



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, 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.

Managing Splunk as an Internal Service at MITRE

Expanding and Demonstrating the Value of Splunk



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

The MITRE Corporation



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

not-for-profit

science & tech support to
federal government

~8,000 employees

part of the ecosystem of federal research centers

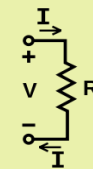
Speaker Info

► My background

- Computer/electrical engineer
- Retired US Air Force
- At MITRE for 14 years
 - Past 8 years working MITRE corporate IT

► Current roles

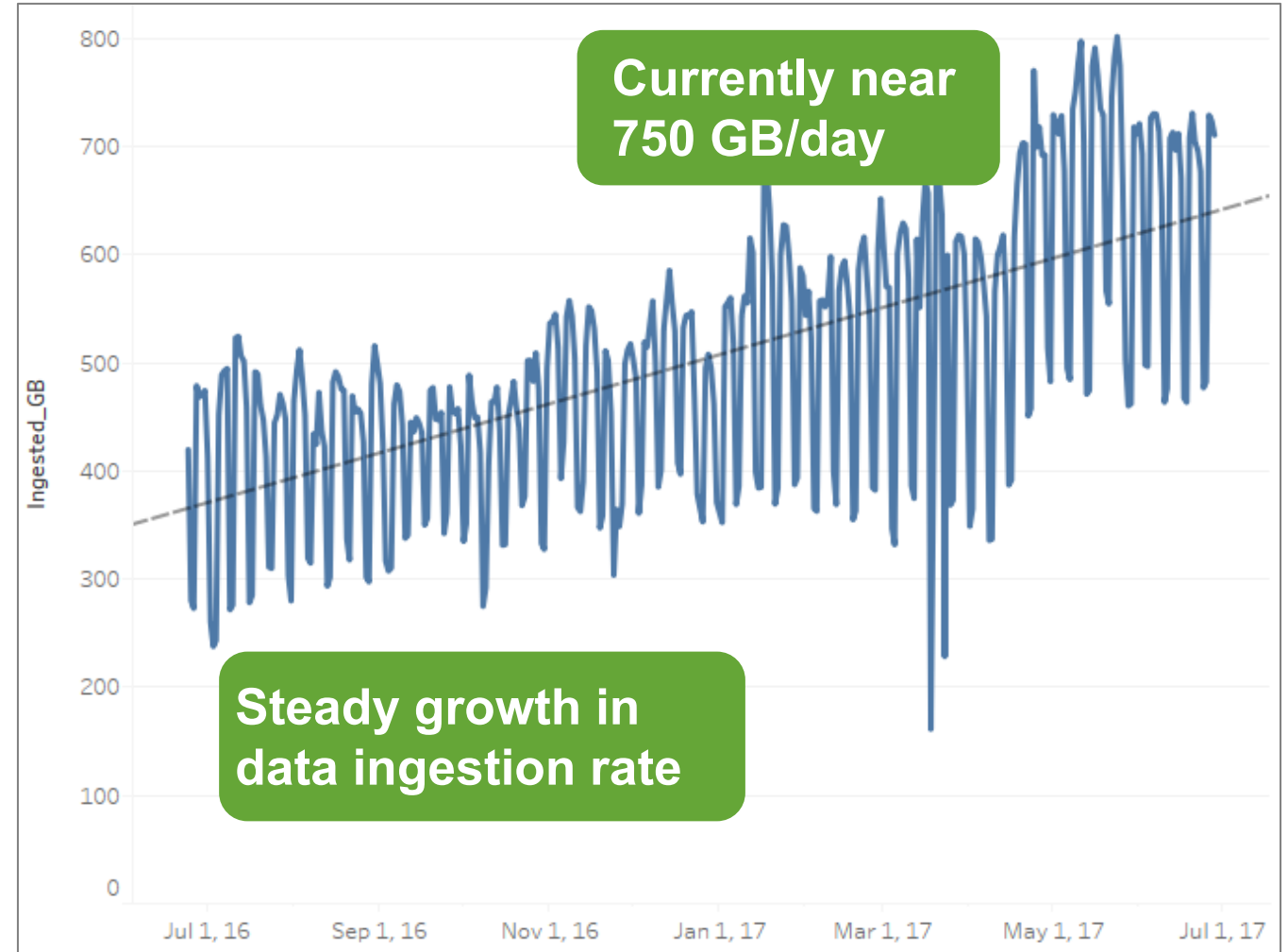
- Team lead
 - Enterprise systems monitoring
 - Performance & automated functional testing
- Corporate IT Splunk service manager
 - Been Splunking for ~2.5 years



Ohm's law $V = I * R$

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**



```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLAFF10ADFF10"
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.14 "screen?category_id=FLOWERS&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
action=purchase&itemId=EST-26&product_id=F1-SW-03" 468 125.17 14.14 "screen?category_id=FLOWERS&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
```

A 3D illustration of a white, stylized human figure with a backpack, climbing a series of orange blocks of increasing height. The figure is positioned on the fourth block from the left, looking up and reaching towards the top of the fifth block. The blocks are arranged in a row, with each subsequent block being taller than the previous one, creating a staircase effect. The background is plain white.

- 

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

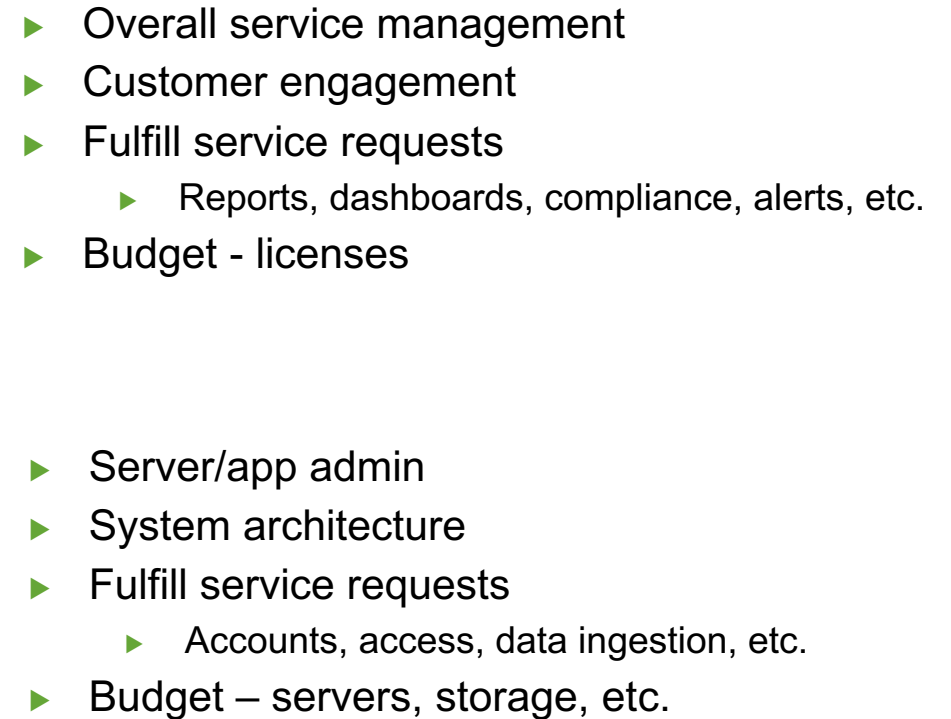


- Searches, reports, dashboards, etc.



- Alerting
- Other services

Define Team Roles



- ▶ **Started thinking about how to increase Splunk's value**





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

CI&T - Corp Splunk Services

Created: 1/10/2017 10:57:13 AM

Welcome!
Welcome to the customer-facing wiki site for corporate Splunk services.
FastJumps: splunkcit, corpsplunk, splunkcorp, splunkservice

This is where you'll find info about available services, announcements, and user resources for the corporate Splunk Enterprise tool.

- POCs:** [Splunk service manager](#), and [Splunk service manager](#) asst. Splunk service manager
- You can email us at: [splunk-service@splunk.com](#)

Services

For CI&T staff, we provide services such as:

- splunk access, data ingestion into Splunk, helping create searches, reports, dashboards, creating alerts, etc.

For non-CI&T staff, we provide services such as:

- IPAC compliance (work-in-progress), corporate pricing for Splunk licenses, sponsor engagements, etc.

More details about these services are available [here](#).

User Resources

We have a [page](#) with some resources to help Splunk users, including help getting started, a Handshake group, and other links

Announcements

Free Splunk Fundamentals Training!

- Splunk now offers Fundamentals 1 training free of charge
- This is a really great opportunity for newbies to get up to speed more quickly, and it might be a nice refresher for other Splunk users.
- More details, including the course agenda, are [here](#)

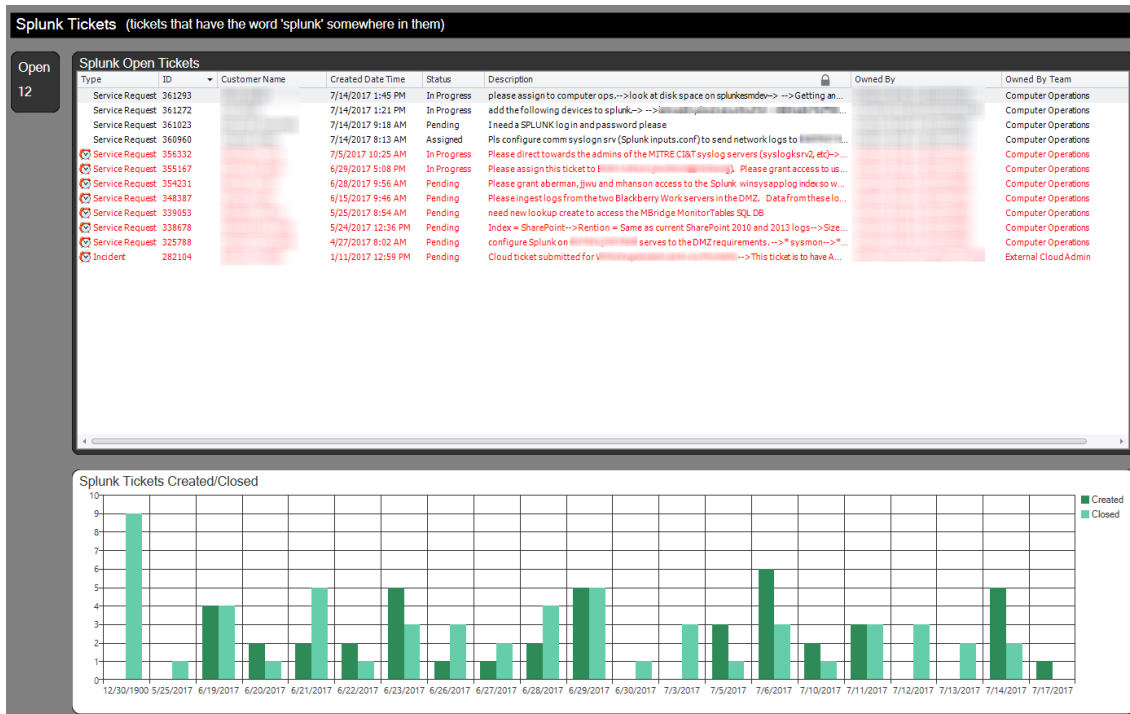
MITRE Slack Channel for Splunk

- For those of you who use MITRE's Slack chat tool ([FJ: slack](#)), we now have a channel dedicated to topics for Splunk users.
- Check out [#splunk](#) the next time you're on Slack.
- It's also a great place to post any Splunk questions you might have.

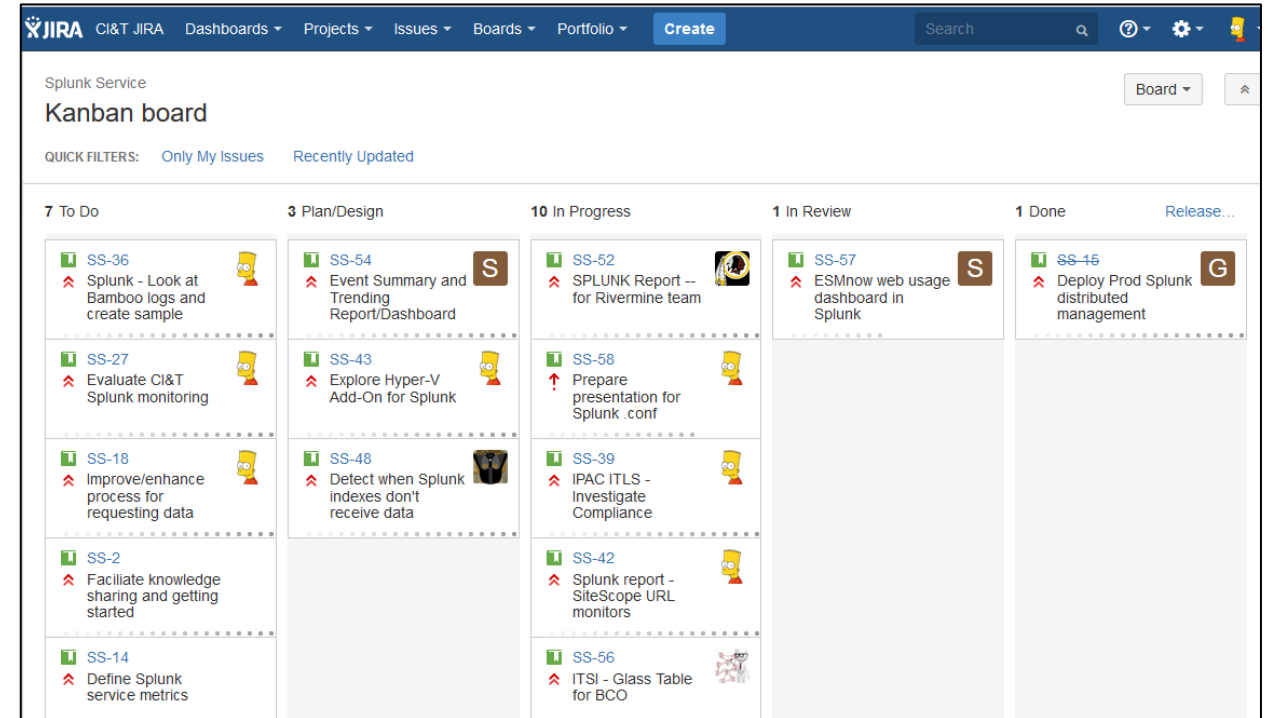
1 Increase Value

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

- 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!)

- Visibility about data already in Splunk

► **Great to foster self-service...**

- **We found more resources to 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

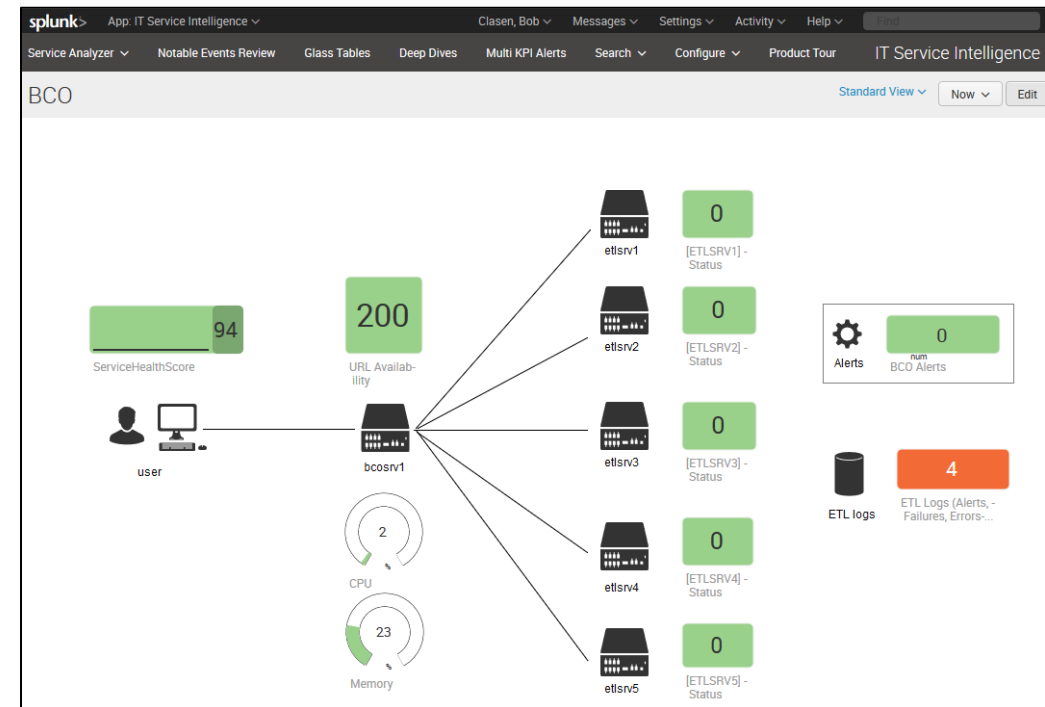
3 Increase Value

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



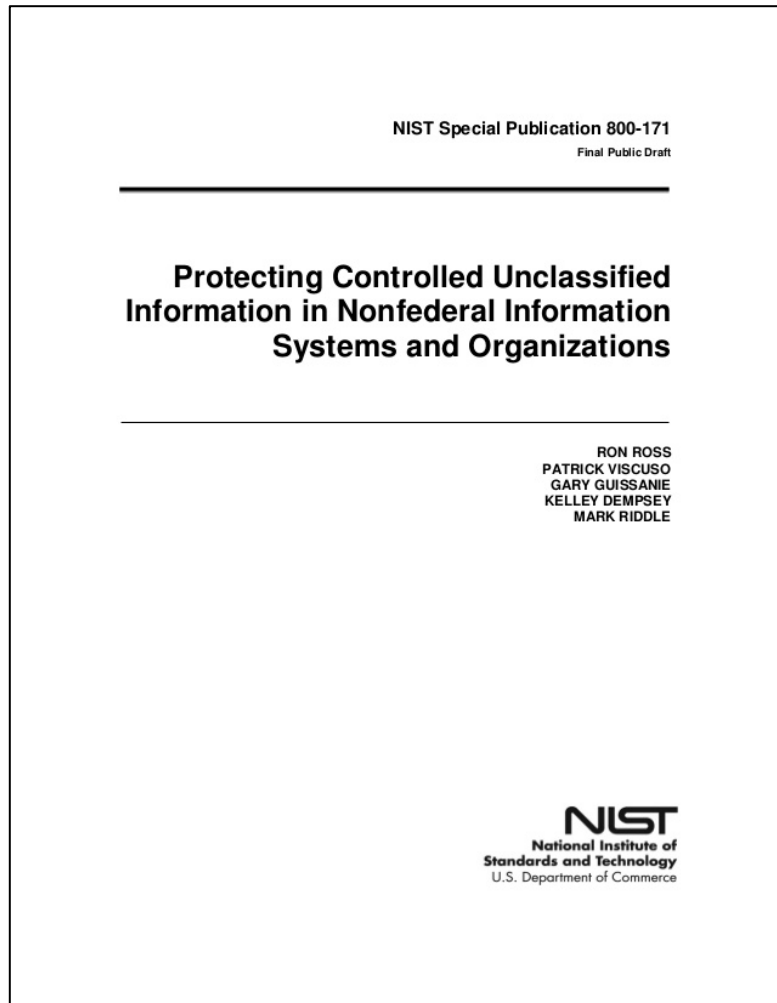
3

Increase
Value

Expand Use Cases (cont.)

► 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

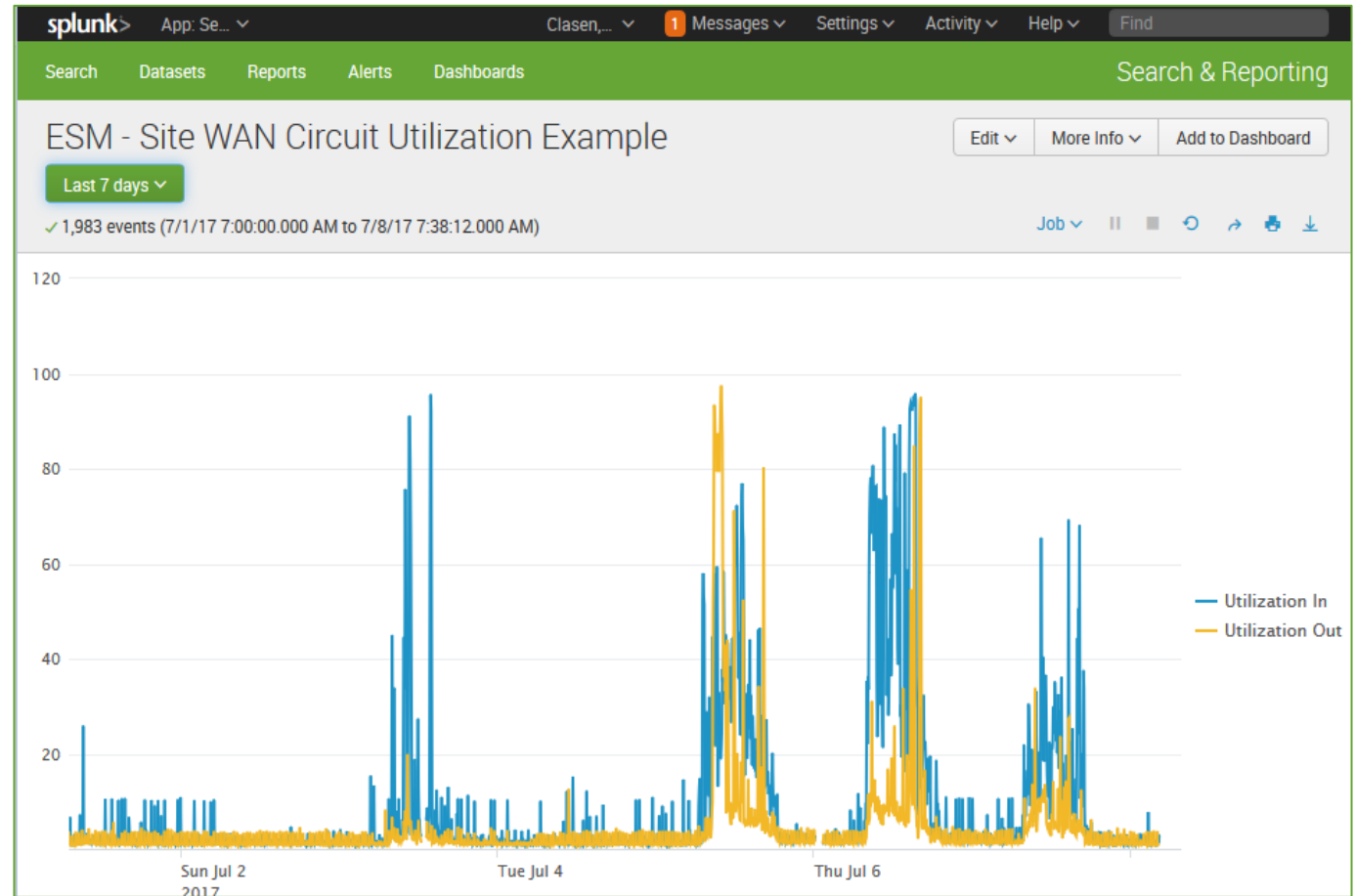
1 Show Value

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

splunk> App: Search & Reporting Clasen,Robert J. Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

ESM -- IT Event Dashboard

Note: Time Picker is only compatible with Preset and Relative options

First Event Time: Last 24 hours x All

Notified Severity: All

Status: All

Manager: x sitescope

Owner: x All

Department: x All

Host: *

Submit Hide Filters

IT Events

Status	Count	First_Event_Time	Age	Manager	Owner	Department	Description	Current_Severity	Notified_Severity
Closed	4	07/10/17 18:46:27	1 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Pipeline-Project-Task-Response-URL - 3.417 sec	Clear	Minor
Closed	7	07/10/17 18:38:20	1 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Portfolio-Hierarchy-Response-URL - 3.308 sec	Clear	Minor
Closed	7	07/10/17 18:37:42	1 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Portfolio-Detail-Response-URL - 2.387 sec	Clear	Minor
Closed	2	07/10/17 18:37:12	1 hours	sitescope	aacc_prod	R10B	AACC-Events-Script - value=EventID-116-GoodEventID-41552-GoodEventID-48117-GoodEventID-48470-GoodEventID-61602-Good23896end perfix	Clear	Minor
Closed	2	07/10/17 15:59:53	4 hours	sitescope	LAN	R10N	authnad-w3-url - 0.125 sec, no frames, no images (17K total)	Clear	Critical
Closed	3	07/10/17 15:07:41	5 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Portfolio-Detail-Response-URL - 2.293 sec	Clear	Minor
Closed	4	07/10/17 14:26:26	6 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Pipeline-Project-Task-Response-URL - 3.806 sec	Clear	Minor
Closed	11	07/10/17 14:19:35	6 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Portfolio-Project-Task-Response-URL - 2.091 sec	Clear	Minor
Closed	6	07/10/17 14:18:20	6 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Portfolio-Hierarchy-Response-URL - 2.168 sec	Clear	Minor
Closed	3	07/10/17 14:17:42	6 hours	sitescope	r10e_infosphere	R10E	ODS-DEV-Get-Portfolio-Detail-Response-URL - 14.696 sec	Clear	Minor
Closed	2	07/10/17 14:01:25	6 hours	sitescope	compass		Compass-INT-URL - 0.078 sec	Clear	Minor
Open	1	07/10/17 13:59:32	6 hours	sitescope	compass		COMPASS-INT-AZA-Create-SR-for-New-Approval - 0 sec, 0 rows,	Minor	Minor

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

► **By managing cost effectively, you improve ROI**

- **Primary cost of Splunk due to licenses**

- ## ► Other cost areas for Splunk

- Personnel
 - Make manual processes more efficient
 - Automate where possible

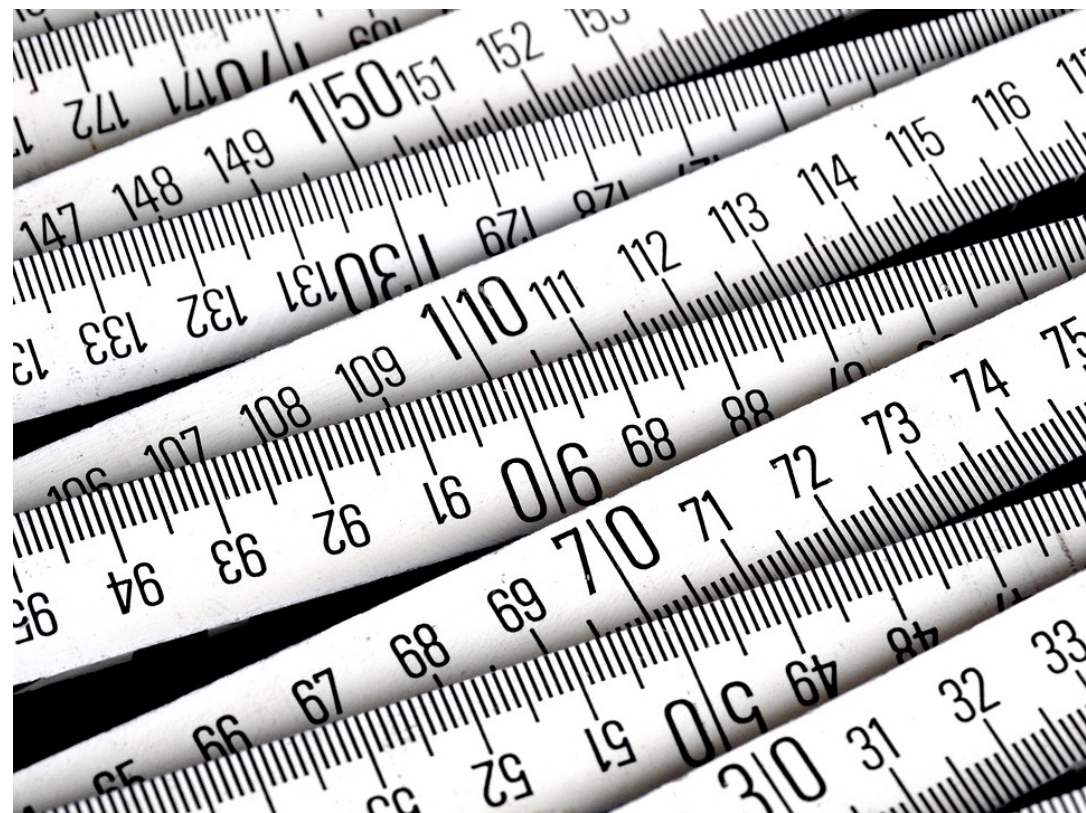


4

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



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Opera/9.80 (Win
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=CB-01" "Mozilla/4.0 (Compaq i
ows NT 5.1; SV1; - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=CB-01" "Mozilla/4.0 (Compaq i
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=CB-01" "Mozilla/4.0 (Compaq i
action=purchase&itemId=EST-26&product_id=CB-01" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=CB-01" "Mozilla/4.0 (Compaq i
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=CB-01" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=CB-01" "Mozilla/4.0 (Compaq i

► Increased value of Splunk at MITRE

- **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

Thank You

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

splunk> .conf2017