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

Approved for Public Release; Distribution Unlimited. Case Number 17-2507.

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.

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

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

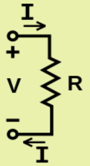
Speaker Info

My background

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

Current roles

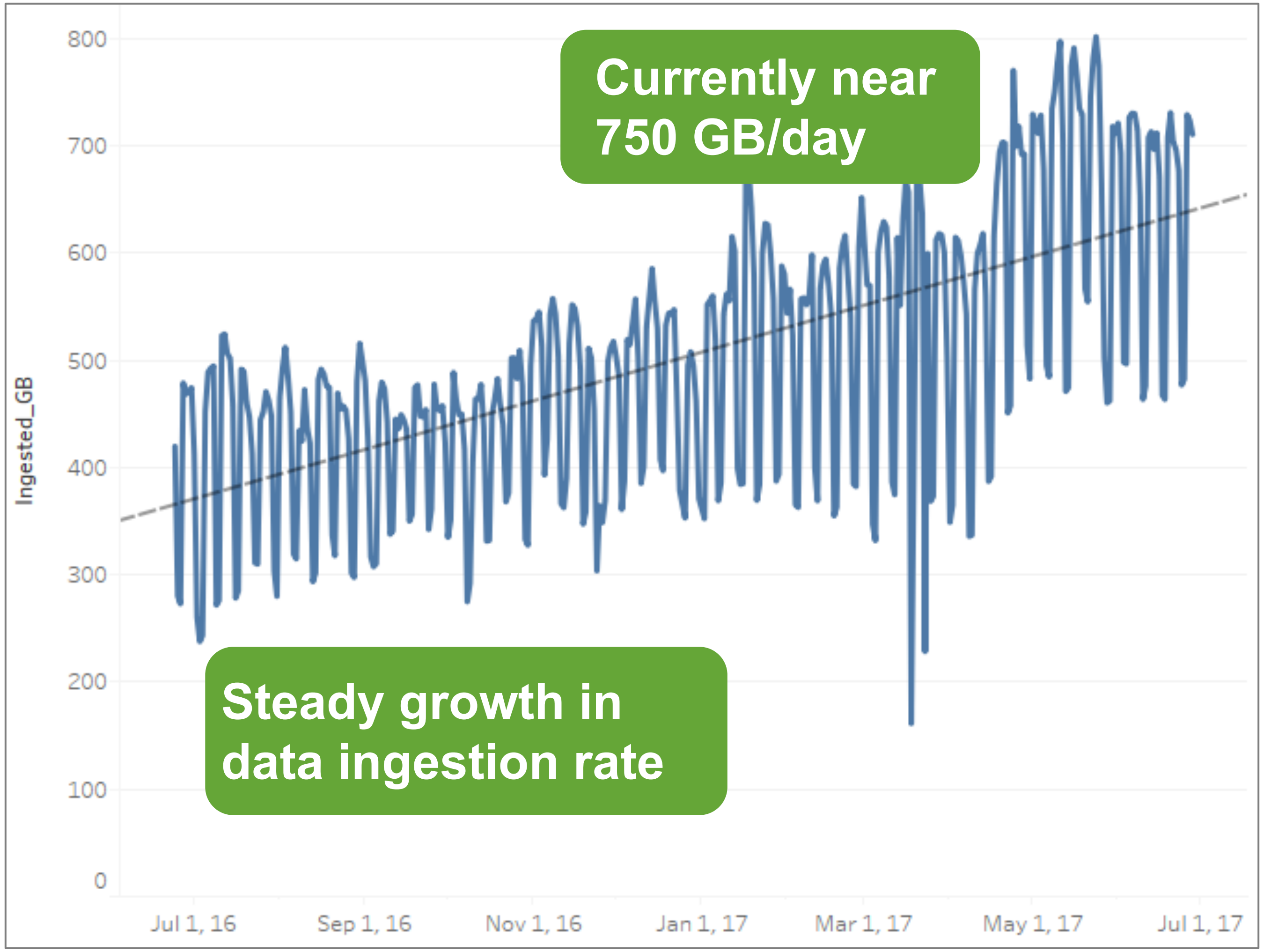
- Team lead
  - Enterprise systems monitoring
  - Performance & automated functional testing
- Corporate IT Splunk service manager
  - Been Splunking for ~2.5 years



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**



Currently near 750 GB/day

Steady growth in data ingestion rate

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

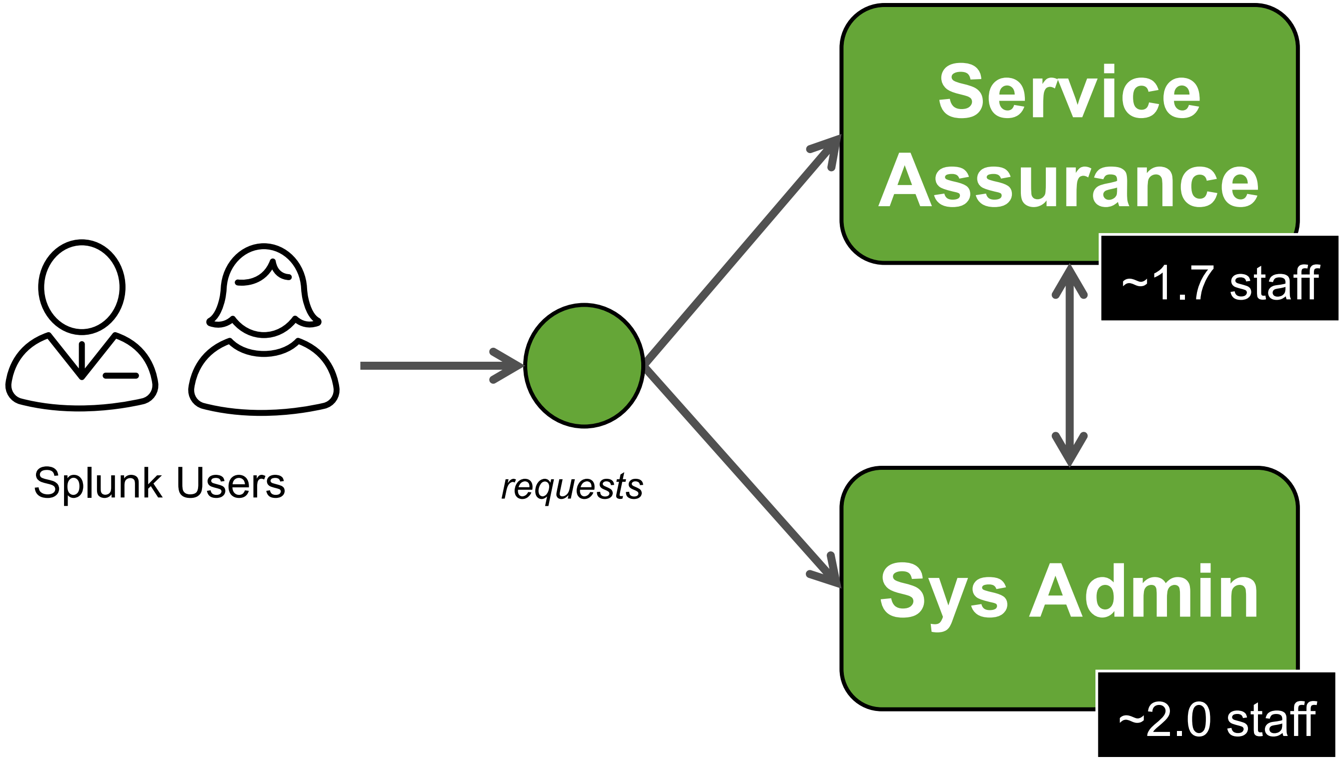
- Splunk service offerings
- How to request
- Typical time needed to fulfill
- Cost
- Points of contact

Service Offerings

- Account and data access
- Ingest new data source into Splunk
- Searches, reports, dashboards, etc.
- Alerting
- Other services

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

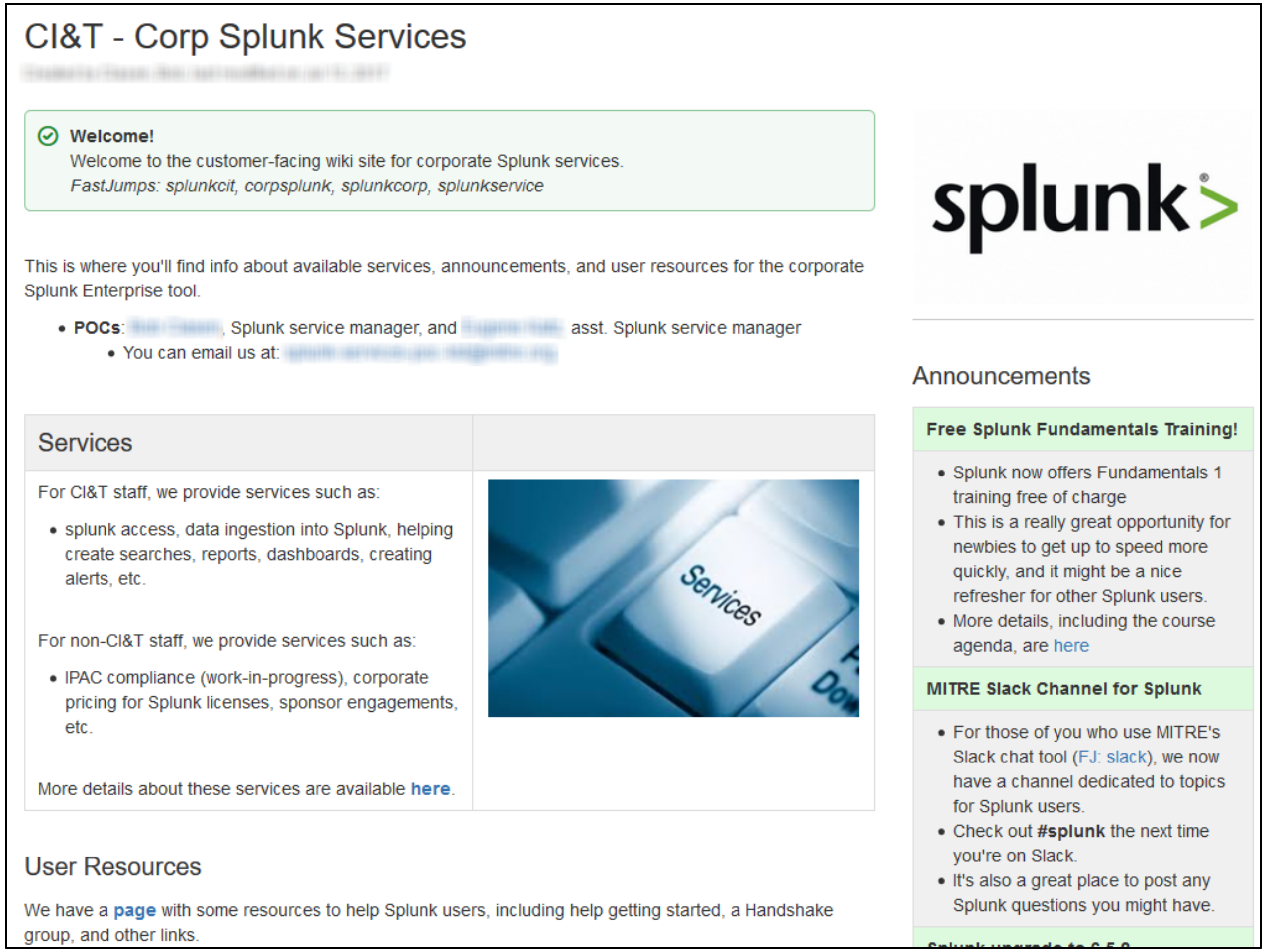
Expand use cases

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

[redacted]

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**: [redacted], Splunk service manager, and [redacted] asst. Splunk service manager
  - You can email us at: [redacted]

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

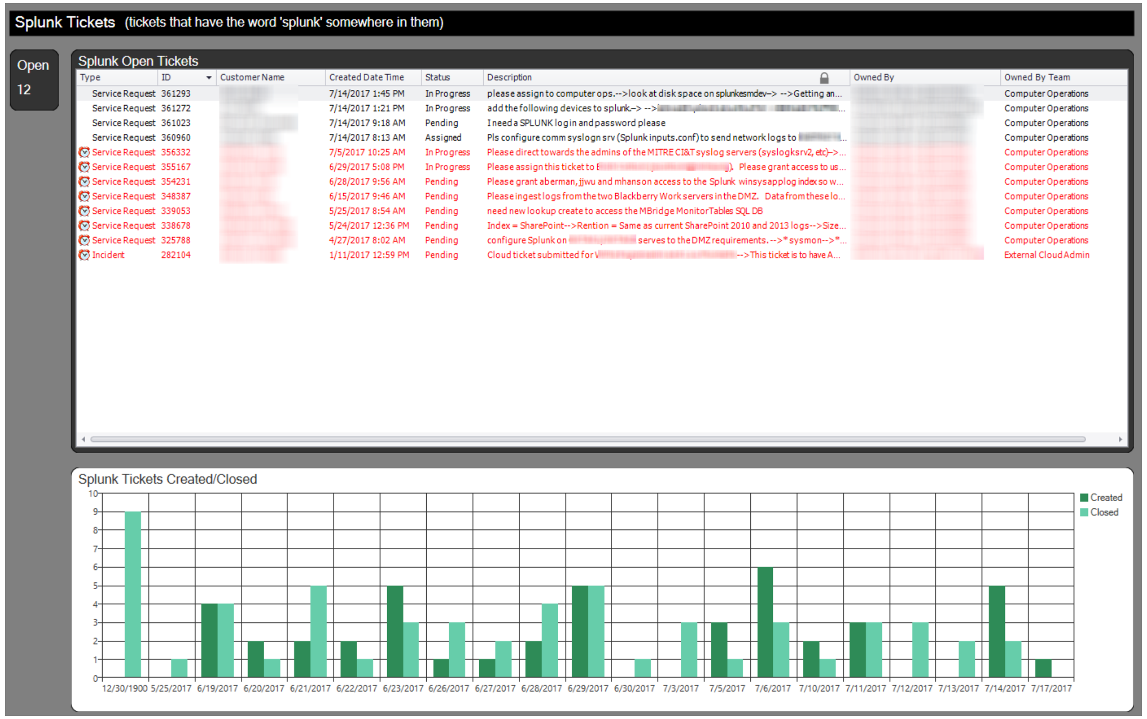
MITRE Slack Channel for Splunk

- 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



Splunk Tickets (tickets that have the word 'splunk' somewhere in them)

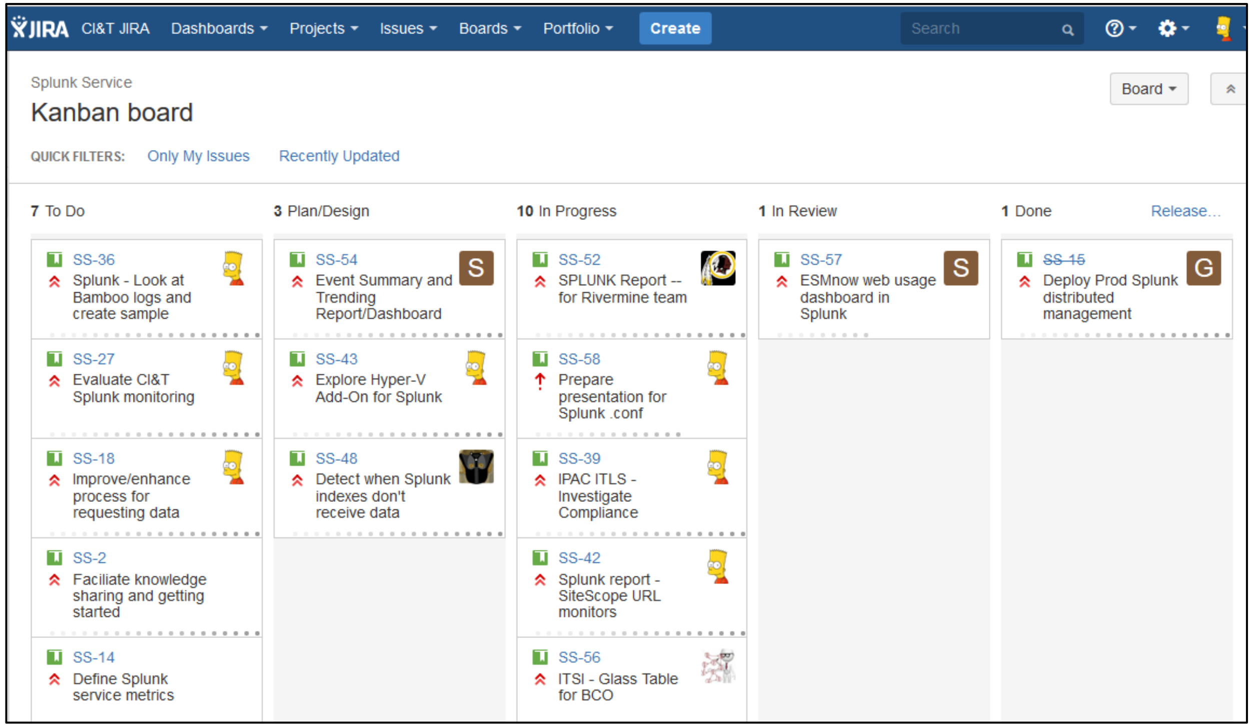
Open
12

Splunk Open Tickets

Type	ID	Customer Name	Created Date Time	Status	Description	Owned By	Owned By Team
Service Request	361293	[redacted]	7/14/2017 1:45 PM	In Progress	please assign to computer ops.-->look at disk space on splunkesmdev--> -->Getting an...	[redacted]	Computer Operations
Service Request	361272	[redacted]	7/14/2017 1:21 PM	In Progress	add the following devices to splunk.--> -->[redacted]...	[redacted]	Computer Operations
Service Request	361023	[redacted]	7/14/2017 9:18 AM	Pending	I need a SPLUNK log in and password please	[redacted]	Computer Operations
Service Request	360960	[redacted]	7/14/2017 8:13 AM	Assigned	Pls configure comm syslogn srv (Splunk inputs.conf) to send network logs to [redacted]...	[redacted]	Computer Operations
Service Request	356332	[redacted]	7/5/2017 10:25 AM	In Progress	Please direct towards the admins of the MITRE CI&T syslog servers (syslogksrv2, etc)-->...	[redacted]	Computer Operations
Service Request	355167	[redacted]	6/29/2017 5:08 PM	In Progress	Please assign this ticket to [redacted]). Please grant access to us...	[redacted]	Computer Operations
Service Request	354231	[redacted]	6/28/2017 9:56 AM	Pending	Please grant aberman, jjwu and mhanson access to the Splunk winsysapplog index so w...	[redacted]	Computer Operations
Service Request	348387	[redacted]	6/15/2017 9:46 AM	Pending	Please ingest logs from the two Blackberry Work servers in the DMZ. Data from these lo...	[redacted]	Computer Operations
Service Request	339053	[redacted]	5/25/2017 8:54 AM	Pending	need new lookup create to access the MBridge MonitorTables SQL DB	[redacted]	Computer Operations
Service Request	338678	[redacted]	5/24/2017 12:36 PM	Pending	Index = SharePoint-->Rention = Same as current SharePoint 2010 and 2013 logs-->Size...	[redacted]	Computer Operations
Service Request	325788	[redacted]	4/27/2017 8:02 AM	Pending	configure Splunk on [redacted] serves to the DMZ requirements.-->* sysmon-->*...	[redacted]	Computer Operations
Incident	282104	[redacted]	1/11/2017 12:59 PM	Pending	Cloud ticket submitted for [redacted]-->This ticket is to have A...	[redacted]	External Cloud Admin

Splunk Tickets Created/Closed

ITSM tickets (Cherwell)



Splunk Service

Kanban board

QUICK FILTERS: Only My Issues Recently Updated

7 To Do

- SS-36 Splunk - Look at Bamboo logs and create sample
- SS-27 Evaluate CI&T Splunk monitoring
- SS-18 Improve/enhance process for requesting data
- SS-2 Faciliate knowledge sharing and getting started
- SS-14 Define Splunk service metrics

3 Plan/Design

- SS-54 Event Summary and Trending Report/Dashboard
- SS-43 Explore Hyper-V Add-On for Splunk
- SS-48 Detect when Splunk indexes don't receive data

10 In Progress

- SS-52 SPLUNK Report -- for Rivermine team
- SS-58 Prepare presentation for Splunk .conf
- SS-39 IPAC ITLS - Investigate Compliance
- SS-42 Splunk report - SiteScope URL monitors
- SS-56 ITSI - Glass Table for BCO

1 In Review

- SS-57 ESMnow web usage dashboard in Splunk

1 Done Release...

- ~~SS-15~~ Deploy Prod Splunk distributed management

Kanban cards (JIRA)

splunk> .conf2017

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

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

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

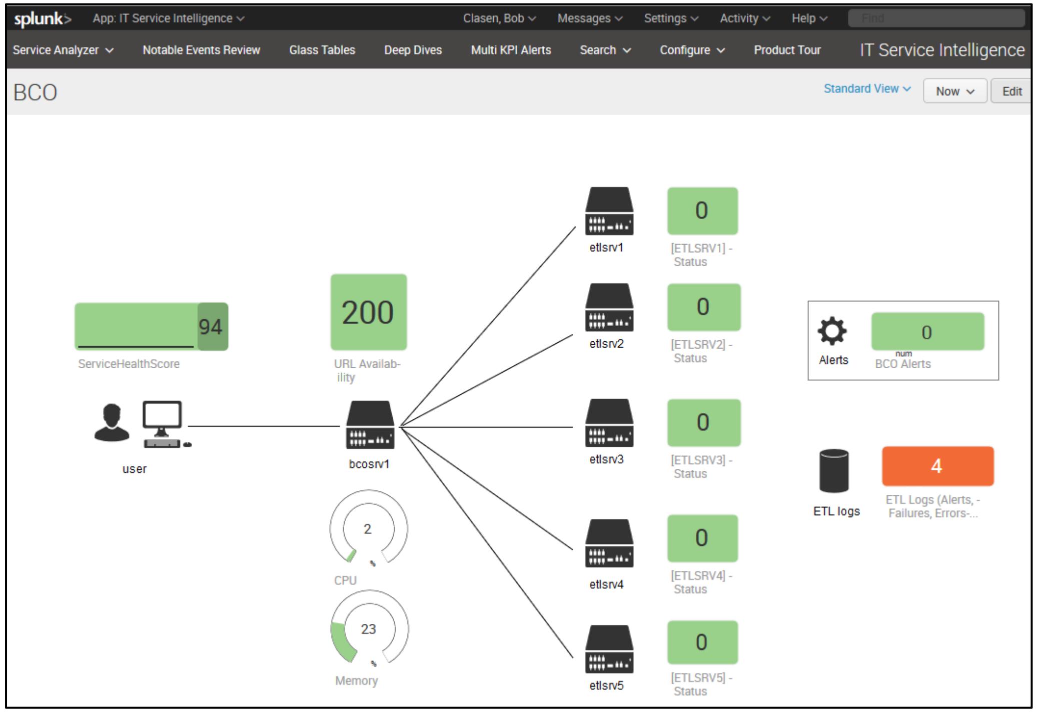
Current Service Offerings

- Account and data access
- Ingest new data source into Splunk
- **NEW** Searches, reports, dashboards, etc.
- Alerting
- Other services

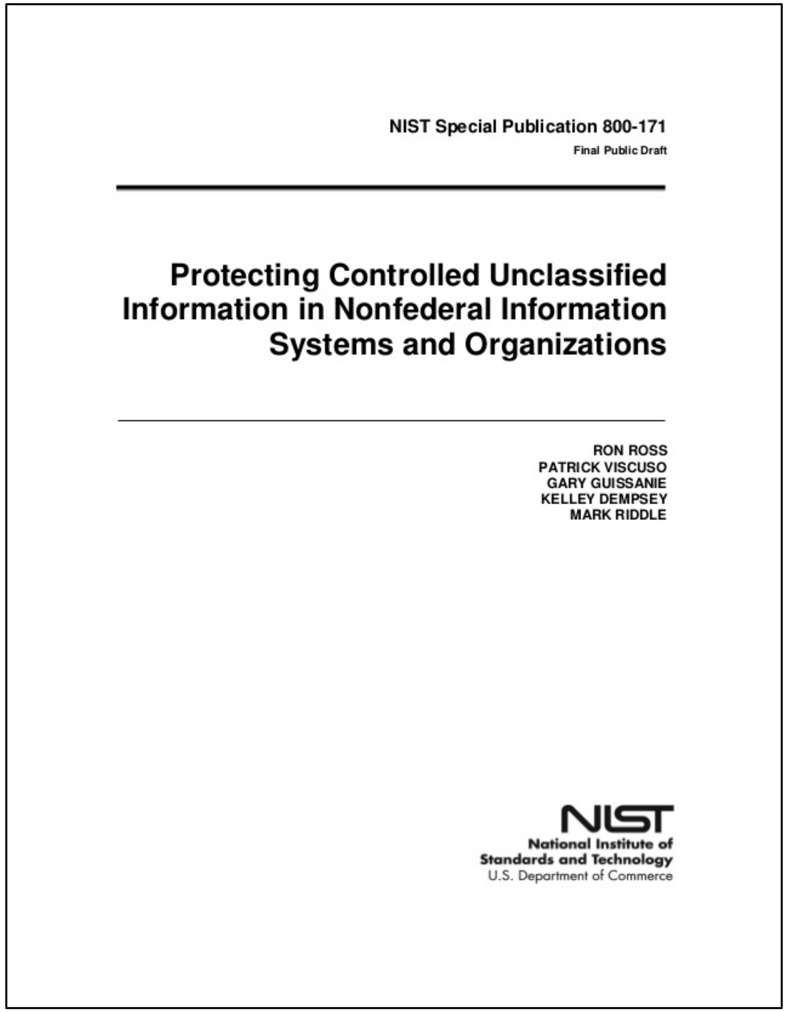
3 *Increase Value*

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



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

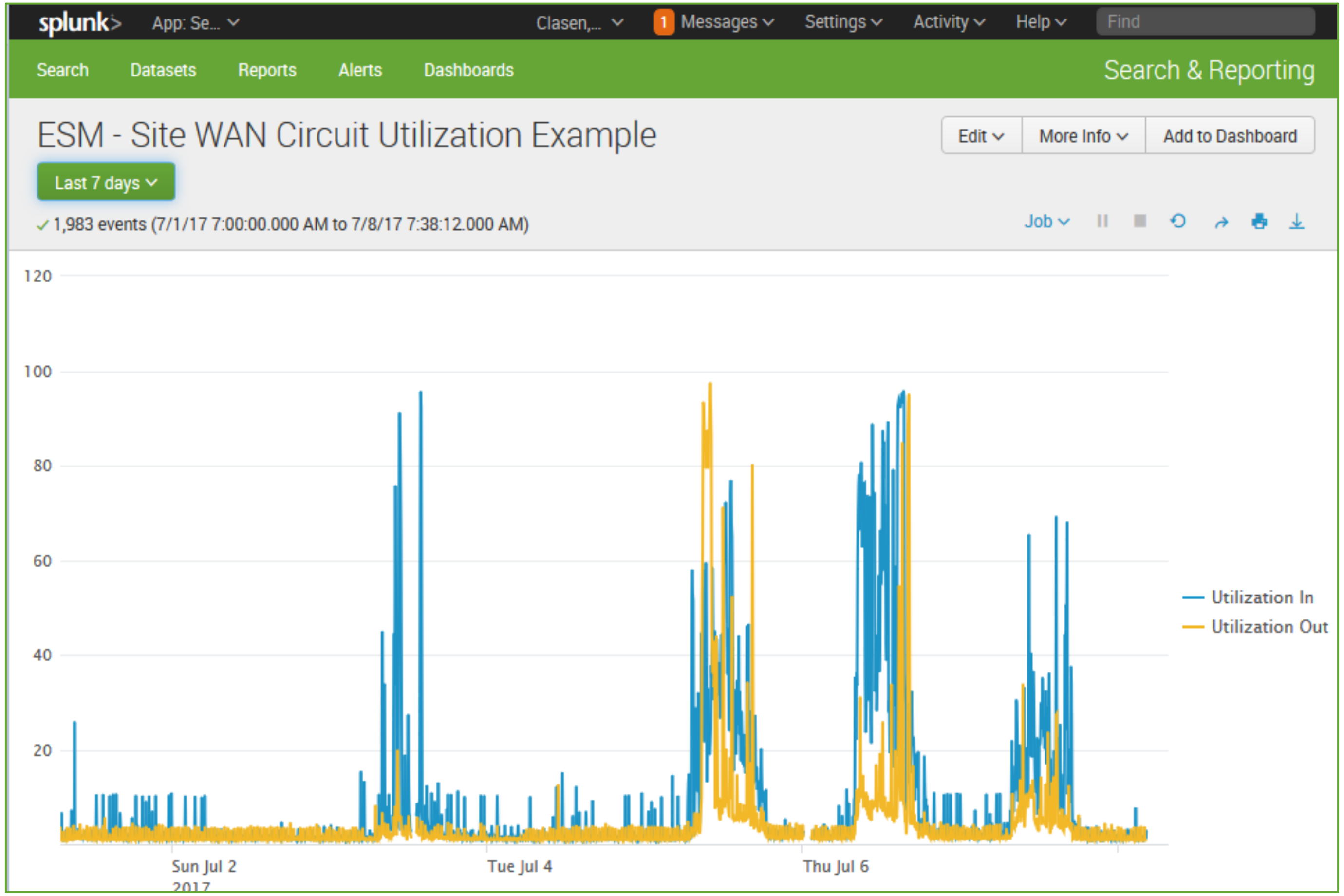
- **With not-for-profits like us, it can be tough to show value/ROI numerically**
  - Lost sales, abandoned shopping carts, etc. aren’t applicable
- **However, we’ve used the following to show Splunk’s value:**

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**

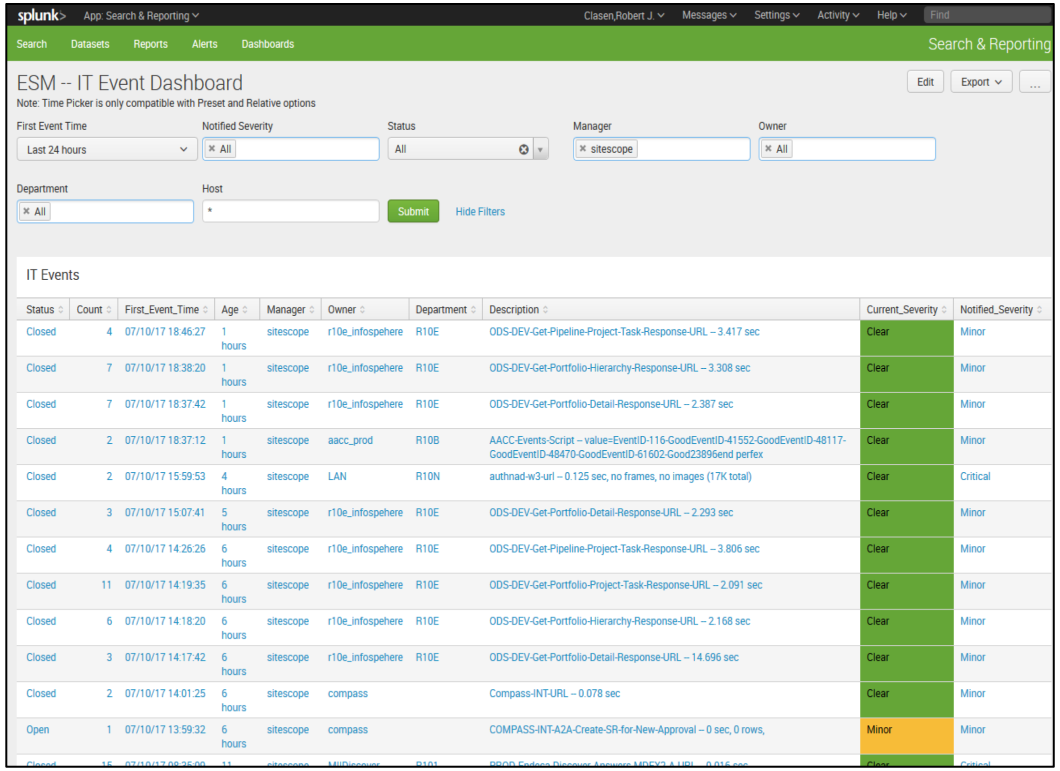


ESM - Site WAN Circuit Utilization Example

✓ 1,983 events (7/1/17 7:00:00.000 AM to 7/8/17 7:38:12.000 AM)

2 Show Value

Find Examples To Demonstrate Value



ESM -- IT Event Dashboard

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

First Event Time: Last 24 hours

Notified Severity: All

Status: All

Manager: sitescope

Owner: All

Department: All

Host: *

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_infospehere	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_infospehere	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_infospehere	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 perfex	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_infospehere	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_infospehere	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_infospehere	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_infospehere	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_infospehere	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-A2A-Create-SR-for-New-Approval -- 0 sec, 0 rows,	Minor	Minor
Closed	15	07/10/17 08:25:00	11	sitescope	MIIDiscover	R101	PROD-Endeca-Discover-Answers-MDEX2-A-URL -- 0.016 sec	Clear	Critical

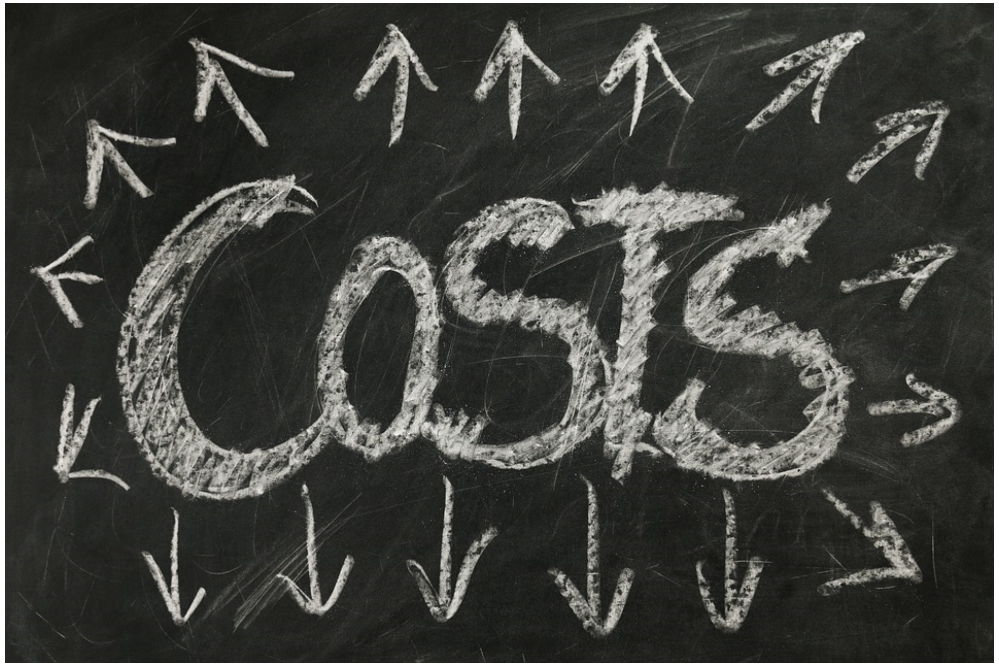
IT Event Dashboard

- **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

Manage Cost

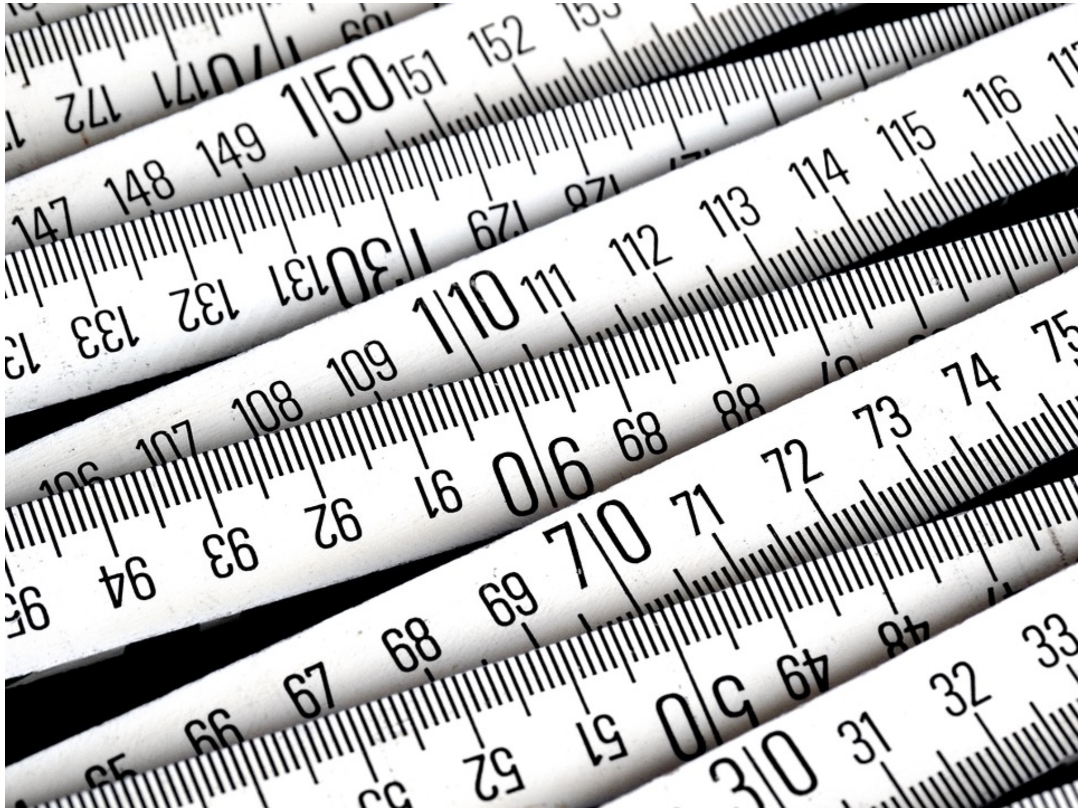
- **By managing cost effectively, you improve ROI**
  - Get same value while reducing cost
- **Primary cost of Splunk due to licenses**
  - Manage license growth
    - Data lifecycle management
    - Track indexes that suddenly grow in size
- **Other cost areas for Splunk**
  - Personnel
    - Make manual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



4 *Show Value*

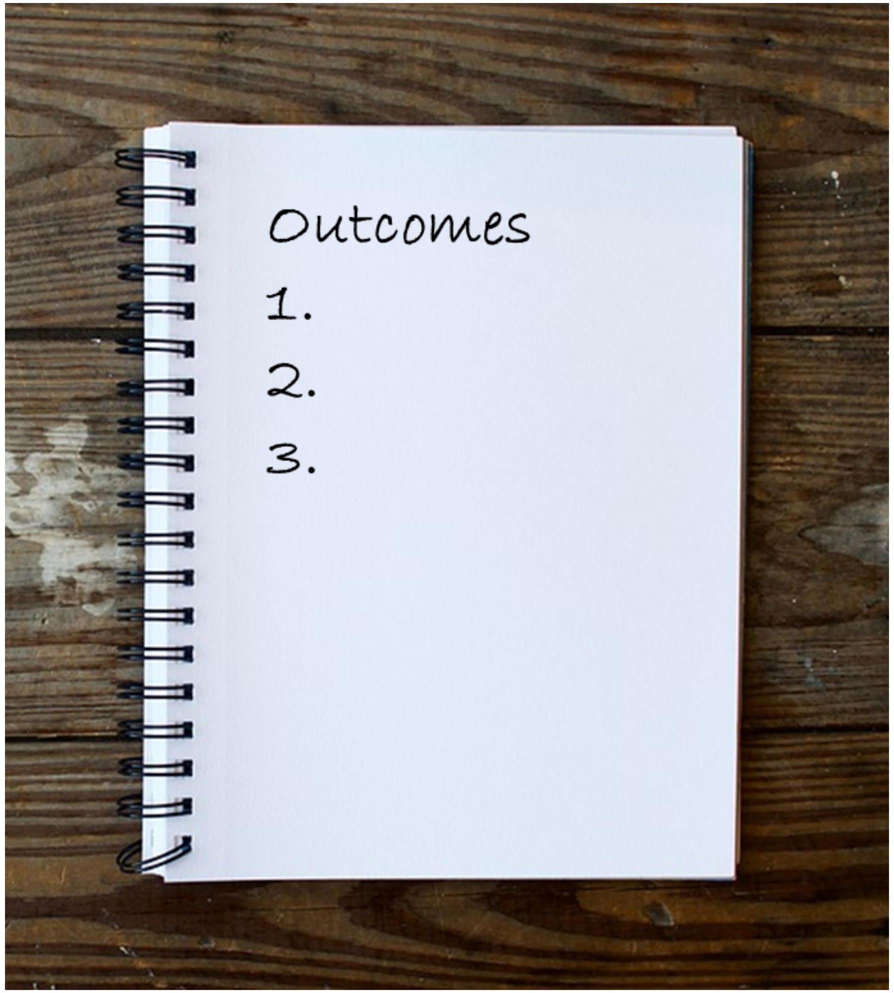
Explore Use Of Metrics

- **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**

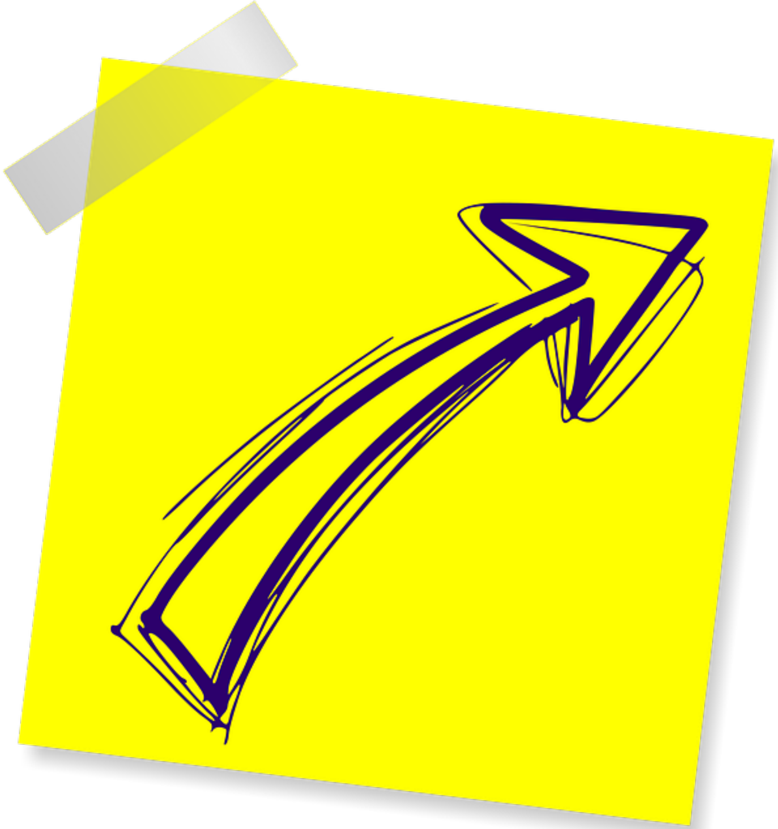


Results

- **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

Thank You

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

splunk> .conf2017