splunk> .conf2017

Managing Splunk As An Internal Service At MITRE

Expanding and Demonstrating the Value of Splunk

Bob Clasen | MITRE Corporate IT Splunk Service Manager

September 2017 | Washington, DC

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> .conf2017

Overview

- **Background**
- **Getting started**
- **Adding value**
- **Demonstrating value**
- **Next steps**

Managing Splunk as an Internal Service at MITRE

Expanding and Demonstrating the Value of Splunk

The MITRE Corporation

part of the ecosystem of federal research centers

established in **1958**
to serve the public interest

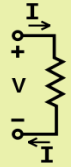
not-for-profit

science & tech support to federal government

~8,000 employees

Speaker Info

- **My background**
  - Computer/electrical engineer
  - Retired US Air Force
  - At MITRE for 14 years
    - Past 8 years working MITRE corporate IT
- **Current roles**
  - Team lead
    - Enterprise systems monitoring
    - Performance & automated functional testing
  - Corporate IT Splunk service manager
    - Been Splunking for ~2.5 years

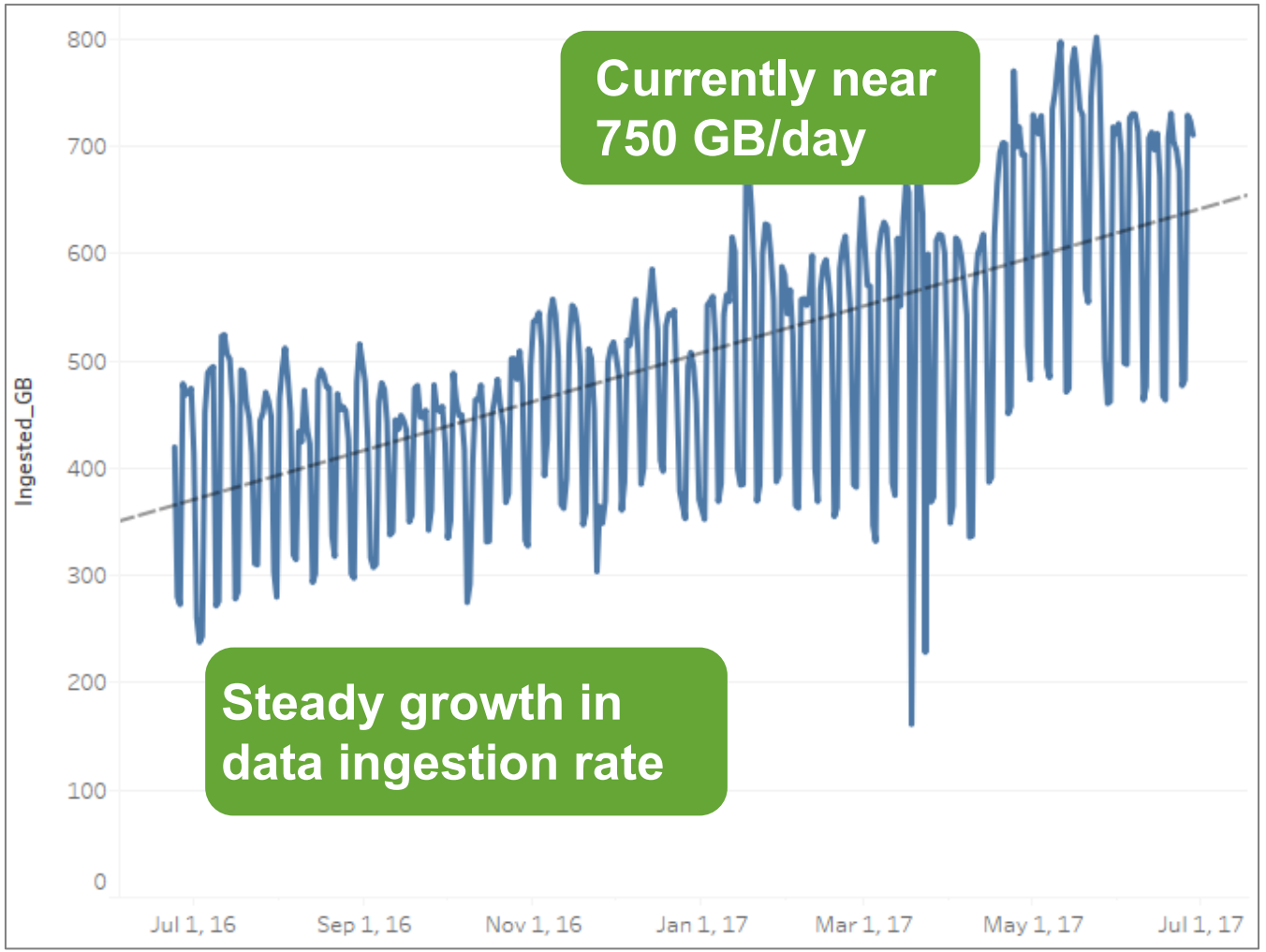


Ohm's law V = I * R

splunk> .conf2017

Background

- **MITRE internal IT**
- **Splunk usage started small**
  - Initial focus cyber-security
  - Handful of ninjas
- **Over time, more data ingested**
  - Cyber folks really happy
- **However, cost of Splunk rose**



splunk> .conf2017

Background (cont.)

- **Only a few teams were using Splunk**
  - Not really leveraging data already there
- **So, Splunk's value wasn't increasing much even though cost was rising**
  - Management wanted to see more ROI
- **This is the story of how we:**
  - Implemented service management
  - Broadened Splunk's usage
  - Demonstrated increased value of Splunk

Getting Started

Service Catalog

- **Initial observations**
  - Wasn't clear what services were available
- **So, we created a services catalog**
  - Splunk service offerings
  - How to request
  - Typical time needed to fulfill
  - Cost
  - Points of contact

Service Offerings

- Account and data access

- Ingest new data source into Splunk
- Searches, reports, dashboards, etc.

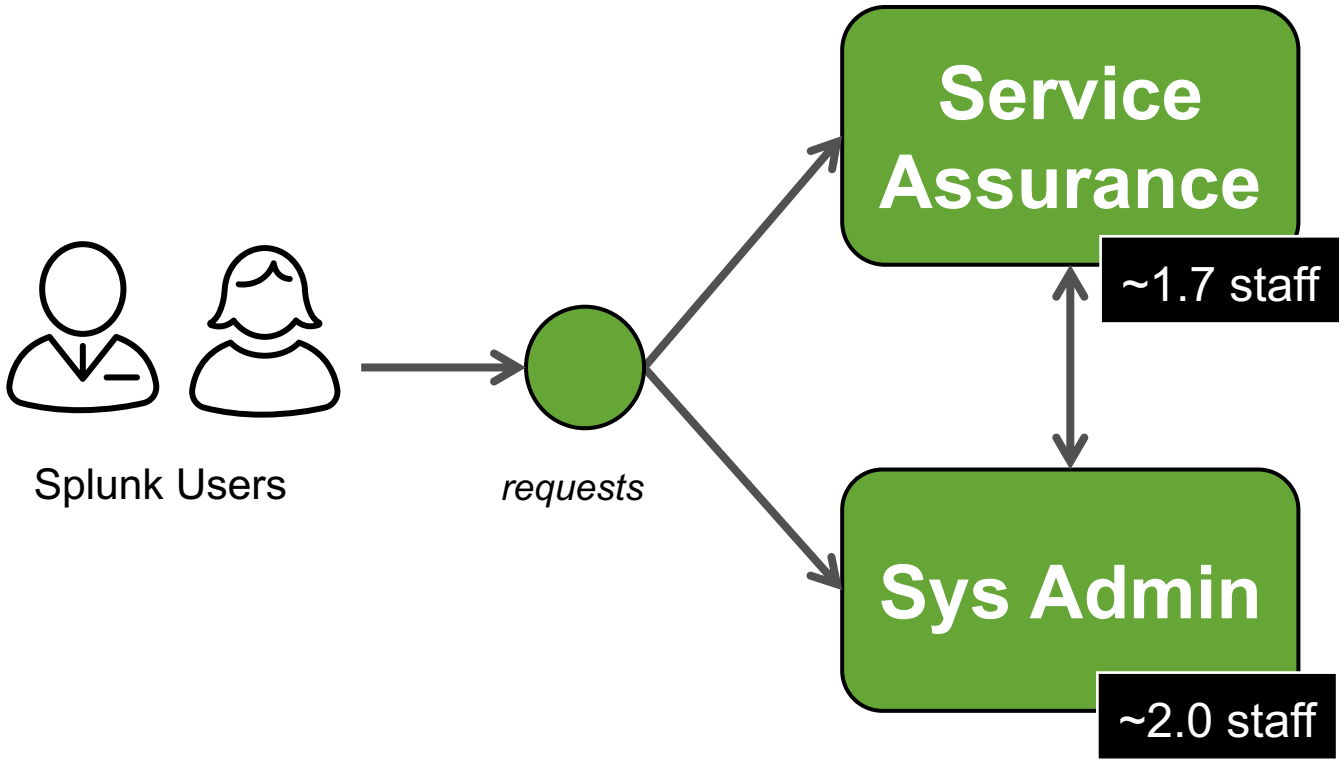
- Alerting

- Other services

splunk> .conf2017

Getting Started (cont.)

Define Team Roles



- Overall service management
- Customer engagement
- Fulfill service requests
  - Reports, dashboards, compliance, alerts, etc.
- Budget - licenses

- Server/app admin
- System architecture
- Fulfill service requests
  - Accounts, access, data ingestion, etc.
- Budget – servers, storage, etc.

Getting Started (cont.)

- Started thinking about how to increase Splunk's value

Three Approaches To Increase Splunk's Value

1

Enable more users

2

Expand beyond self-service

3

Expand use cases

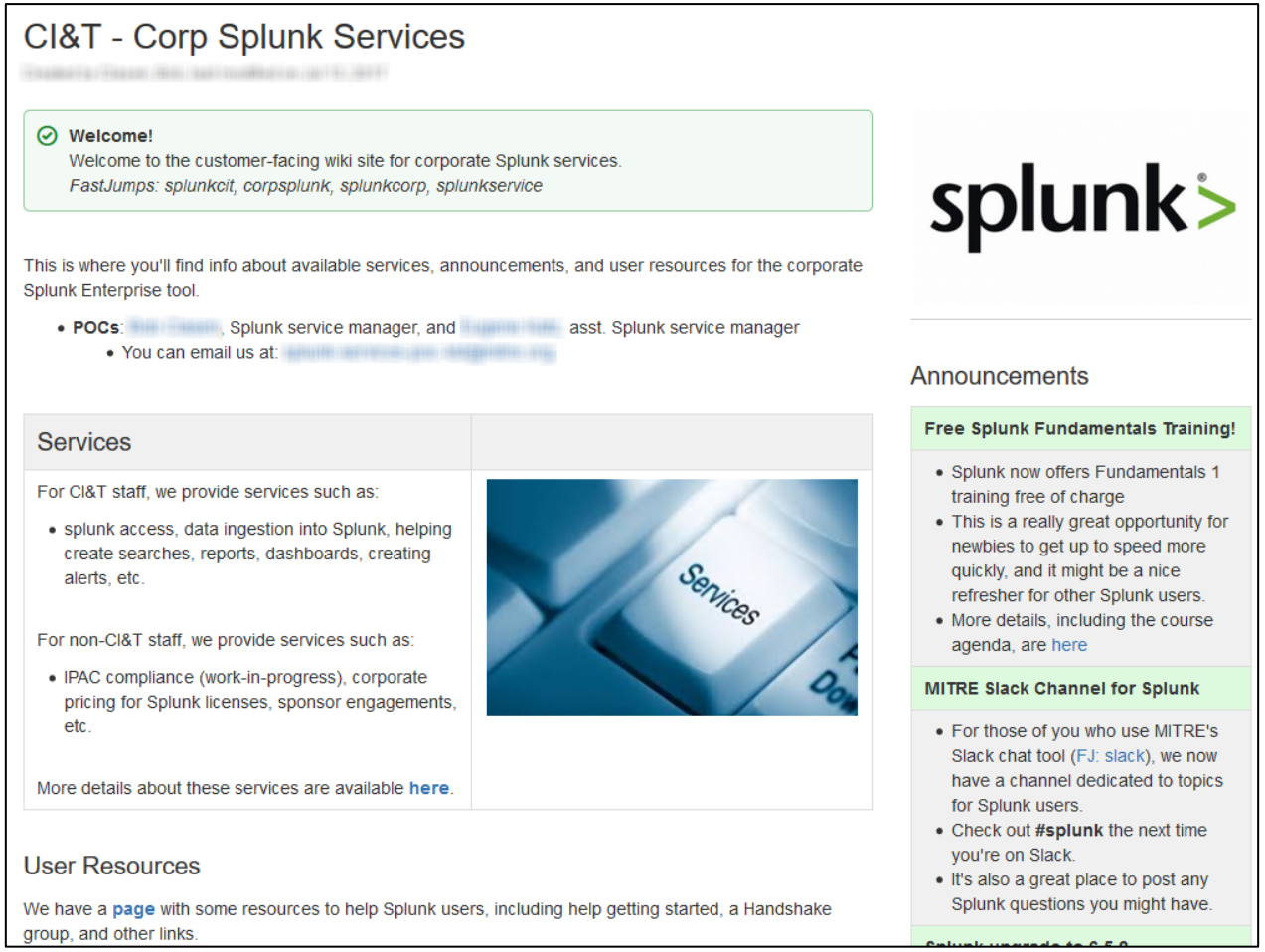
splunk> .conf2017

1 *Increase Value*

Enable More Users

- **Made it easier to get info about services**
  - Created a wiki page
    - Service catalog
    - Announcements
    - User resources
    - POCs for more info

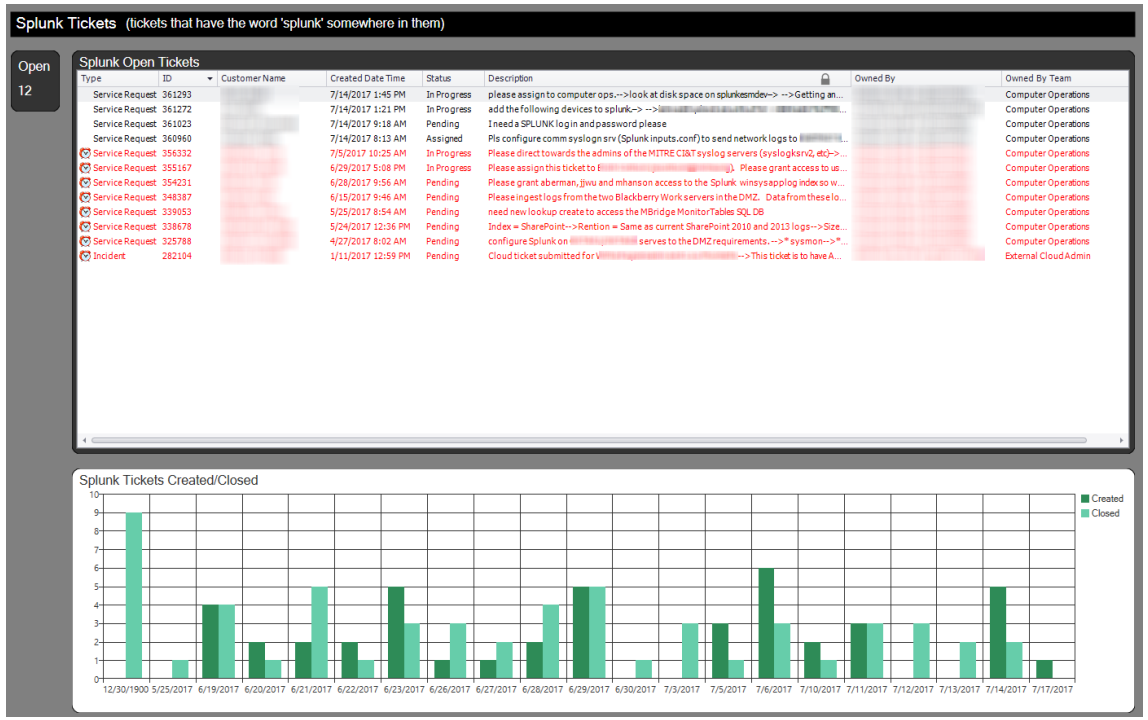
One-stop shop for Splunk info



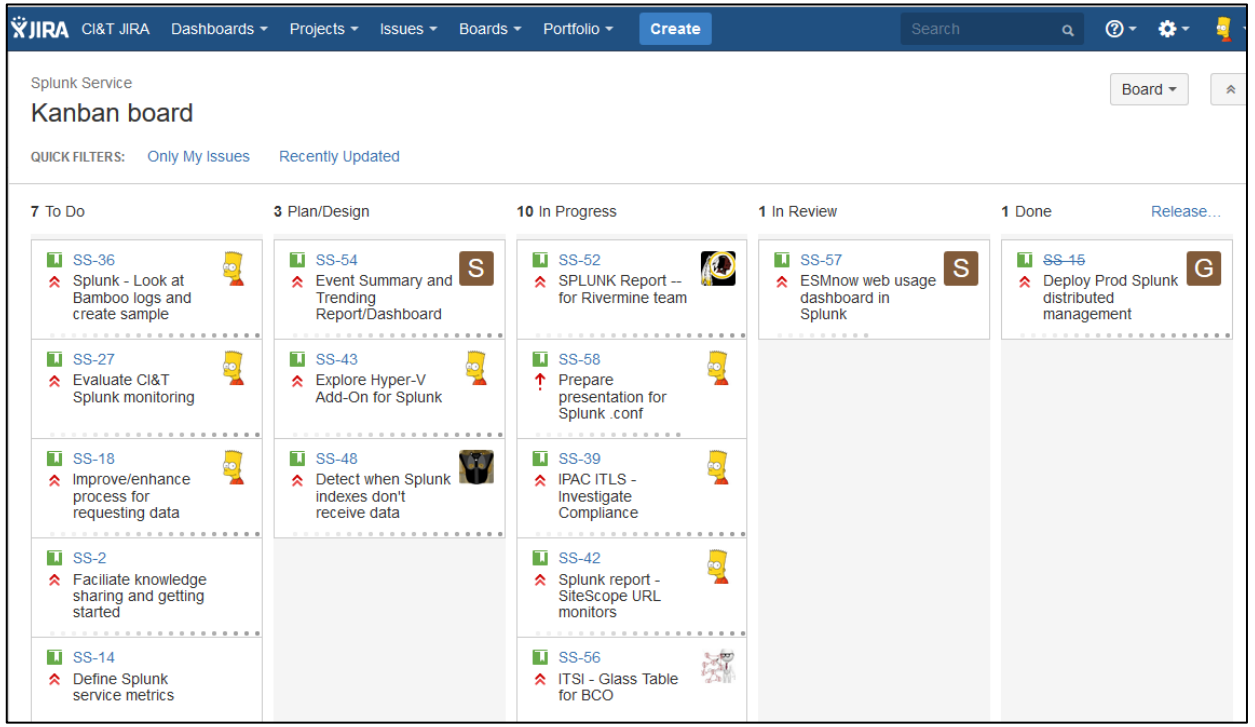
1 *Increase Value*

Enable More Users (cont.)

- **Tracked request fulfillment to ensure good customer service**



ITSM tickets (Cherwell)



Kanban cards (JIRA)

1 *Increase Value*

Enable More Users (cont.)

- **Provided info, training, knowledge sharing, etc.**
  - Initially, we weren't staffed to help folks get their data out of Splunk
    - Users had to figure out their own searches, reports, etc.
  - So, we tried to help
    - Brown bags
    - Splunk overview meetings targeted to specific teams
    - Technical exchange meetings
    - Message boards and chat channels
    - Splunk workshops and user groups
    - Pointers to Splunk tutorials, training, videos, etc.

Note:
Work with your Splunk reps for more ideas about helping your users

1 *Increase Value*

Enable More Users (cont.)

- **Created data governance model**
  - Make data more widely available
    - Facilitate analysis across silos
  - Also need to safeguard data
    - Define sensitive info and limit access
  - Free the data! (and protect it, too!)
- **Created data catalog**
  - Visibility about data already in Splunk

2 *Increase Value*

Expand Beyond Self-Service

- **Great to foster self-service…**
  - But, some folks don't have time and/or skillset
    - Learn SPL, etc.
- **We found more resources to help**
  - Adjusted monitoring team work program
    - They were using Splunk for monitoring
    - Made them available to help others
  - Created new full-time position for Splunk reporting
    - Primary focus on compliance
    - Also available for general Splunk help

2 *Increase Value*

Expand Beyond Self-Service (cont.)

- **As a result, we now offer new services**
  - Searches, reports, dashboards, etc.
  - Some users just need a jump start
    - They can take it from there
  - Others just want the reports to appear
    - Don't care how they get there
- **Market these services to teams**
  - Show them value of Splunk
  - Then, help them get started

Current Service Offerings

- Account and data access
- Ingest new data source into Splunk

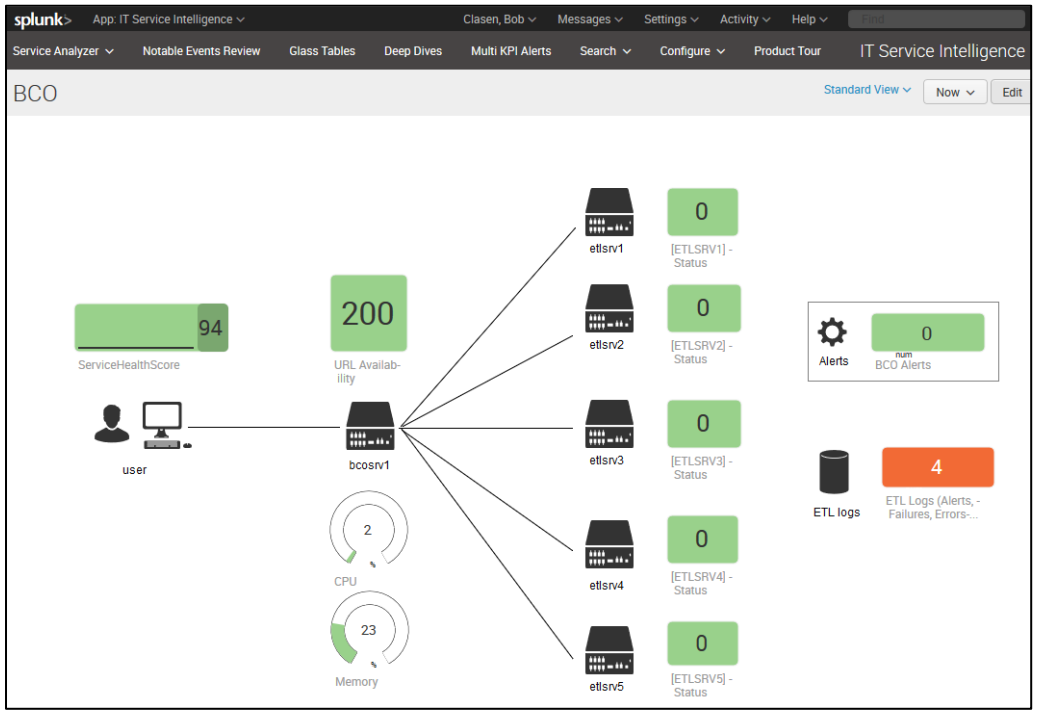
NEW

- Searches, reports, dashboards, etc.
- Alerting
- Other services

3 *Increase Value*

Expand Use Cases

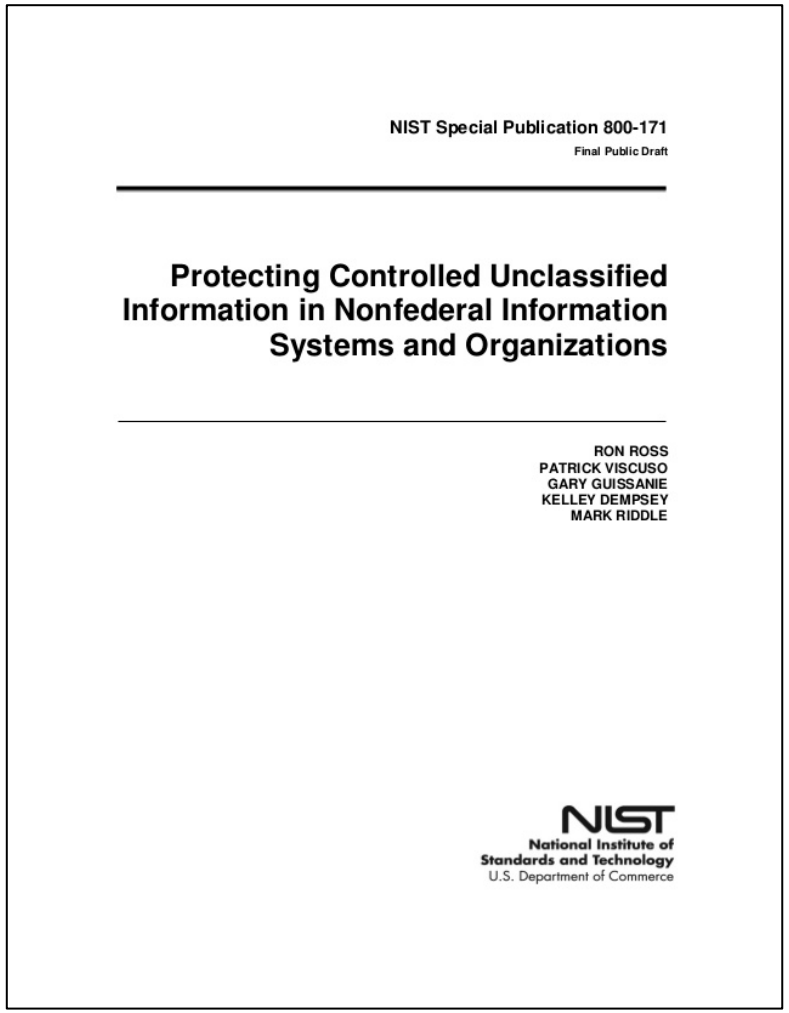
- **Initially just enterprise security use case**
- **Added IT Operations use cases**
  - Dashboards to provide better awareness of:
    - Health of WAN circuits, application availability, etc.
  - Worked with dev teams to ingest app logs
    - No need for RDP/SSH to access logs
  - Started using IT Service Intelligence app
    - Better awareness and faster root-cause analysis
    - Still new to us



splunk> .conf2017

3 *Increase Value*

Expand Use Cases (cont.)


NIST Special Publication 800-171
Final Public Draft

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- **Adding compliance use case**
  - Defense Federal Acquisition Regulation Supplement (DFARS)
    - NIST 800-171
  - MITRE must comply with DFARS by Dec 2017
    - Dept of Defense contracts
  - Will use Splunk for compliance reporting
    - Just getting started with this

Measuring And Showing Value

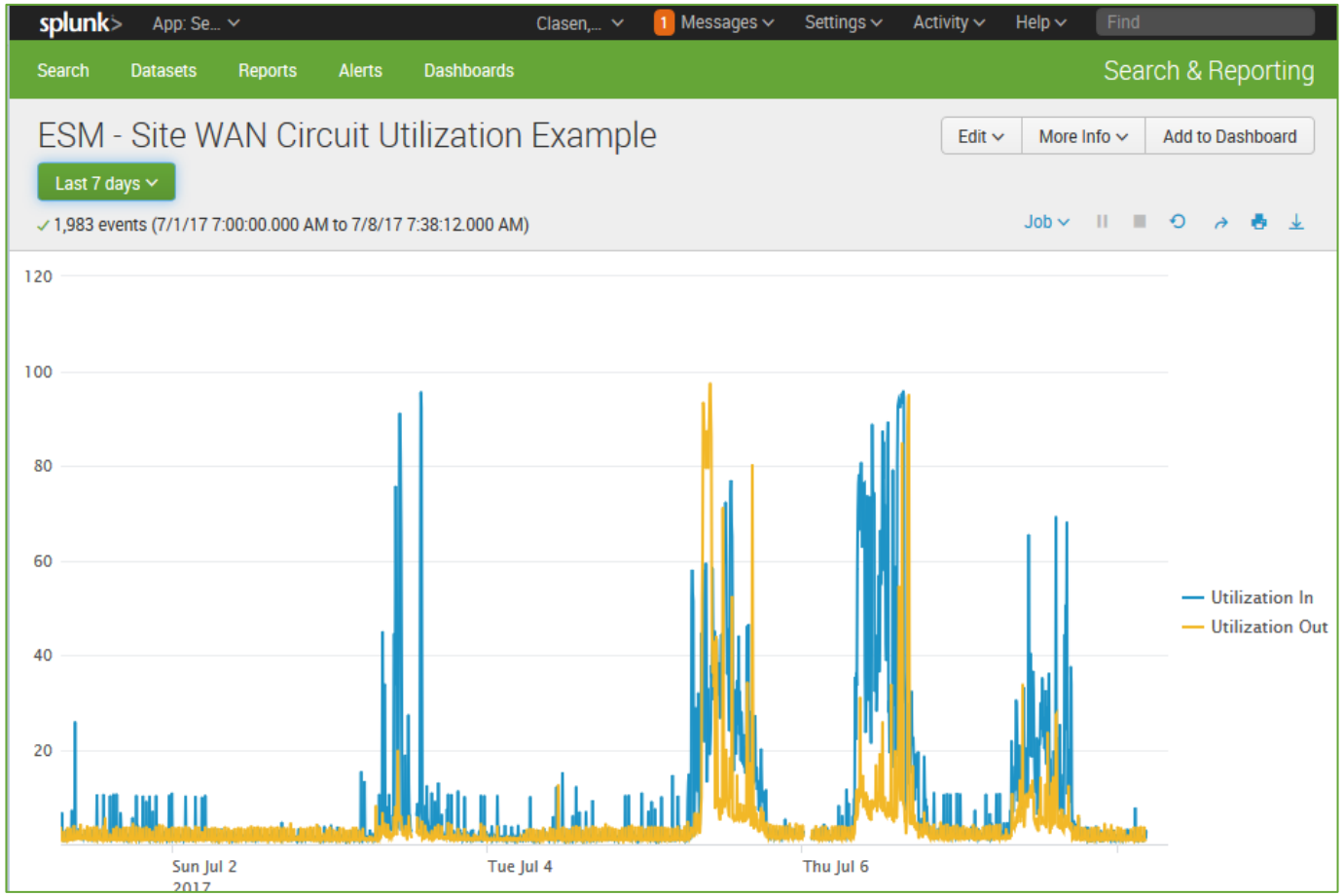
- **With not-for-profits like us, it can be tough to show value/ROI numerically**
  - Lost sales, abandoned shopping carts, etc. aren't applicable
- **However, we've used the following to show Splunk's value:**

1. **Replace other tools with Splunk**
2. **Show example dashboards to demonstrate value**
3. **Manage cost**
4. **Explore use of metrics**

1 *Show Value*

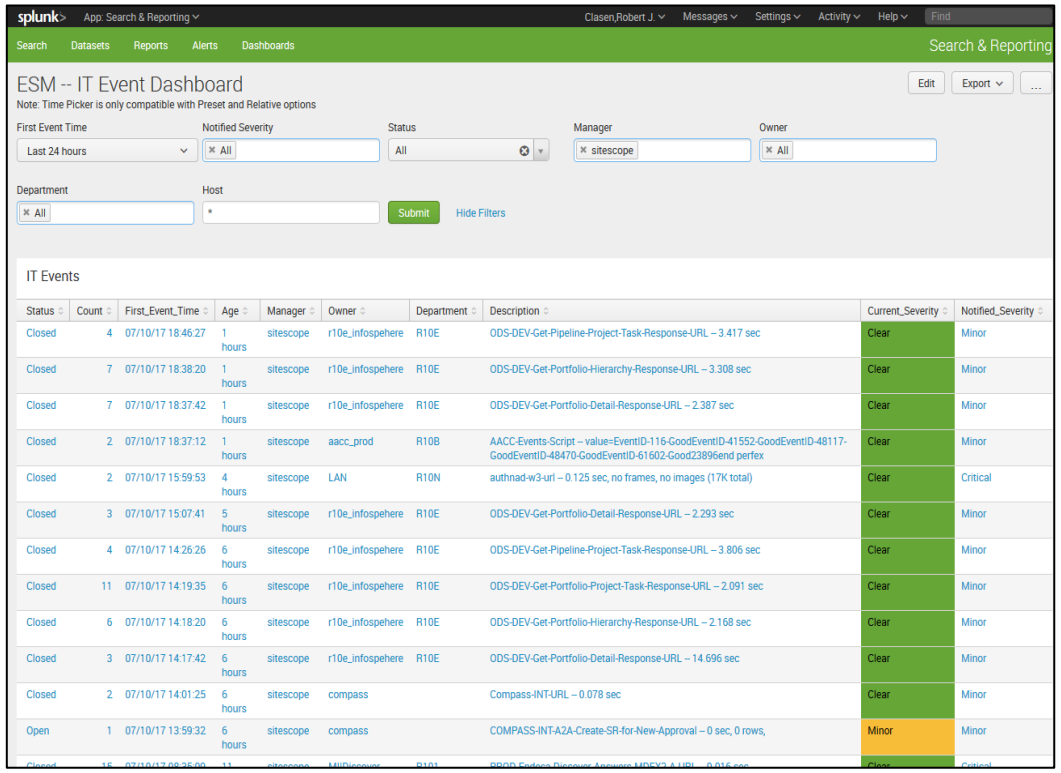
Replace Other Tools With Splunk

- **Retired two tools and now use Splunk instead**
  - Visualization of historic network monitoring data
  - Web analytics
- **Can quantify money saved**



2 *Show Value*

Find Examples To Demonstrate Value



IT Event Dashboard

- **Show example reports/dashboards that demonstrate value**
  - "Advertise" these to users, teams, management
  - Show concrete examples of how Splunk can:
    - Save time
    - Provide better situational awareness
    - Faster root-cause analysis
    - Provide business value by:
      - Reducing downtime (faster time to recovery)
      - Ideally, prevent downtime by enabling proactive actions

splunk> .conf2017

3 *Show Value*

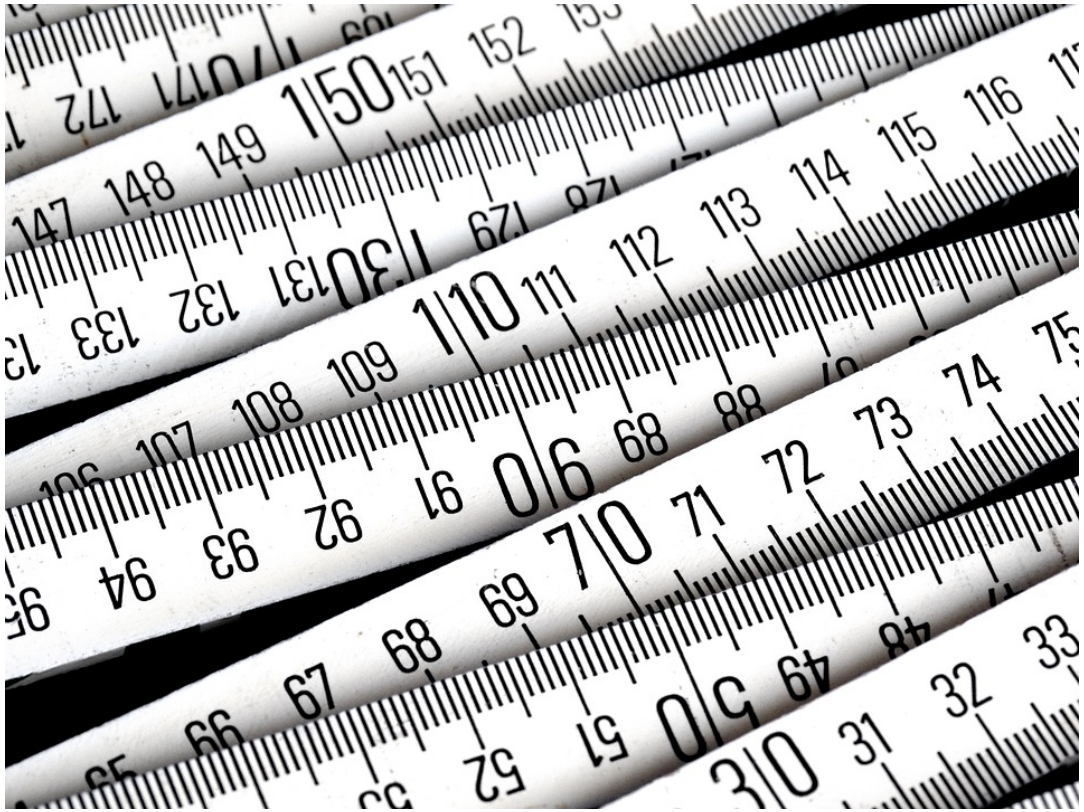
Manage Cost

- **By managing cost effectively, you improve ROI**
  - Get same value while reducing cost
- **Primary cost of Splunk due to licenses**
  - Manage license growth
    - Data lifecycle management
    - Track indexes that suddenly grow in size
- **Other cost areas for Splunk**
  - Personnel
    - Make manual processes more efficient
    - Automate where possible

4 *Show Value*

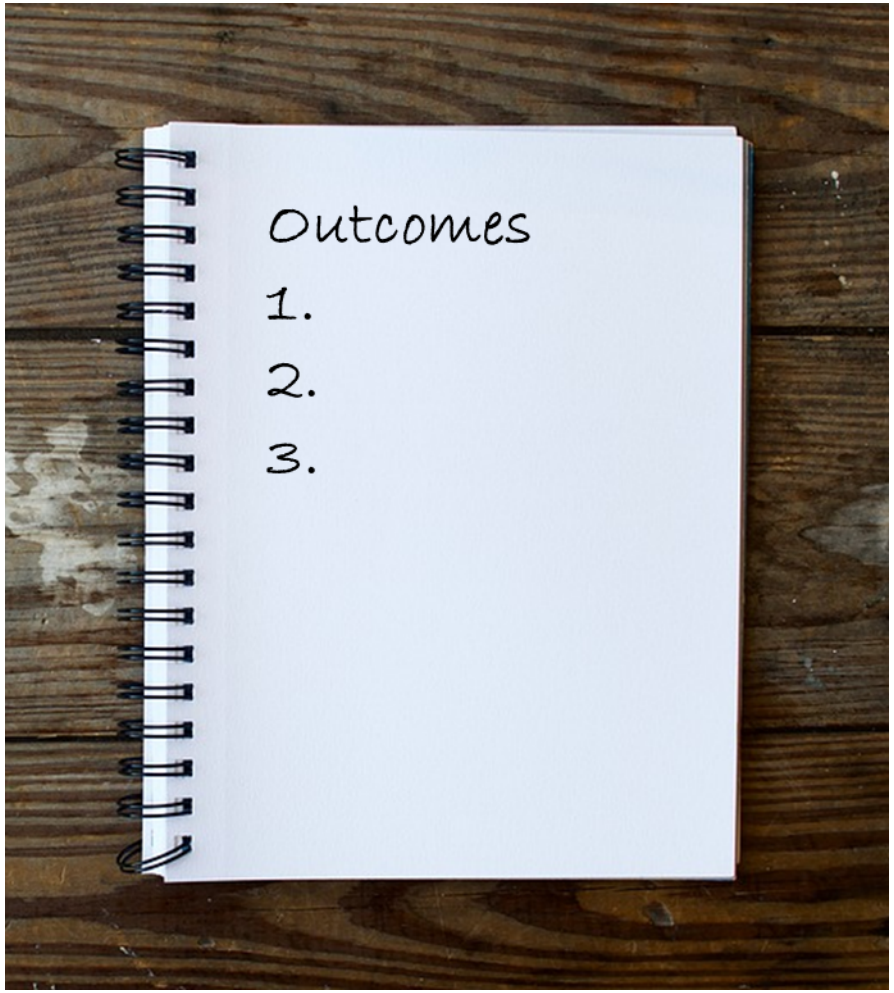
Explore Use Of Metrics

- **Of course, numbers can lie, but they can also be useful**
- **We're looking at quantitative metrics:**
  - Amount of data being ingested
  - Number of:
    - Users
    - Searches/reports
    - Service requests
  - Service/application availability
- **Still a work-in-progress**

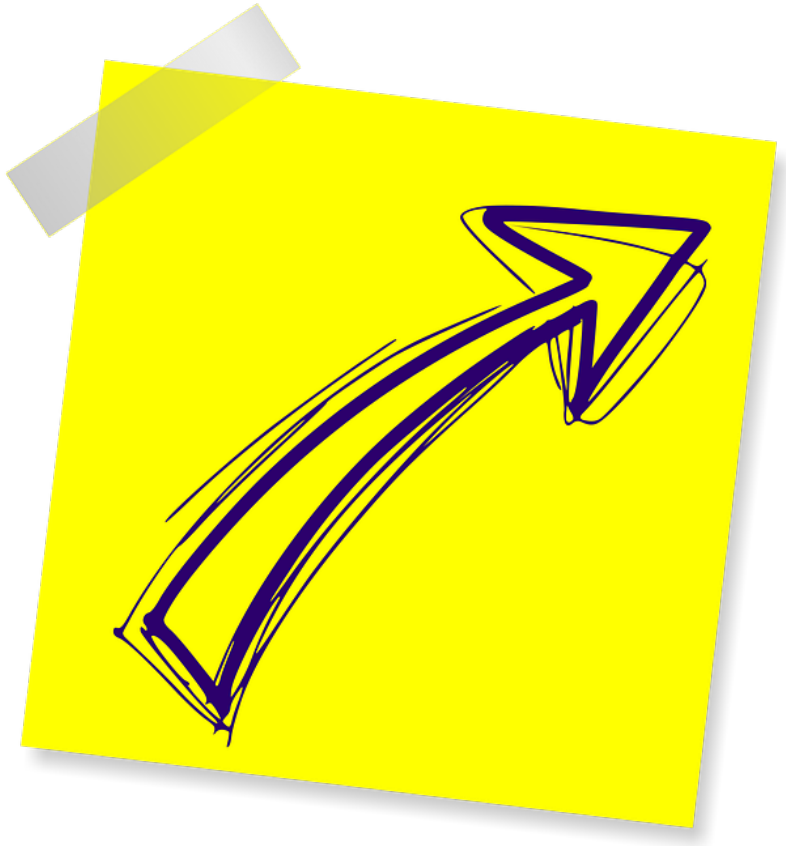


Results

- **Increased value of Splunk at MITRE**
  - More people use it for more use cases
    - Solve issues faster
    - Prevent some issues from occurring
    - Improve availability of business services
- **Demonstrated value**
  - Qualitative and quantitative
  - Show ROI to managers and peers



Next Steps



- **Continue works-in-progress**
  - Metrics
  - Expanding IT Ops use cases
  - Compliance use case
- **Enhance monitoring of Splunk health**
  - As more folks rely on Splunk, it needs to be available
- **Explore other Splunk use cases**
  - App delivery (DevOps)
  - Business analytics

Let's Continue The Conversation

- **Would be glad to talk more about…**
  - What we've done so far and our plans
  - What you've done
- **Let's chat**
  - During conference breaks
  - After the conference
    - Email: rclasen@mitre.org

Deutsche Fotothek [CC BY-SA 3.0 de (http://creativecommons.org/licenses/by-sa/3.0/de/deed.en)], via Wikimedia Commons

splunk> .conf2017

Thank You

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