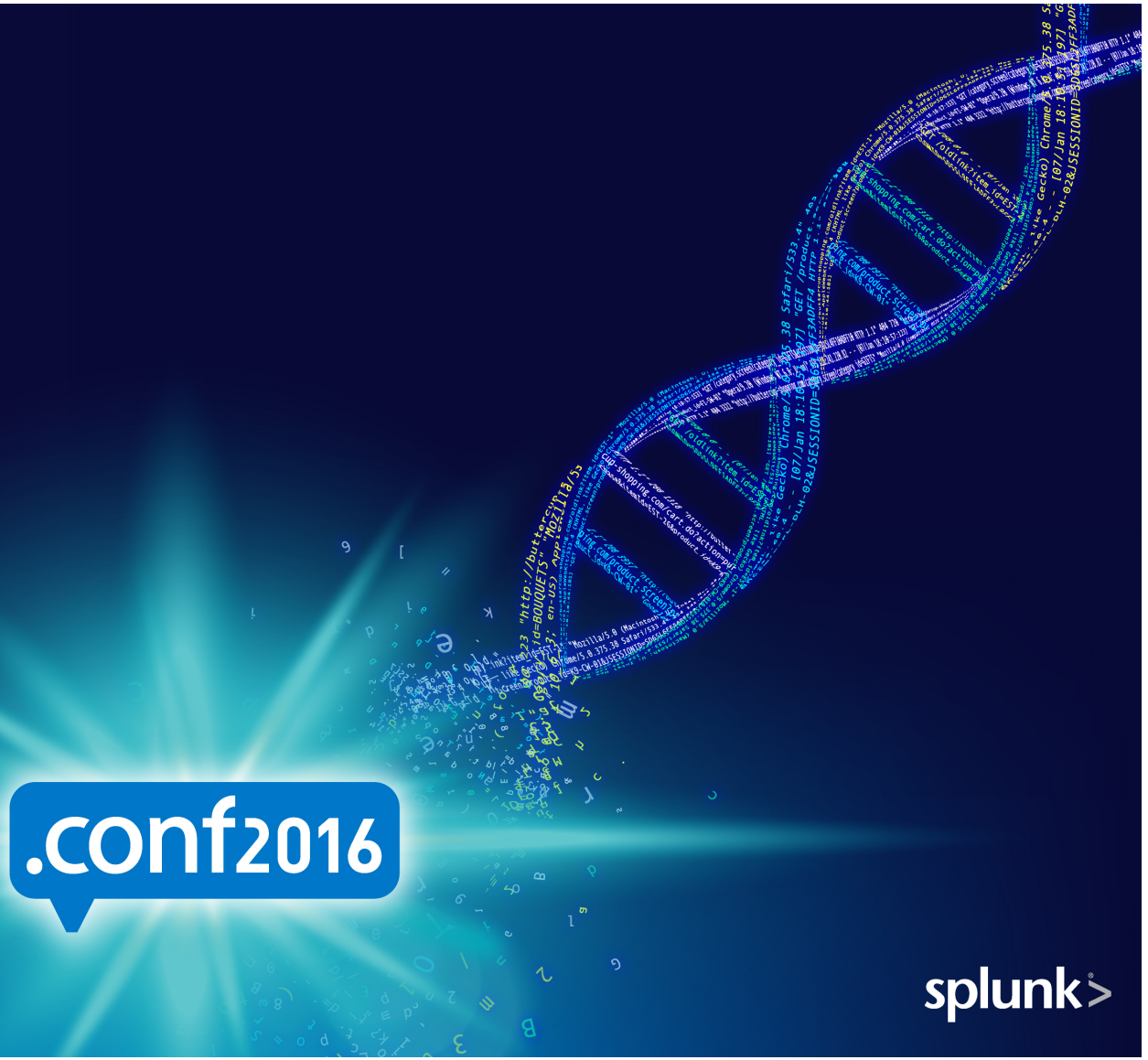
- Splunk for Information Assurance & Government Compliance
- What's New in 6.2?
- The Splunk Way to IT Operations Management

What Now?

Related breakout sessions and activities…

- How Anaplan Used Splunk Cloud and ITSI to Monitor Our Cloud Platform
  TUESDAY 3:15pm - 4:00pm Dolphin E1/2
- Machine Learning and Anomaly Detection in Splunk IT Service Intelligence
  TUESDAY 4:20pm - 5:05pm Dolphin Southern 2
- Modernizing Enterprise Monitoring at the World Bank Group using Splunk IT Service Intelligence
  TUESDAY 5:25pm - 6:10pm - Dolphin Southern 2
- Splunk IT Service Intelligence: Keep your boss and their bosses informed and happy (and still sleep at night)!
  THURSDAY 2:35pm - 3:20pm Dolphin Southern 1

THANK YOU



.conf2016

splunk>