Gaining Executive Support for Splunk by Positioning it's Value

Doug May

AVP, Global Markets Specialization

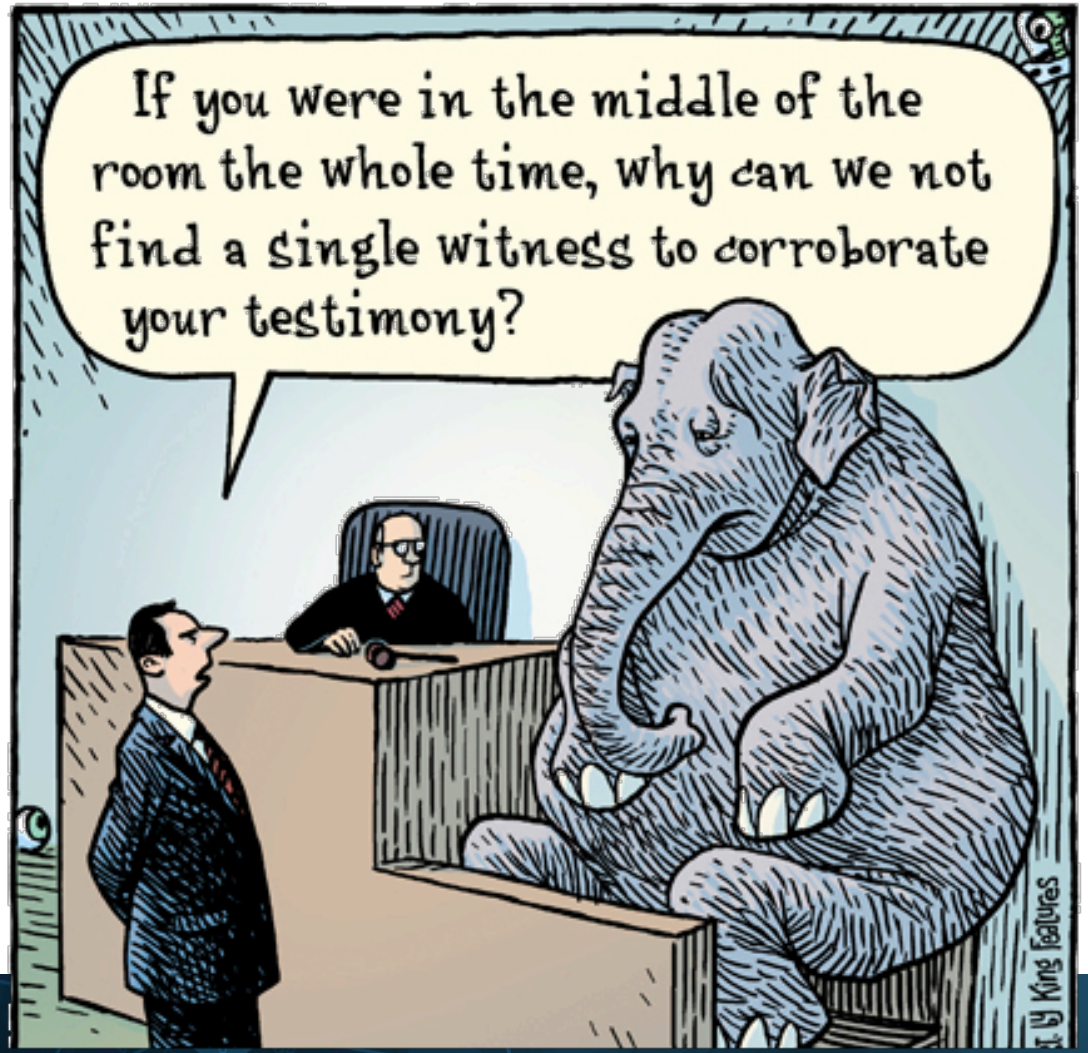
Splunk

splunk>

Disclaimer

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 the 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.


If you were in the middle of the room the whole time, why can we not find a single witness to corroborate your testimony?
BY King Features

Business Value Consulting at Splunk

Help Splunk document the **projected** and **already realized business value** of making machine data accessible, usable, and valuable for everyone

Common Deliverables:

- CFO-Ready Business Cases
- Value Realization Studies
- Usage Maturity & Staffing Readiness
- Enterprise Adoption Roadmaps
- Customer and Industry Benchmarks

600+

Engagements Worldwide Since 2013

Why Position *Business* Value?

Your process requires it

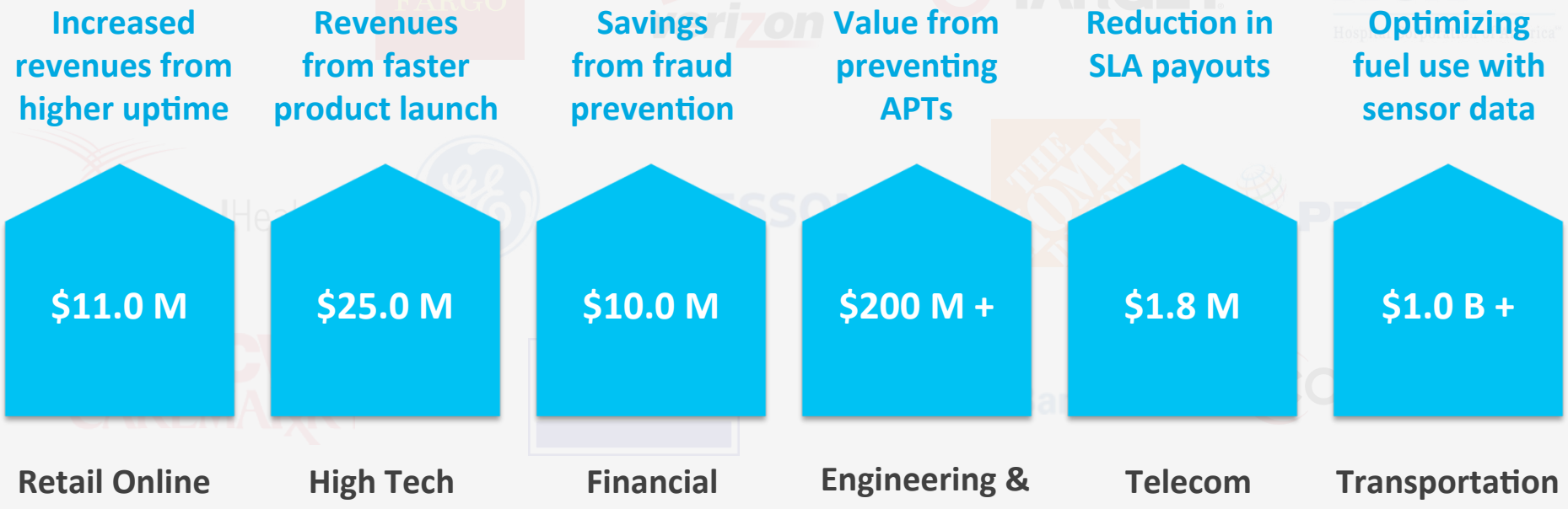
Create and maintain visibility

Replicate success across the organization

Accelerate enterprise adoption

Maximize business results

Proven *Business* Value Across Industries



In addition to significant labor savings enabling scalability and innovation

Splunk is a **Hidden Gem**

What business value do I get?

I'm invincible!

Way cool, dude.

splunk>

Top Challenges to Positioning Value

Time

Not Enough Time to Assess Your Value

Tools

Lack of Tools to Make Value Measurement Easy

Data

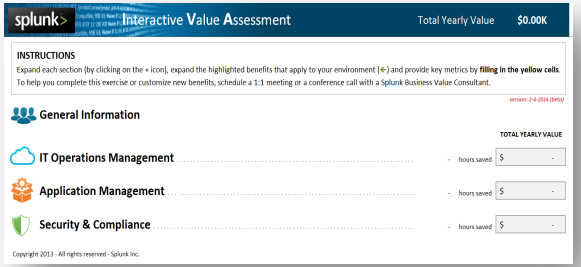
Lack of Splunk and Industry Benchmarks

We're Eliminating Challenges Today!

Time ✓

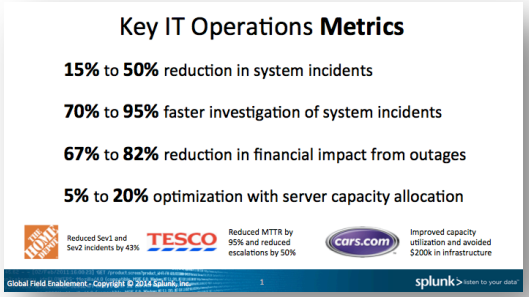
Tools, Content and Team Will Save You Time

Tools ✓



All Splunk Tools Are Available to All of You

Data ✓



Access to Splunk and Industry Benchmarks

Best Practices for Gaining Executive Support

Taking your Splunk deployment to the next level

1

Align with Key Business Objectives

2

Qualify and Quantify Business Value

3

Incremental Steps with a Big Picture Plan

4

Measure, Track, and Report Your Success

Value is in the Eye of the Beholder

1

Align with Key Business Objectives

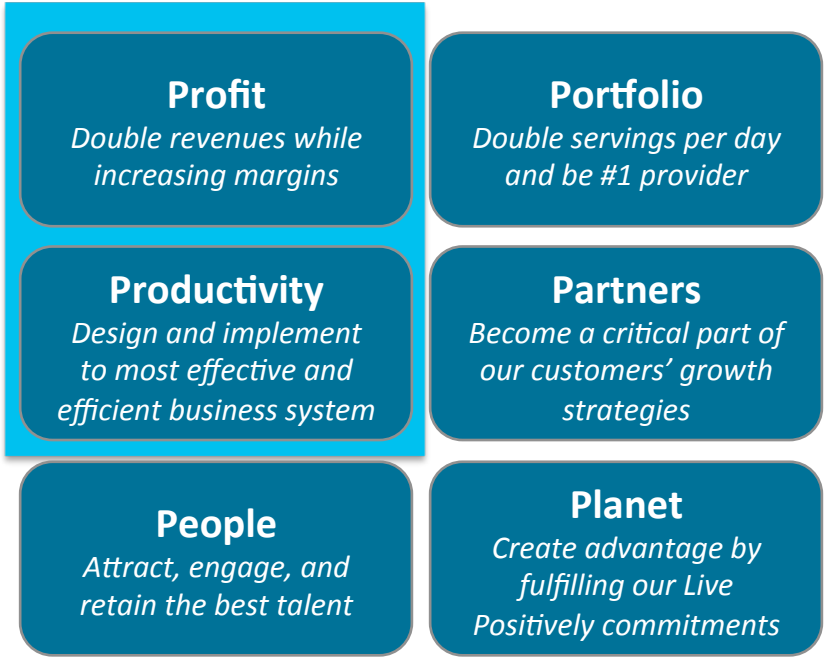
Maybe it's not.

Did you know you can save 15% on your car insurance when you call Geico?

Is that important to ***you***?

A Real Example: **Fortune 100 Company**

*"We also launched a **productivity and reinvestment program to create $550 million to $650 million in annual savings by 2015**. By freeing up resources via supply-chain optimization, improved marketing effectiveness, **operational excellence** and **systems standardization**, **we can invest more in innovation**, marketing and additional "feet on the street**" to drive our growth**." - Fortune 100 CEO*



From investor presentations, annual reports, and executive presentations

Steps to **Qualify Value**

2

Qualify and Quantify Business Value

- ✓ Align your project with something strategic
- Talk with **influential** and knowledgeable people
- Document **why** something should change or be added
- Describe the **current challenges** or barriers
- Identify the **“desired”** state
- *Summarize and socialize to gain support*

A Real Example: **Fortune 100 Company**

Visibility to Environment Health & User Exp.

- Brute force approach providing visibility to key processes isn't working and won't scale
- Operations still lacks complete end-to-end visibility to the environment's health, use and trends
- Blinds spots still exist in monitoring and data access for Operations which could help improve troubleshooting and uptime / availability

Troubleshooting Incidents / Issues

- Operations troubleshooting is cumbersome and suboptimal
- It's still manual across IT silos
- It's difficult to find root cause of incidents quickly
- Performance issues are difficult to resolve
- Outages and impact are elongated due to manual efforts and silos
- Teams are distracted from their core work when they're troubleshooting

DESIRED STATE VISION:

Complete visibility to environment health & trends across full application stack for all stakeholders

Proactively avoid issues before the business is impacted

Reduce MTTR with rapid root cause analysis

Incident / Issue Notification

- Brute force approach to proactive monitoring isn't working consistently and won't scale
- There's a "Waterfall effect" – small issues go without broader notification triggering other issues eventually leading to a bigger incident
- Users are aware of issues before Operations and call the helpdesk
- All the lights are "green" but still ~65% of incidents overall are reported first by the business

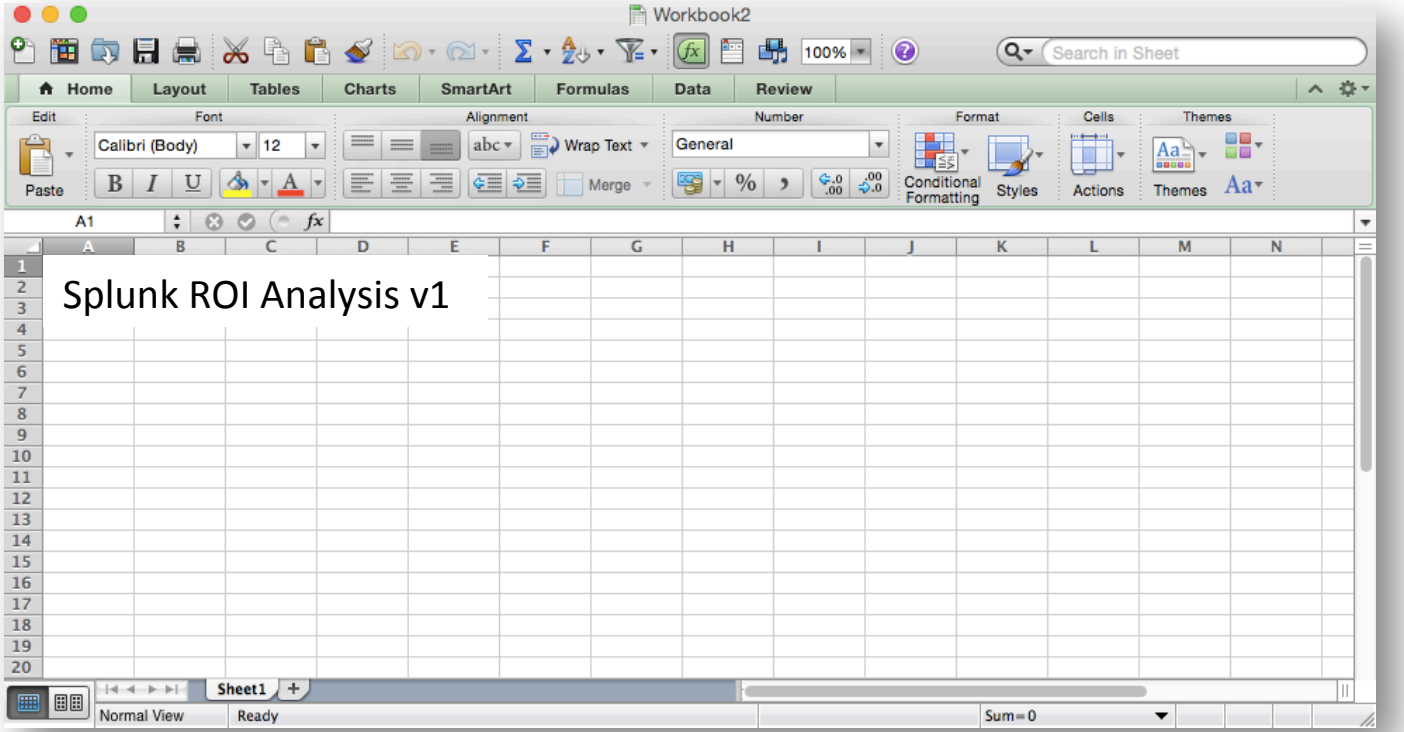
Recurring Incidents / Issues

- The Problem Management process isn't working because there are many high severity incidents still without root cause determined
- As a result, Operations is solving the same problems again and again
- Opportunities exist to improve on incident avoidance since @25%+ of incidents are repeats

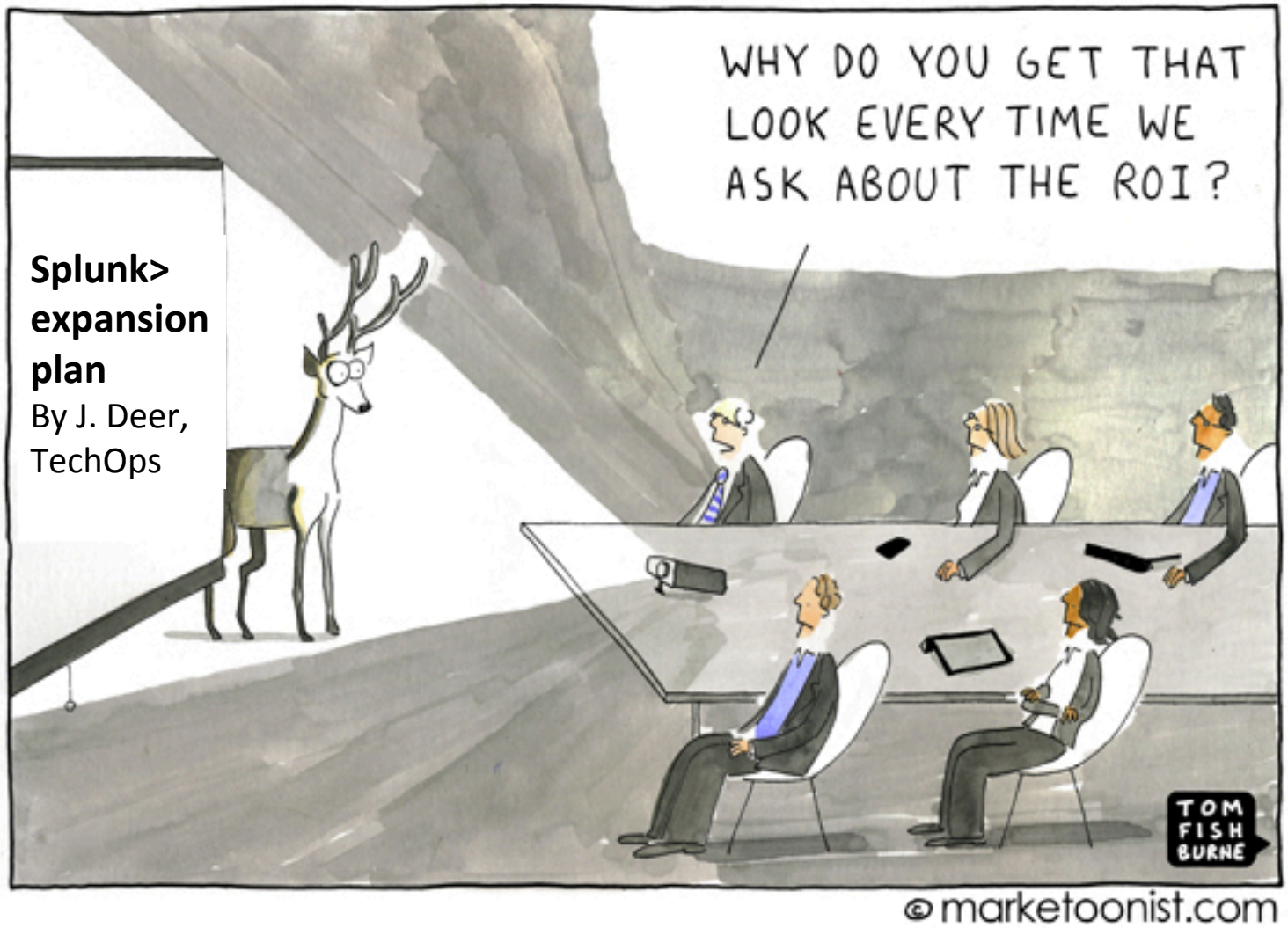
Building the ROI & **Calculating Value**

Have you built an ROI before?

- Step 1:
  - Open Excel



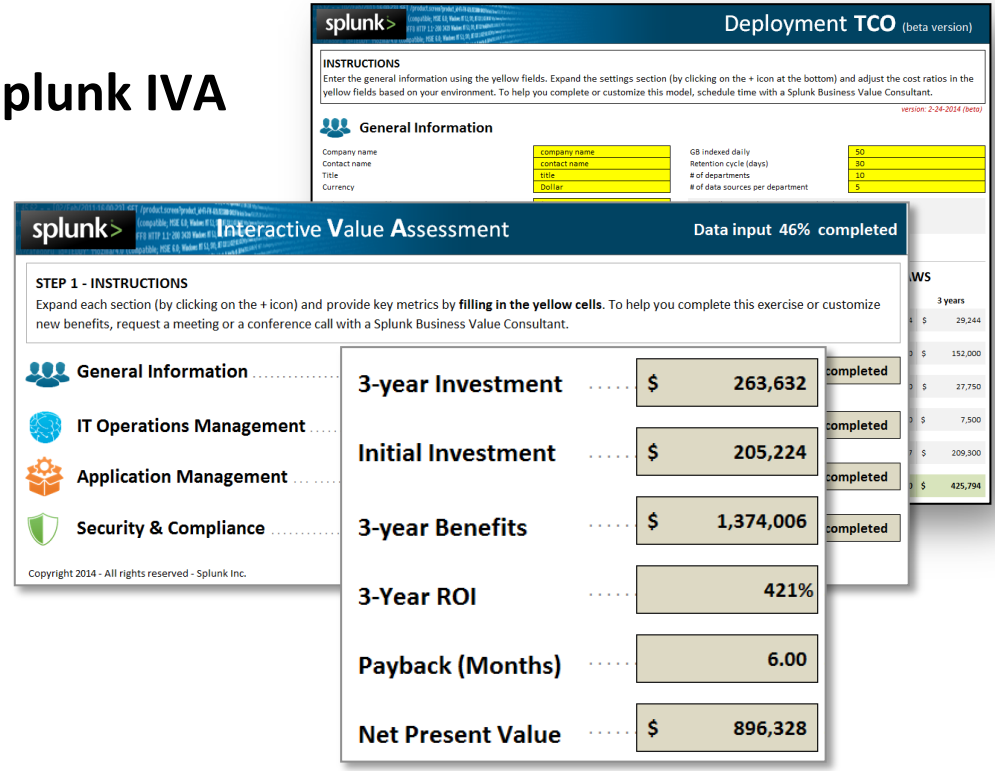
- Step 2: ***??***
  - Fill in the blanks


WHY DO YOU GET THAT LOOK EVERY TIME WE ASK ABOUT THE ROI?
Splunk> expansion plan
By J. Deer, TechOps
TOM FISH BURNE
©marketoonist.com

Quantifying Value with Splunk Tools

- **Financial Analysis Made Easy – Splunk IVA**
  - Over 45 Value Calculators
  - Driven by **Actual Customer Results**
  - Complete Financial Analysis
  - Best Practice TCO Models

- **Don't Forget**
  - Follow the Impact
  - Capture All the Value
  - *Summarize and Socialize*



Leverage the **Common Benefits & Benchmarks**

Documented by BVC through 600+ engagements worldwide

IT Operations

15-45% reduction in high priority incidents

70-90% reduction in incident investigation time

67-82% reduction in financial impact

5-20% increase in capacity utilization

Application Delivery

70-90% reduction in QA defect/failure investigation

10-50% improvement in time to market

80-90% less time building reports and dashboards

10-50% increase in value for key projects

Security & Compliance

70-90% faster detection and triage of security events

70-90% reduction in incident response time

10-50% reduction in risk of data breach, IP theft, fraud

70-90% reduction in compliance reporting time

Splunk Customer Success Stories

Documented by BVC through 600+ engagements worldwide

IT Operations

Reduced Sev1 and Sev2 incidents **by 43%**

Reduced troubleshooting time **by 70%** and user impact **by 40%**

Improved capacity utilization and **avoided $200k** in infrastructure

Application Delivery

Went from **1 release/day to 8** with Splunk and added no new staff

Reduced developer time troubleshooting **by 95%** and shortened their development cycles **by 30%**

Security & Compliance

Reduced the number of security incidents **by 80%** with faster detection

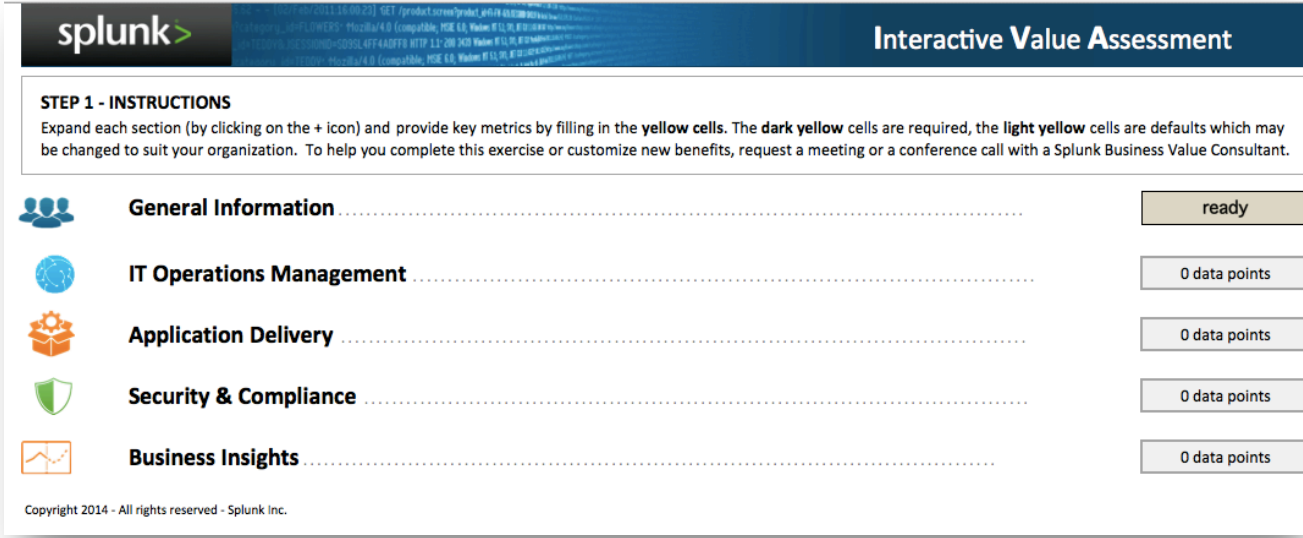
Reduced investigation effort by more than **75%**

Reduced the time to report on SAS70 compliance **by 83%**

Splunk **IVA Highlights**

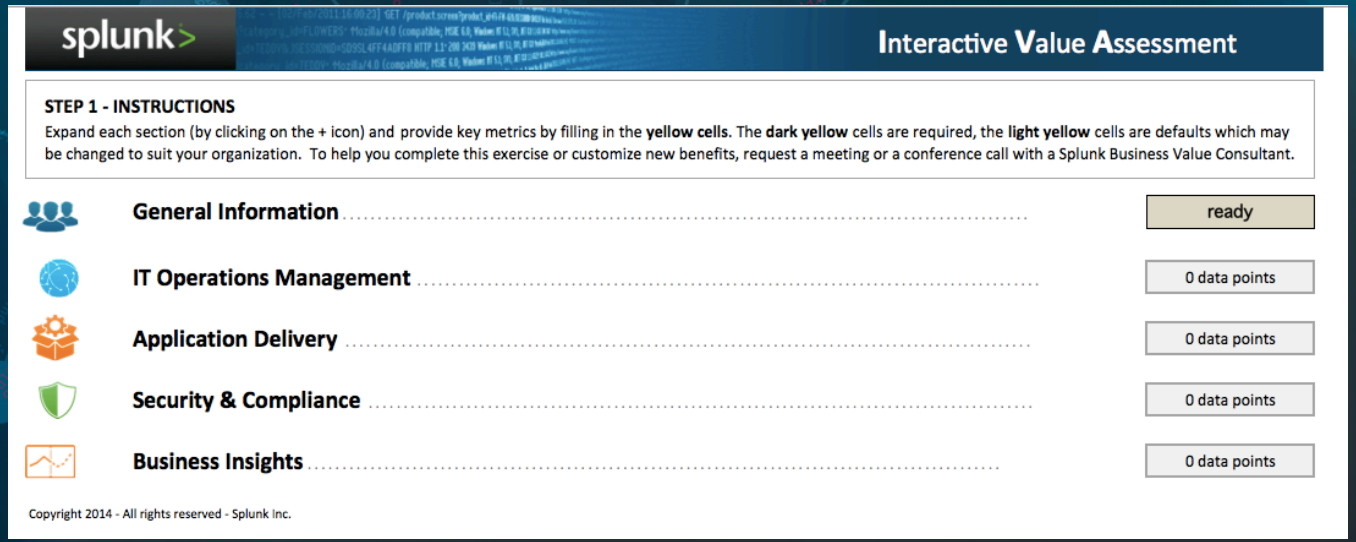
Interactive Value Assessment

- Calculate value in **1 or multiple areas**
- **45+ value calculators** covering common benefits of Splunk
- **Full financial analysis**
- Built-in industry benchmarks and **customer case studies**



.conf2015

Splunk Interactive Value Assessment (IVA) Demonstration



splunk>

Execute Against a **Strategy**

Take directional, incremental steps

3

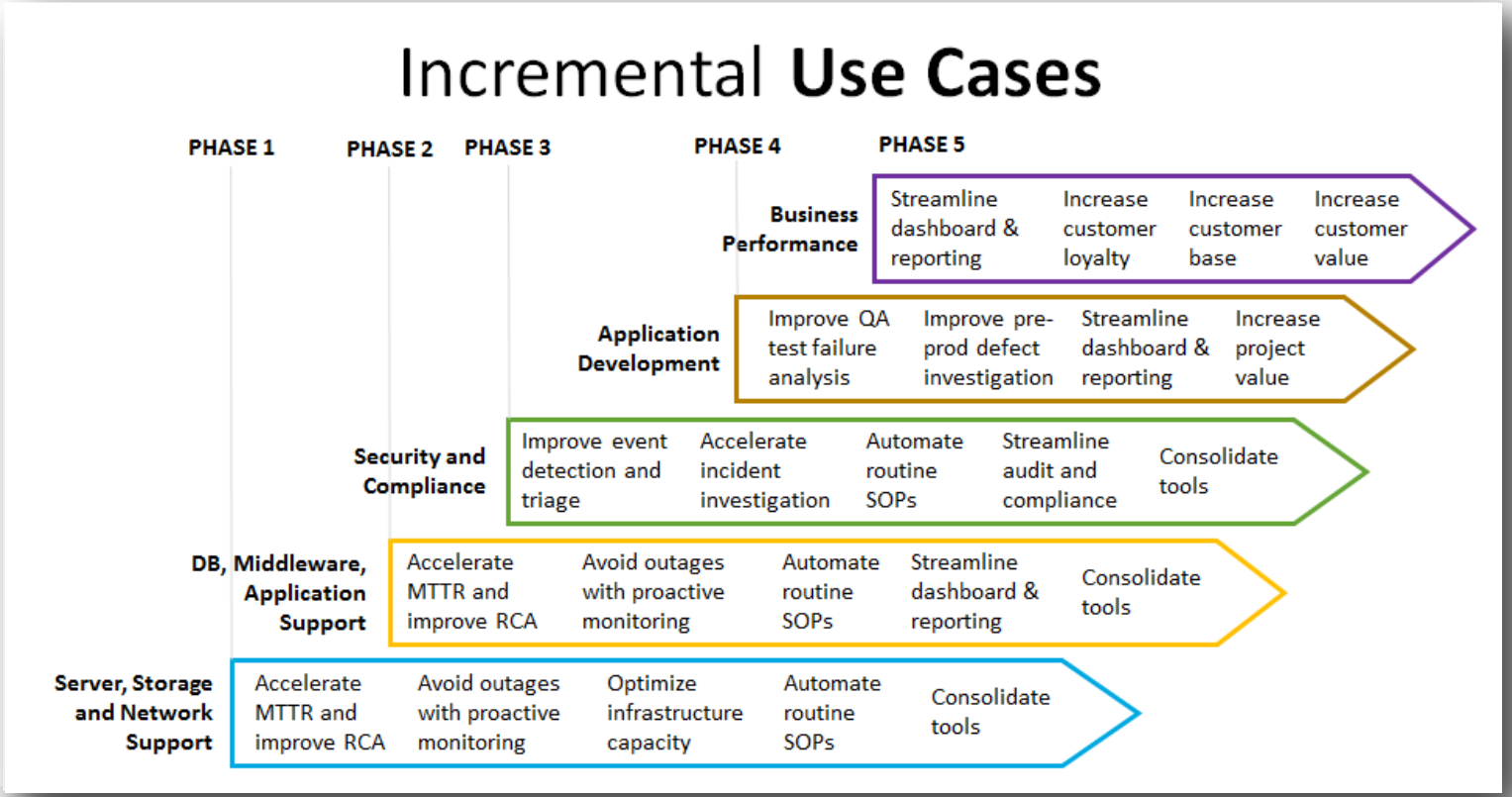
Incremental Steps with a Big Picture Plan

- **Avoid being reactive** – avoid driving by data source
- Develop a strategic plan to leverage Splunk

✓ *Link the plan to strategic company goals*

- Use Splunk tools and benchmarks to document and quantify the anticipated value
- Set baselines for success
- Commit to measure value realized post deployment

What **Your Splunk Strategy** Might Look Like



Measuring & Tracking Success

Helping you take it to the next level

4

Measure and Track Your Success

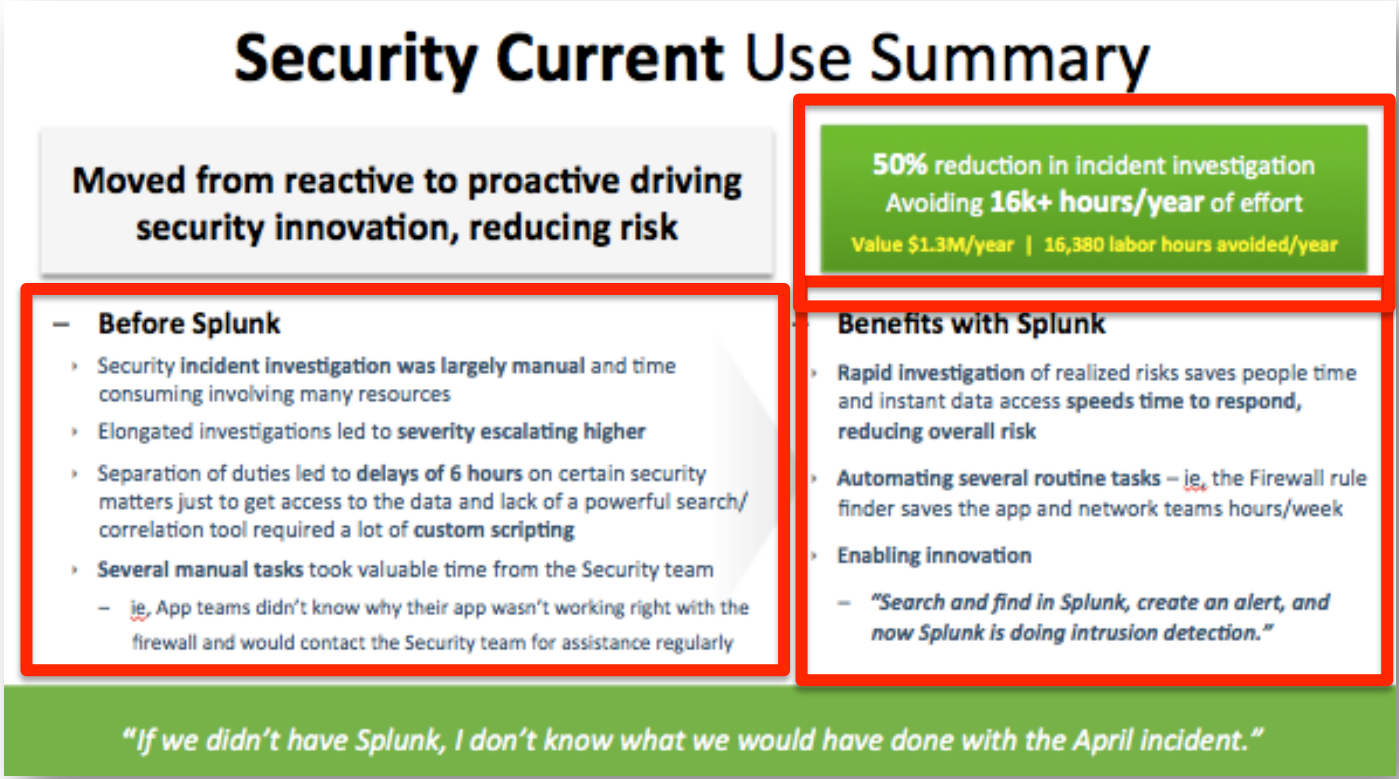
- **Demonstrating success will help further the cause**
- Tell the story of your Splunk usage
- Compare your success against Splunk customer benchmarks
- Assess your usage and staffing maturity
- Then bring it all together

Value Realization	Usage Maturity	Skills Readiness

Measure Success with **Value Realization**

"Money follows money well spent"

- Summarize **BEFORE and AFTER** Splunk
- **Capture metrics** of improvement
- **Socialize** your success



NOTE: *From a $40B+ Global Retailer*

Usage **Adoption Drives Value**

Usage **Maturity Assessment – IT OPS**

Compare your current use to the most common that drive value

Groups	% Data Indexed	Log Collection	Incident Investigation		Root Cause Analysis	Proactive Alerting	Operational Dashboards	Business Analytics	Capacity Planning
			Level 1 Triage	Level 2 & 3 Escalation					
Virtualization	0%	○	○	○	○	○	○	○	
OS - Unix	25%	◐	◐	◐	○	○	○	○	○
OS - Windows	0%	○	○	○	○	○	○	○	○
Storage	33%	◐	◐	◐	◐	○	○	○	○
Network	100%	●	●	●	◐	○	○	○	○

● = Splunk fully in use ◐ = Splunk partially in use ○ = Splunk not in use

Usage **Maturity Assessment – APP DEV**

Compare your current use to the most common that drive value

Top Apps	% Indexed	Evaluate and Assess Needs		Develop and Release	
		Data Collection	Business Insight	Test Failure Analysis	Defect Investigation
SAP	0%	○	○	○	○
Warehouse Mgt	0%	○	○	○	○
E-Commerce Website	50%	○	○	◐	◐
Call Center	80%	●	●	○	○

● = Splunk fully in use ◐ = Splunk partially in use ○ = Splunk not in use

Usage **Maturity Assessment – SECURITY**

Compare your current use to the most common that drive value

Data Sources	% Indexed	Log Collection	Level 1 Triage	Monitoring / Alerting	Investigations	Incident Response	Compliance Reporting	Routine Log Reviews
Threat Intel: (3rd Party)	70%	◐	Currently handled by MSSP	●	●	●	○	○
Threat Intel: (OS Blacklist)	70%	◐		◐	●	●	○	○
Network: (Firewall)	90%	◐		○	●	●	○	○
Network: (IDS/IPS)	90%	◐		◐	●	●	○	○
Endpoint: (PCLM)	80%	◐		◐	●	●	○	○
Access & Identity Mgt	75%	◐		◐	◐	◐	○	○

● = Splunk fully in use ◐ = Splunk partially in use ○ = Splunk not in use

Usage **Maturity Assessments – SECURITY CONTROLS**

Compare your current use to the most common that drive value

Critical Control	In Place?
Monitor unauthorized devices or software	○
Monitor unmanaged devices or software	○
Monitor configuration compliance	○
Monitor patch compliance	●
Monitor malware defense	●
Monitor application software security	◐
Monitor wireless access control	◐
Analyze audit logs with time-based correlation	●

Critical Control	In Place?
Monitor use of ports, protocols, and services	●
Monitor controlled use of admin privileges	●
Monitor perimeter IDS	●
Monitor controlled / uncontrolled access	●
Monitor orphan, expired, miss use of accounts	○
Monitor potential exfiltration of information	●
Monitor secure IP restriction policies	●
Maintain data going back months	◐

● = Splunk fully in use ◐ = Splunk partially in use ○ = Splunk not in use

A $1.5B Online Retailer

A Real Customer Example - Operations

Most common uses of Splunk delivering value

Business Service Components	% of Data Indexed	Log / Data Collection	Incident Investigation		Root Cause Analysis	Proactive Alerting	Operational Dashboards	Business Analytics
			Level 1 Triage	Level 2 & 3 Escalation				
Custom Web Apps	80%	◐	◐	◐	◐	◐	○	○
3rd Party Web-Apps	100%	●	●	●	●	●	○	○
Apps	75%	◐	◐	◐	◐	◐	○	○
Web Server	50%	◐	◐	◐	◐	◐	○	○
Database	100%	●	●	●	●	●	○	○
OS	100%	●	●	●	●	●	○	○
Network	95%	◐	◐	◐	◐	◐	○	○

● = Splunk fully in use ◐ = Splunk partially in use ○ = Splunk not in use

Leverage the **Common Benefits & Benchmarks**

Documented by through 500+ engagements worldwide

IT Operations

15-45% reduction in high priority incidents

70-90% reduction in incident investigation time

67-82% reduction in financial impact

5-20% increase in capacity utilization

Application Delivery

70-90% reduction in QA defect/failure investigation

10-50% improvement in time to market

80-90% less time building reports and dashboards

10-50% increase in value for key projects

Security & Compliance

70-90% faster detection and triage of security events

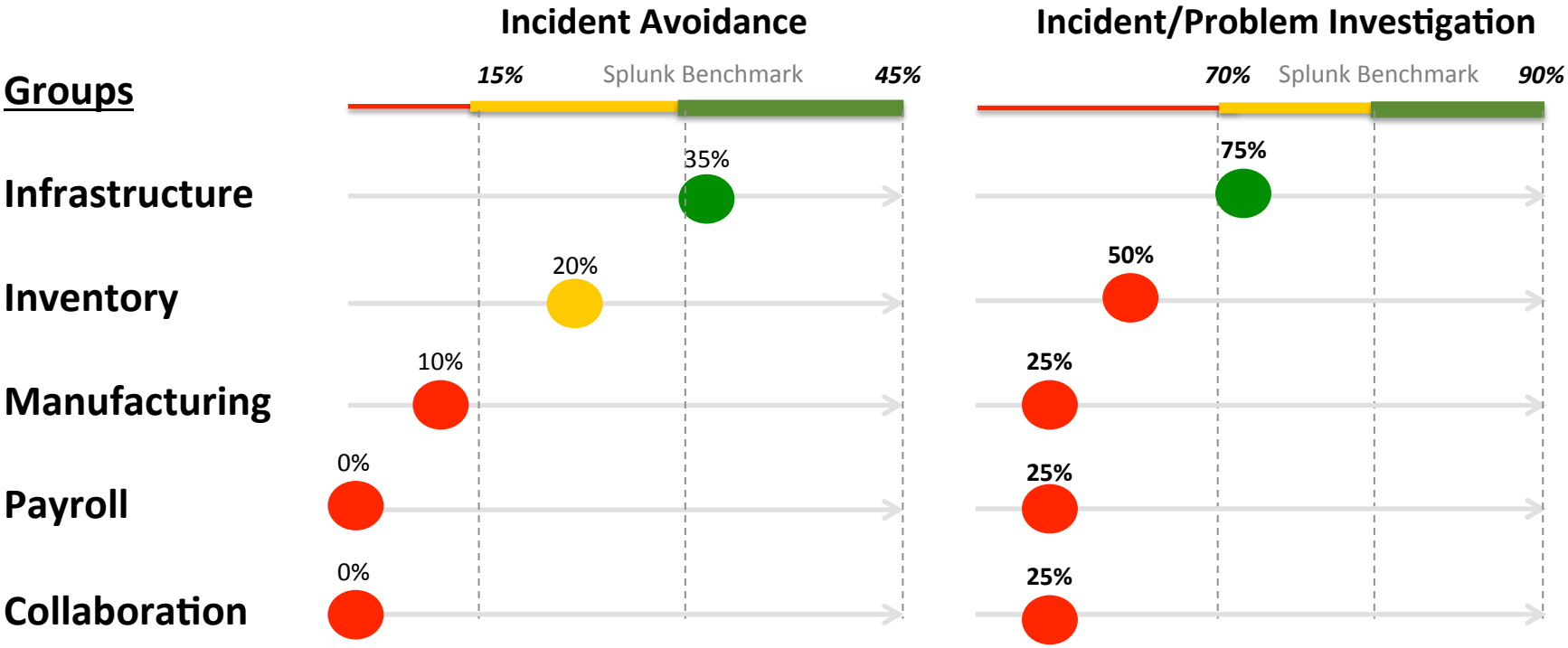
70-90% reduction in incident response time

10-50% reduction in risk of data breach, IP theft, fraud

70-90% reduction in compliance reporting time

Map Your Progress vs. Splunk Benchmarks

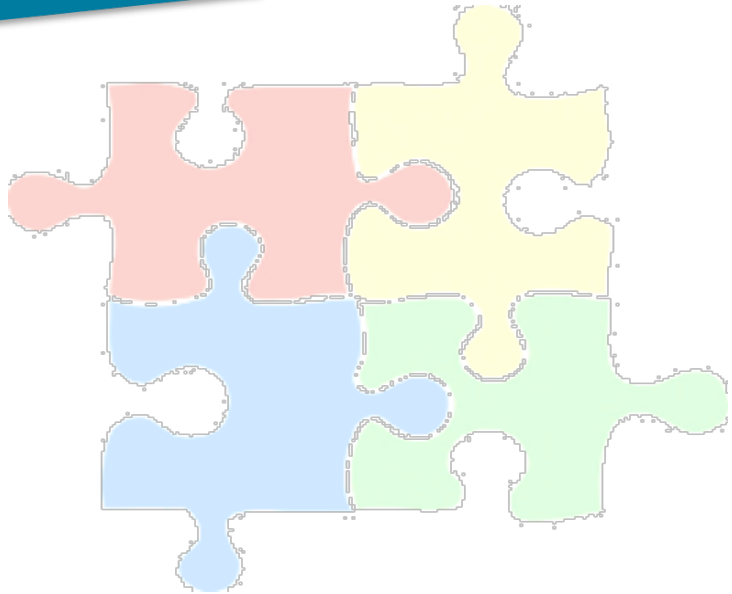
Estimates based on Value Realization and Usage Maturity



Splunk **Staffing Readiness**

Be sure you have the staff and skills to maximize value

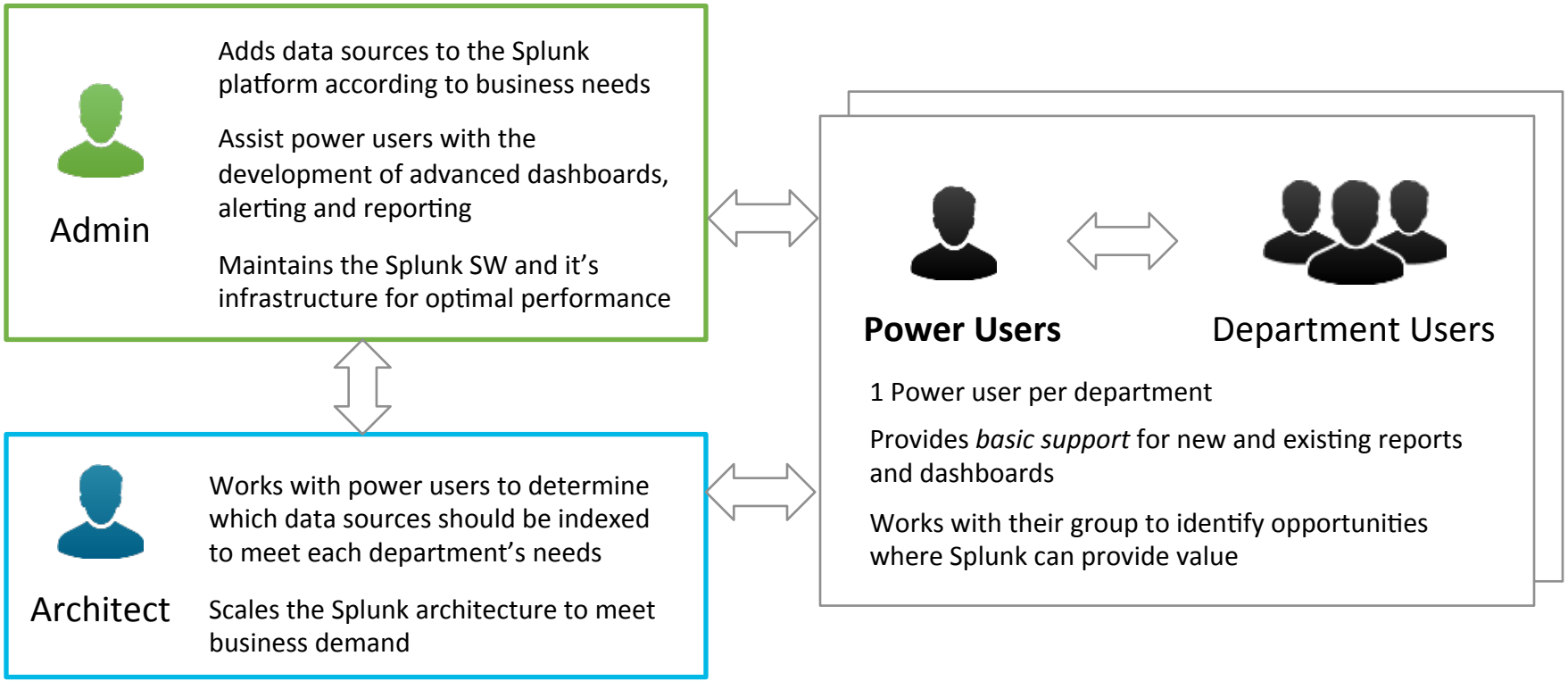
Skills Readiness



A successful and scalable deployment of Splunk relies on the orchestration of key roles and responsibilities, primarily centered around:

- ✓ **Architecture**
- ✓ **Administration**
- ✓ **User adoption (Power User)**
- ✓ **Application development**

Basic **Communication** Framework



Splunk **Roles & Recommended Training**

For Splunk On-premises

Splunk Roles	Using Splunk	Splunk Administration	Searching and Reporting	Creating Knowledge Objects	Advanced Searching & Reporting	Developing Apps with Splunk	Developing with Splunk SDKs
Architect	**Required**	**Required**	Optional	Optional	Optional	Optional	Optional
Admin	**Required**	**Required**	Optional	Optional			
Power User	**Required**		**Required**	**Required**	Optional		
Developer	**Required**	Optional	**Required**	**Required**	Optional	**Required**	Optional

Splunk **Architect Role**

Responsibilities

- Accountable for the design of the Splunk architecture
- Fully understands concepts and best practices for sizing, scaling, and deploying Splunk across your organization so that performance meets current and future needs
- Works with power users to determine data sources to be ingested to meet each department's needs
- ***Part time for < 500GB; 1 Full time for 500GB to 1TB; 2 for >1TB***

Splunk Part-Time Architect(s)	Using Splunk	Splunk Administration	Searching and Reporting	Creating Knowledge Objects	Advanced Searching & Reporting	Developing Apps with Splunk	Developing with Splunk SDKs
• **#name**	●	●	○	○	○	○	

= Required = Optional = Splunk training completed = Training required but not completed = Optional training not completed

Splunk **Admin Role**

Responsibilities

- Maintains the Splunk SW and it's infrastructure for optimal performance
- Adds data sources to the Splunk platform according to Power User needs
- Assist power users with the development of advanced dashboards, alerting and reporting
- ***Part time for < 500GB; 1 Full time for 500GB to 1TB; 2+ for >1TB***

Splunk Administrator(s)	Using Splunk	Splunk Administration	Searching and Reporting	Creating Knowledge Objects	Advanced Searching & Reporting	Developing Apps with Splunk	Developing with Splunk SDKs
• **#name**	●	●	○	○			

= Required = Optional = Splunk training completed = Training required but not completed = Optional training not completed

Splunk **Power User Status**

Recommendation: 1 power-user per group

Responsibilities

- Works with their group to identify opportunities where Splunk can provide value
- Collaborates with the Splunk admin(s) to add new data sources to address their requirements
- Provides *basic support* for new and existing reports and dashboards to their group

Splunk Power User(s)	Using Splunk	Splunk Administration	Searching and Reporting	Creating Knowledge Objects	Advanced Searching & Reporting	Developing Apps with Splunk	Developing with Splunk SDKs
• Web • **John S.**	●		●	●	○		
• Security • **Sally B.**	●		●	●	○		
• Infrastructure • **Mike G.**	●		●	●	○		

= Required = Optional ● = Splunk training completed ● = Training required but not completed ○ = Optional training not completed

Splunk **Developer Role**

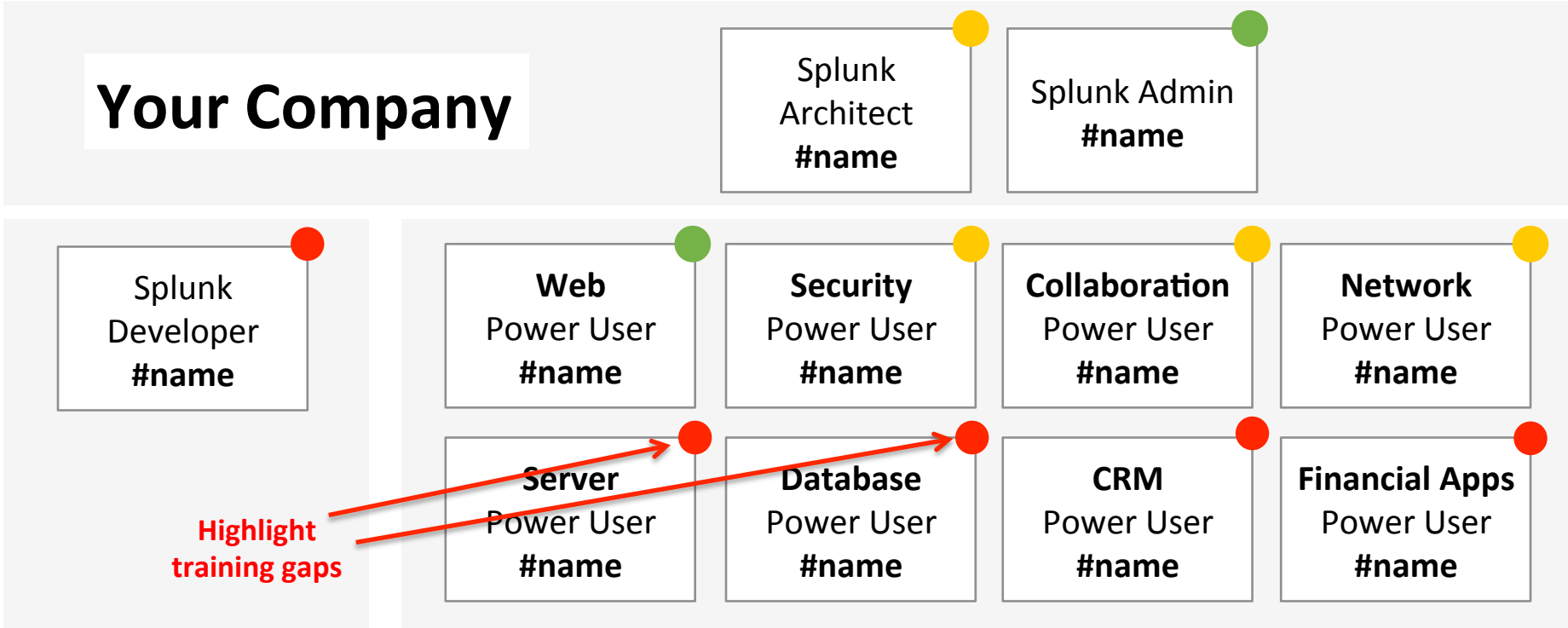
Responsibilities

- Splunk developers are only required if applications are developed on top of the Splunk platform
- Create rich, interactive dashboards and forms, and package Splunk knowledge objects for distribution across your organization

Splunk Developer(s)	Using Splunk	Splunk Administration	Searching and Reporting	Creating Knowledge Objects	Advanced Searching & Reporting	Developing Apps with Splunk	Developing with Splunk SDKs
• Shared • **#name**	●		●	●	○	●	○

= Required = Optional = Splunk training completed = Training required but not completed = Optional training not completed

Map Your Splunk Team

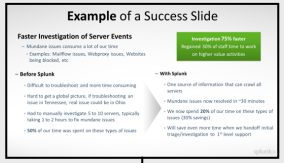


Bringing It All Together

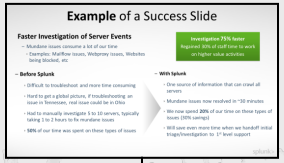
splunk>

Taking it to the **Next Level**

Document Success for Server & Network teams



Document Success for App & DB teams



IT Operations

Value Realized:

- **faster** detection,
- **faster** investigation,
- **faster** root cause analysis of system incidents

Application Support

Value Opportunity:

- **faster** detection,
- **faster** investigation,
- **faster** root cause analysis of application incidents
- **fewer** developer escalation

Application Development

Value Opportunity:

- **faster** test analysis,
- **faster** investigation of pre-production bugs,
- **faster** releases cycles

Security & Compliance

Value Opportunity:

- **faster** detection, **faster** triage,
- **faster** investigation of security incidents

A $40B+ Retailer

Success from Current Use

Positive ROI achieved on ~$1.7M spend to date

20,414
Yearly Hours

$3.92M
Yearly Value

Web Team

42% reduction in business impact
Avoiding revenue loss of **$2.3M/yr**
Value $2.5M/year | 2,445 hours/year

Proactively monitoring a $1.5B revenue platform entirely with Splunk.

Reducing manual effort and impact
Avoiding revenue displacement and loss

"We almost had an outage today. We saw some things in Splunk. That saved us a 1.5 hour incident and almost $300,000."

Opportunities:
Get full stack of data in for additional efficiencies (network, VM, storage, DB)

Security

50% reduction in incident investigation
Avoiding **16k+ hours/yr**
Value $1.3M/year | 16,380 hours/year

Rapid search and investigation of security incidents. Went from reactive to proactive.

Reducing manual effort, impact and risk
Innovating – search to alert to IDS

"If we didn't have Splunk, I am not sure what we would have done with the April incident."

Opportunities:
Apply to PCI readiness saving GRC team effort, enabling continuous compliance.

Infrastructure

50% reduction in incident investigation (when leveraged)
Value $124,102/yr* | 1,589 hours/yr*

Resolving complex issues rapidly; opportunity for even more value.

Reducing manual effort and impact
Realizing only partial benefits today

"When there's a problem, it's tricky to figure out where it is. Splunk's a helpful tool to have."

Opportunities:
Get full environment data in. Use more consistently across team to capture value.

See detailed calculations of value, usage adoption, and staffing maturity schedules in the Appendix.

Benchmarks Used for Infrastructure Calcs

A $40B+ Retailer

Functional Adoption Summary

Comparing [customer]'s current usage against the most common Splunk uses driving value

IT & APPLICATION OPERATIONS	% Usable Data Indexed	Log Collection	Incident Investigation		Root Cause Analysis	Proactive Alerting	Operational Dashboards	Business Analytics	Capacity Planning
			Level 1 Triage	Level 2 & 3 Escalation					
Web Team	**75%** NW*, VM, DB, Storage	◐	●	●	●	●	●	●	◐
Infrastructure	**20%** DB, VM, Windows, Storage	◐	◐	◐	○	○	○	○	○

SECURITY & COMPLIANCE	% Data Indexed	Log Collection	Level 1 Triage	Monitoring / Alerting	Investigations	Incident Response	Compliance Reporting	Routine Log Reviews
Security	**80%** 3rd party intel, AIM	◐	MSSP	◐	●	●	○	○

● = Splunk fully in use ◐ = Splunk partially being used ○ = Splunk not being used

Refer to adoption charts for each team in the Appendix for more details

A $40B+ Retailer

Functional Adoption – Web Team

.Com Business Service	% Data Indexed	Log Collection	Incident Investigation		Root Cause Analysis	Proactive Alerting	Operational Dashboards	Business Analytics	Capacity Planning
			Level 1 Triage	Level 2 & 3 Escalation					
Web/App Server	100%	●	●	●	●	●	●	●	●
Database	0%	○	○	○	○	○	○	○	○
Virtualization	10%	◐	○	○	○	○	○	○	○
OS	100%	●	●	●	●	●	●	●	●
Storage	20%	◐	●	○	○	●	●	○	○
Network*	90%	◐	○	○	○	○	○	○	○

● = Splunk fully in use ◐ = Splunk partially being used ○ = Splunk not being used

NOTE: VMware data not ingested. Storage visibility is limited to VM instance. Host and SAN would be beneficial.
* Network data is being collected today but in a separate Splunk instance due to be joined later this year.

A $40B+ Retailer

Functional Adoption – Security Controls

Critical Control	In Place?
Monitor unauthorized devices or software	○
Monitor unmanaged devices or software	○
Monitor configuration compliance	○
Monitor patch compliance	●
Monitor malware defense	●
Monitor application software security	◐
Monitor wireless access control	◐
Analyze audit logs with time-based correlation	●

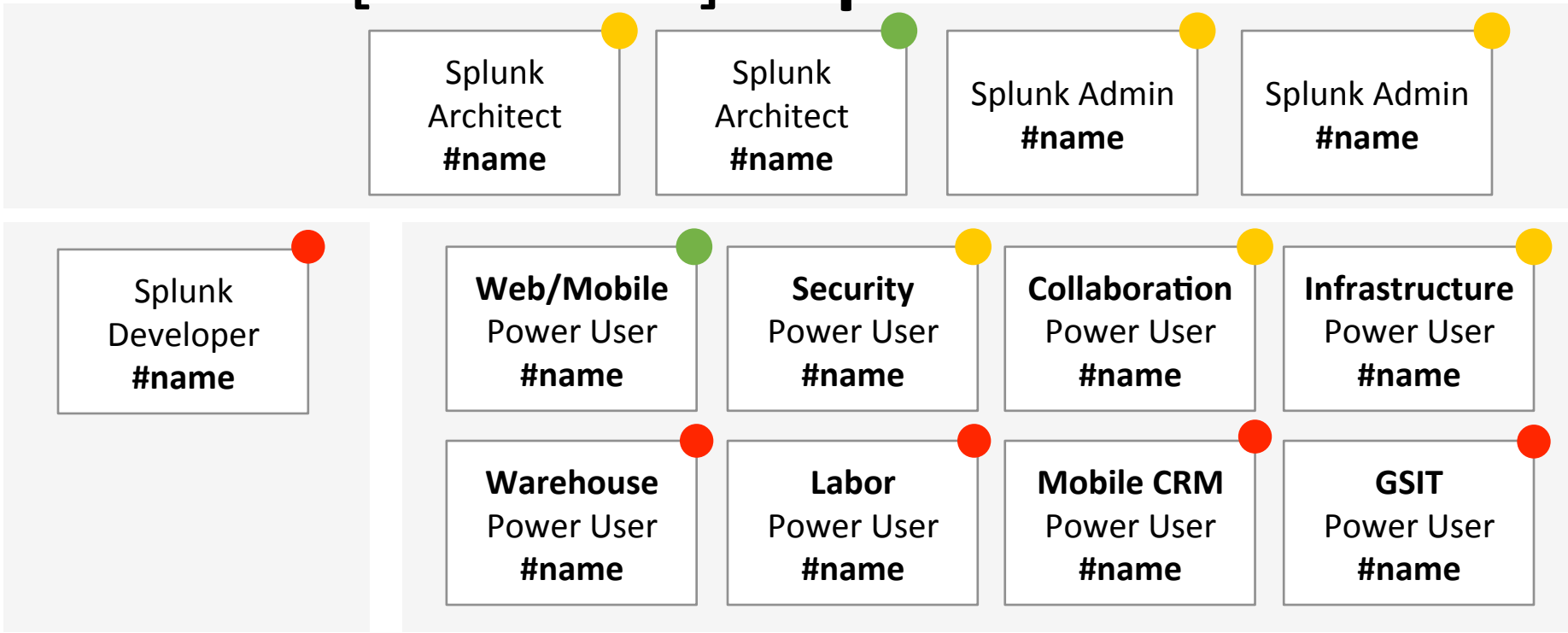
Critical Control	In Place?
Monitor use of ports, protocols, and services	●
Monitor controlled use of admin privileges	●
Monitor perimeter IDS	●
Monitor controlled / uncontrolled access	●
Monitor orphan, expired, miss use of accounts	○
Monitor potential exfiltration of information	●
Monitor secure IP restriction policies	●
Maintain data going back months	◐

● = Splunk fully in use ◐ = Splunk partially in use ○ = Splunk not in use

Current assessment of Splunk usage at [customer] for the SANS 20 security controls.

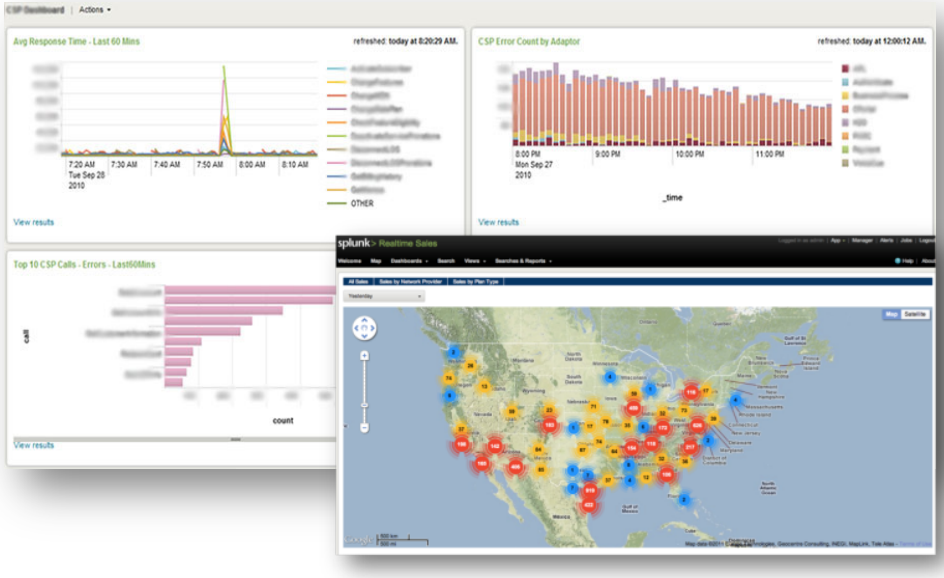
A $40B+ Retailer

[customer]'s **Splunk Team**



Real-time Operational Intelligence

- Splunk **reduced outage frequency 15%**, delivering an annual ROI of $1.3M
- Drives capacity and maintenance window planning
- Delivered executive dashboards showing activations by minute, by channel, by market, by device type in hours, not weeks or months



cricket communications

Ty Prikkhi
Senior Operations Manager

"In a matter of hours, Splunk lets us build dashboards to compare and correlate whatever we want—nothing else lets us do that."

Splunk **Application Support/Dev Benchmarks**

Know what to project and/or compare how you're doing

15% to **45%** reduction in application incidents

70% to **90%** faster investigation of QA defects and incidents

10% to **50%** faster time to market

10% to **50%** increase in value for key projects

eTravel

Reduced the number of incidents leading to 9M Euro per year in revenue recaptured

NBC UNIVERSAL

Went from 1 release/day to 8 because of Splunk

TESCO

Shortened their development cycles by 30%

A $40B+ Retailer

Future Value Opportunities (1 of 2)

A Proactive Operations approach will reduce impact hours
Collaboration to avoid 171,348 employee hours/year

19,725
Yearly Hours

$7.5M
Yearly Value

Collaboration

Incidents reduced **25%** | Impact **67%**
Avoiding **34 hours/yr** impact time
Value $5.2M/year | 1,501 IT hours/year

Basic monitoring puts **Collaboration at risk as it grows** from ~6k to 200k+ users and becomes the portal to key apps

Proactively monitor to avoid incidents and employee productivity loss (171k hrs)

Speed incident investigation and resolution, reducing manual effort

"We expect 20% more issues as we go from @6,000 to 200,000+ users."

Labor Scheduling

70% reduction in incident investigation
Sev1 time reduced **96 hours/year**
Value $433,544/year | 5,549 hours/year

Shift from reactive to proactive **improving Labor stability and availability** enabling maximum scheduling efficiency

Proactively monitor to avoid incidents and protect Partner productivity

Speed incident investigation and resolution, reducing manual effort

"Last Tuesday if we got a heads up from Splunk we could have resolved it in 1 hour instead of 5."

Warehouse

25% reduction in incidents
Avoiding **12 hours/year** impact time
Value $1.0M/year | 828 hours/year

Become more proactive further leveraging centralized, real-time data to avoid and reduce impact time

Proactively monitor to avoid incidents and business impact

Further reduce investigation effort over current, isolated log search solution

"If we had a dashboard showing us the app, database, server, and network health, we could get ahead of potential issues and resolve them before impact."

Best Practices for Gaining Executive Support

Taking your Splunk deployment to the next level

1

Align with Key Business Objectives

2

Qualify and Quantify Business Value

3

Incremental Steps with a Big Picture Plan

4

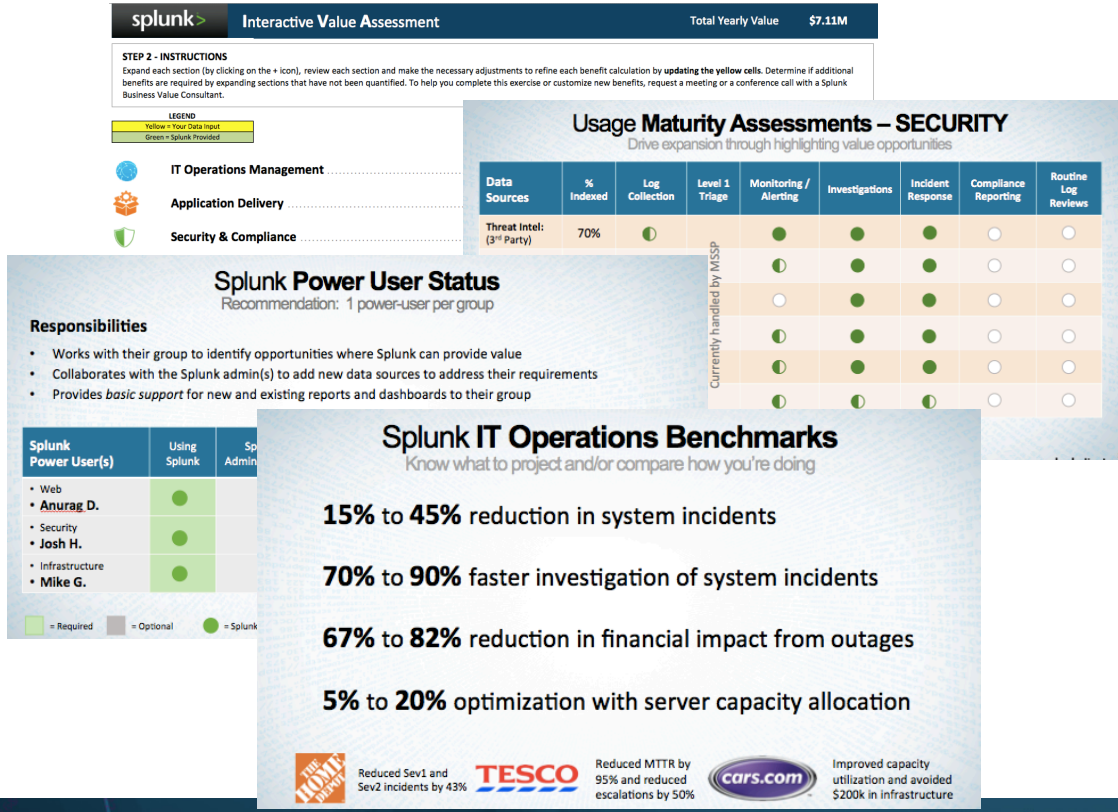
Measure, Track, and Report Your Success

Helping You **Gain Executive Support**

- Your Regional Sales Manager
- Your Splunk Partner
- A Splunk Business Value Consultant
- Your Splunk Advisory Engineer (SAE)

Ask Any of Us For…

- The Interactive Value Assessment (IVA) Excel model
- Usage adoption **maturity assessment** templates
- Splunk **staff readiness** templates
- Splunk common **benefits and benchmarks**



Thank you!

Doug May
AVP, Global Markets Specialization
dmay@splunk.com

splunk>