splunk> .conf2017

Center of Excellence Framework

A new approach on an old story.

Hans Skalle & David Zimmerman | Splunk Business Value & Customer Success

27 Sept 2017 | Washington, DC

Forward-Looking Statements

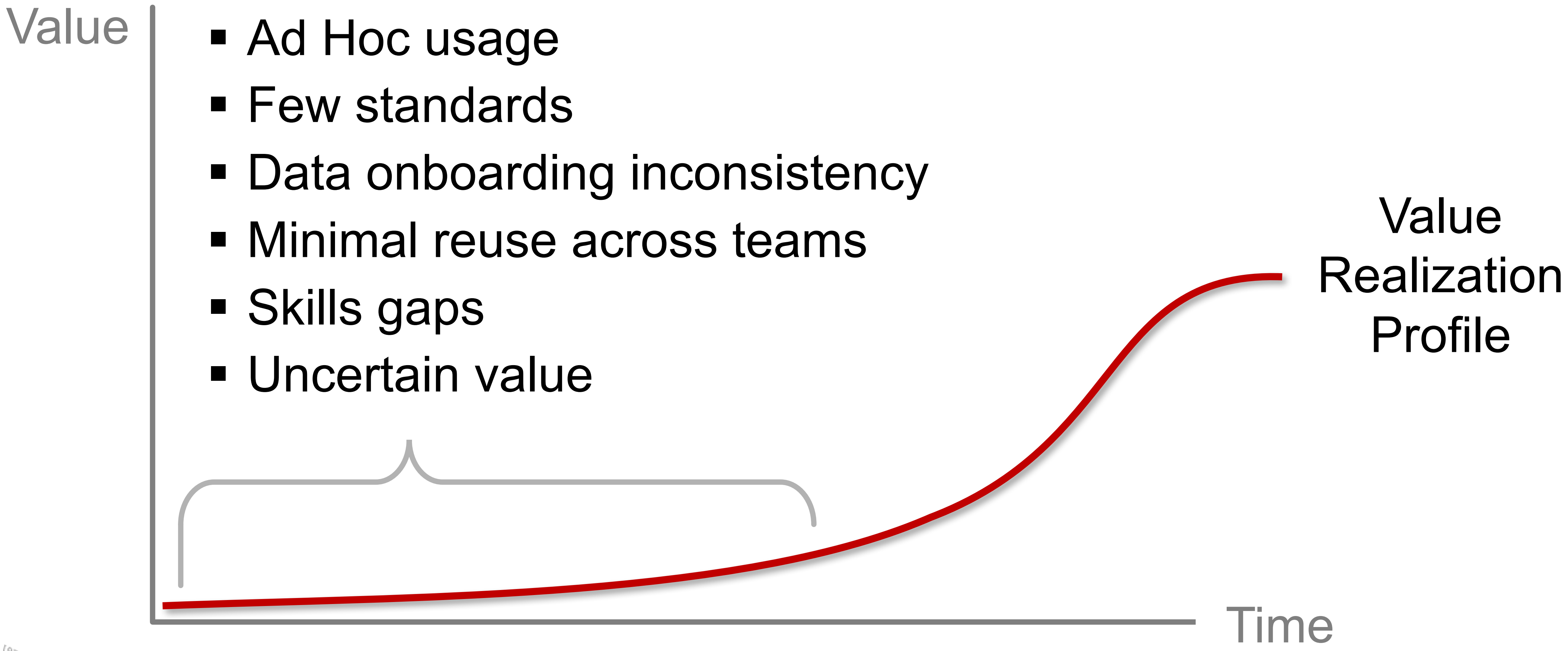
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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.

Why a Splunk CoE?

listen to your data

What We’ve Learned

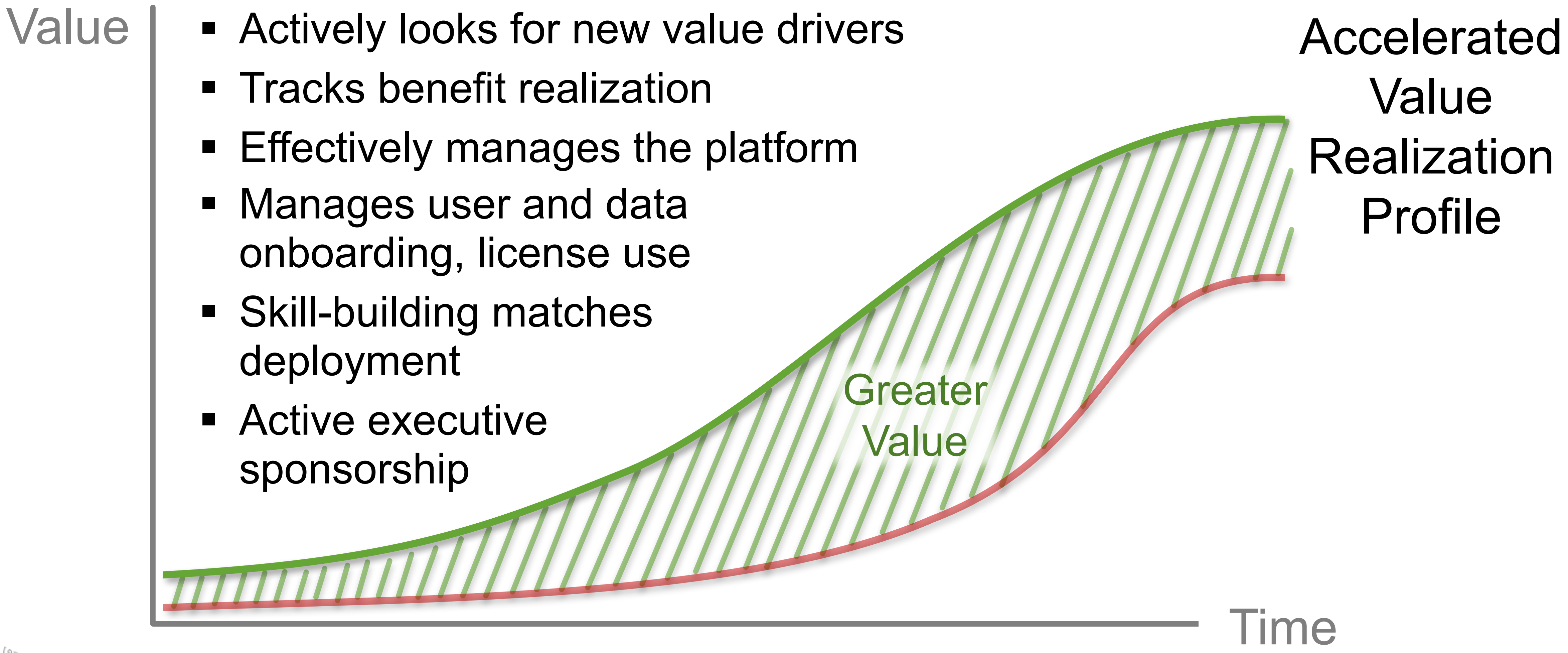


- Ad Hoc usage
- Few standards
- Data onboarding inconsistency
- Minimal reuse across teams
- Skills gaps
- Uncertain value

What We've Learned

Using best practices early to accelerate customer value and success

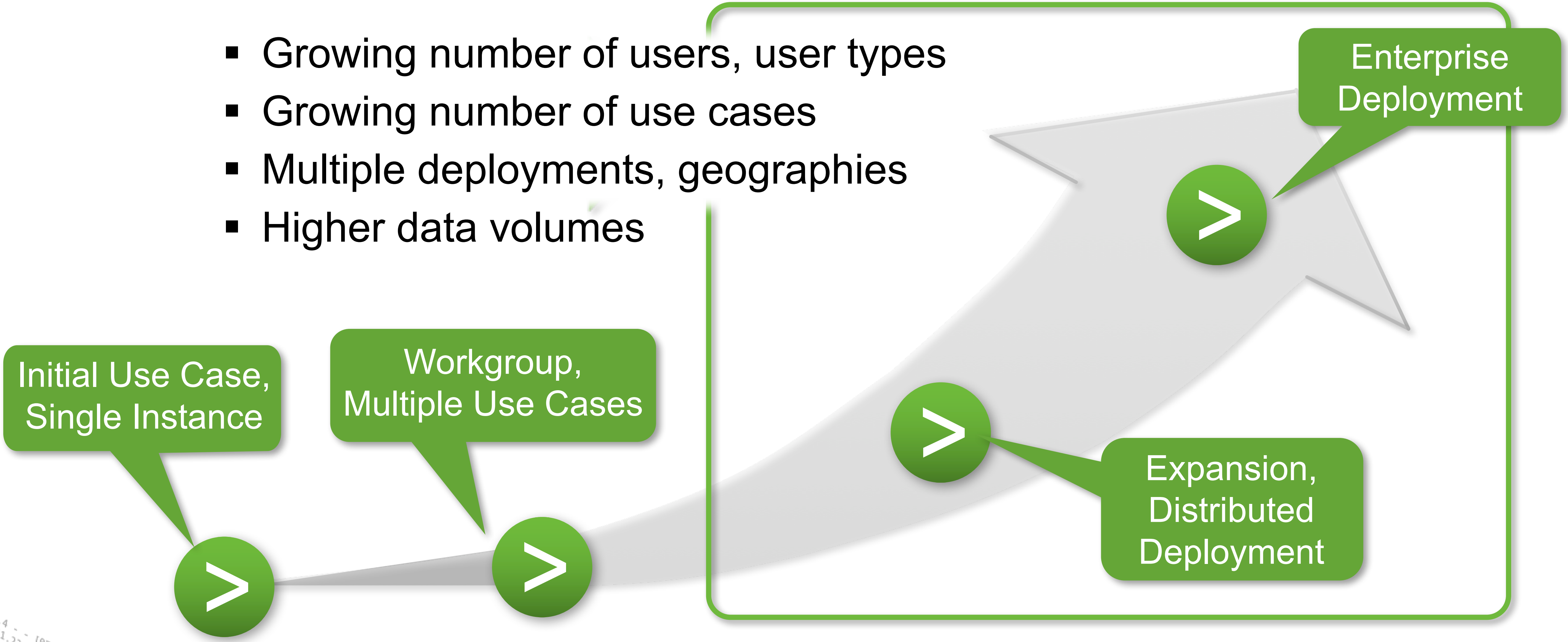
- Actively looks for new value drivers
- Tracks benefit realization
- Effectively manages the platform
- Manages user and data onboarding, license use
- Skill-building matches deployment
- Active executive sponsorship



When does a CoE Add Value?

A CoE can help reduce complexity and cost through best practices and reuse

- Growing number of users, user types
- Growing number of use cases
- Multiple deployments, geographies
- Higher data volumes

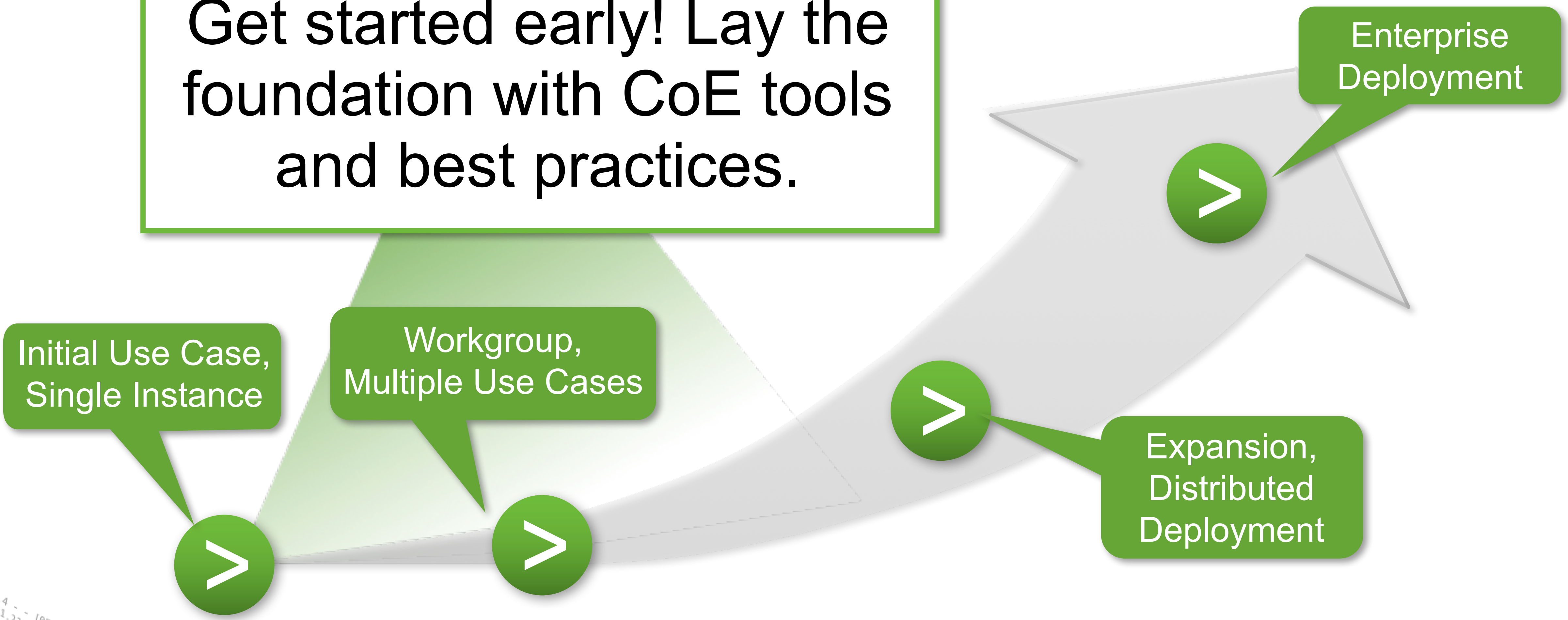

Initial Use Case, Single Instance
Workgroup, Multiple Use Cases
Expansion, Distributed Deployment
Enterprise Deployment

See Splunk Whitepaper: Building a Splunk Center of Excellence, 2017

When does a CoE Add Value?

A CoE can help reduce complexity and cost through best practices and reuse

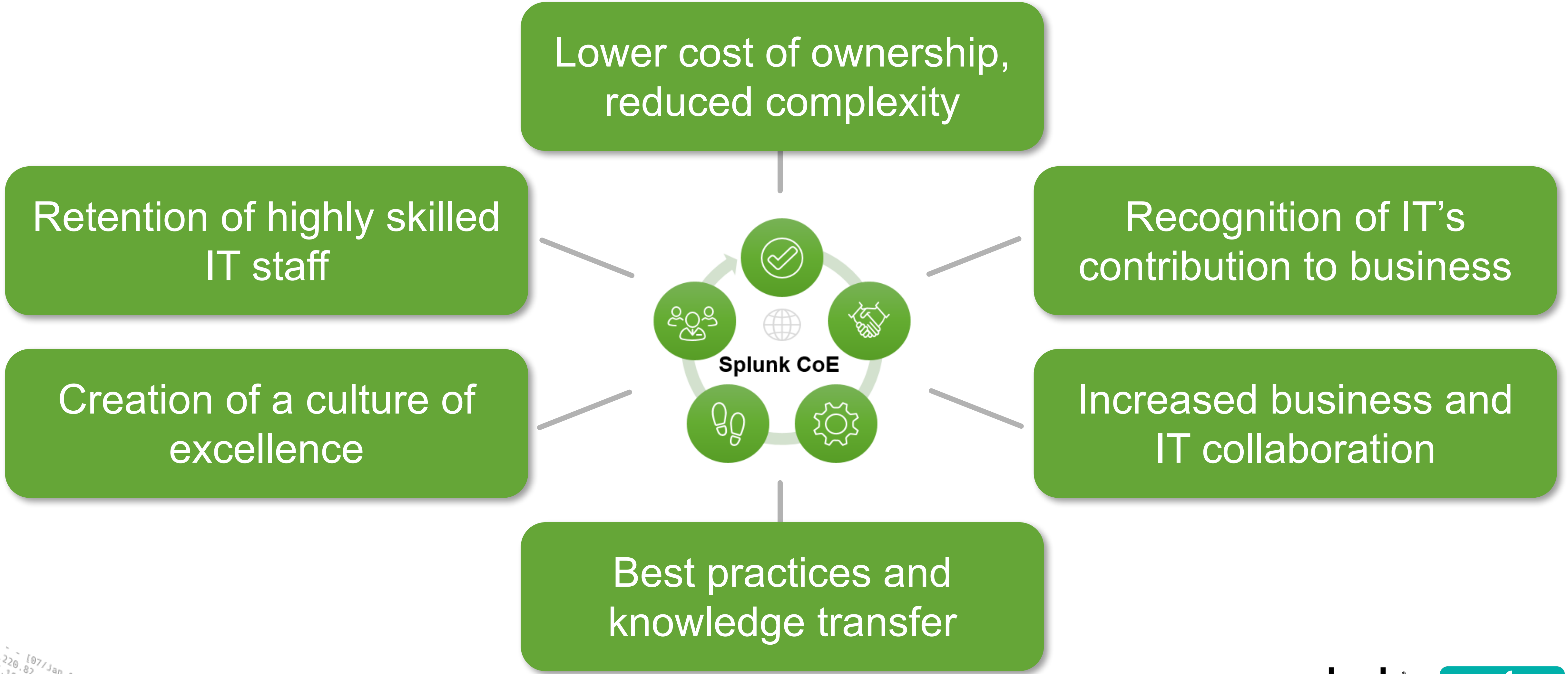
Get started early! Lay the foundation with CoE tools and best practices.


Initial Use Case, Single Instance
Workgroup, Multiple Use Cases
Expansion, Distributed Deployment
Enterprise Deployment

See Splunk Whitepaper: Building a Splunk Center of Excellence, 2017

Why a Splunk CoE?

The benefits of CoE best practices



Lower cost of ownership, reduced complexity

Retention of highly skilled IT staff

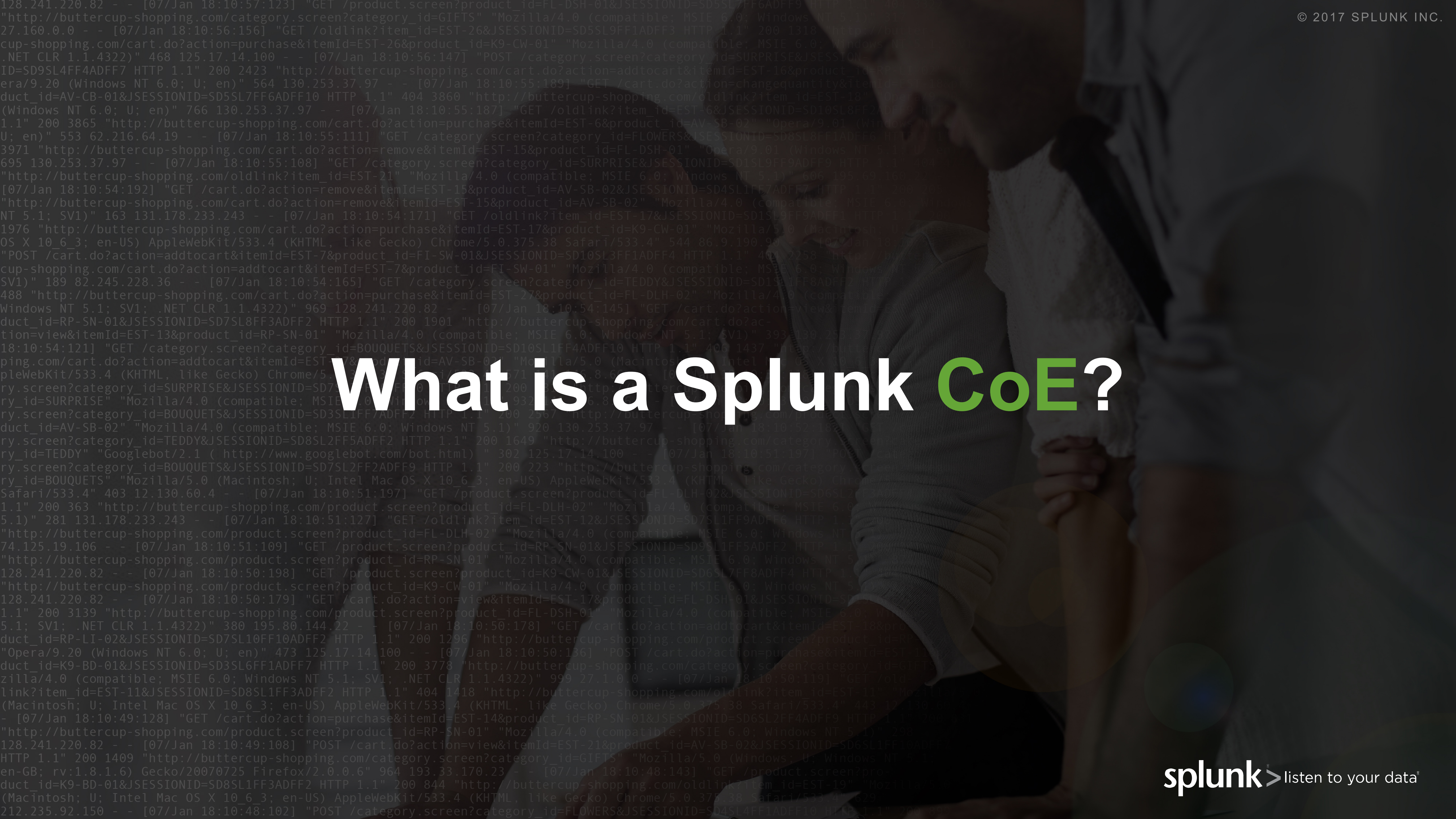
Recognition of IT's contribution to business

Creation of a culture of excellence

Increased business and IT collaboration

Best practices and knowledge transfer

See Splunk Whitepaper: Building a Splunk Center of Excellence, 2017



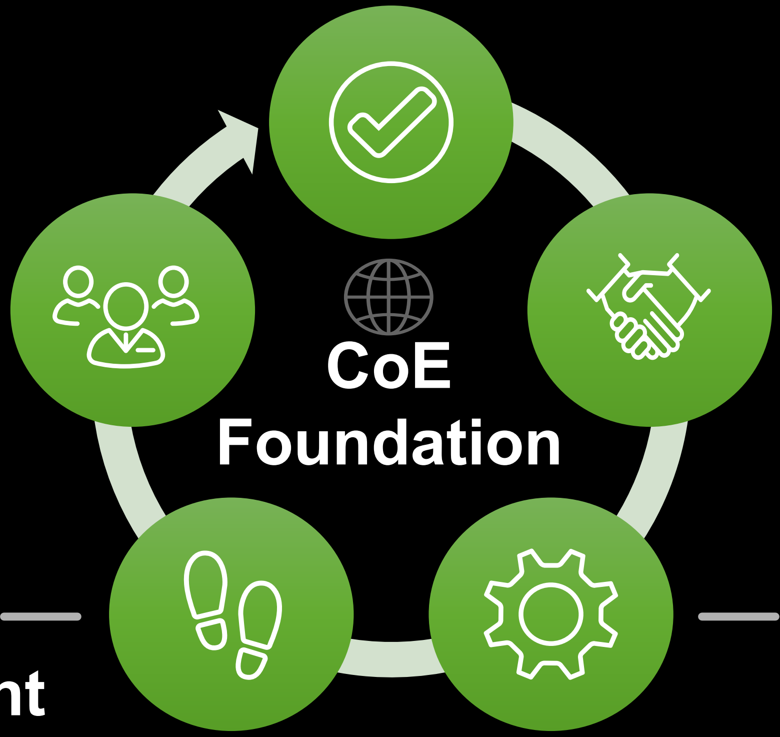
What is a Splunk CoE?

A best practices center focused on Splunk Governance, Operational Excellence, Enablement and Collaboration designed to accelerate and grow Business Value.

CoE Description

Splunk Center of Excellence

Six competencies supported by best practice accelerators



CoE Foundation

Business Value

- Business-driven objectives
- Value Realization

Governance

- Standards and processes
- Decision-making

Operational Excellence

- Deployment and maintenance
- Support

User Enablement

- Orientation
- Education and empowerment

Collaboration

- Community
- Sharing

What does a CoE do?

Supporting Competencies

- CoE Foundation Services
- Business Value
- Governance
- Operational Excellence
- Enablement
- Collaboration

- Platform Mgmt.
- Data Lifecycle Mgmt.
- User Lifecycle Mgmt.
- KO and App Lifecycle Mgmt.
- Use Case Lifecycle Mgmt.
- Exec Interlock
- Program Mgmt.

Best practice-based capabilities that include tools, techniques, standards, processes and oversight

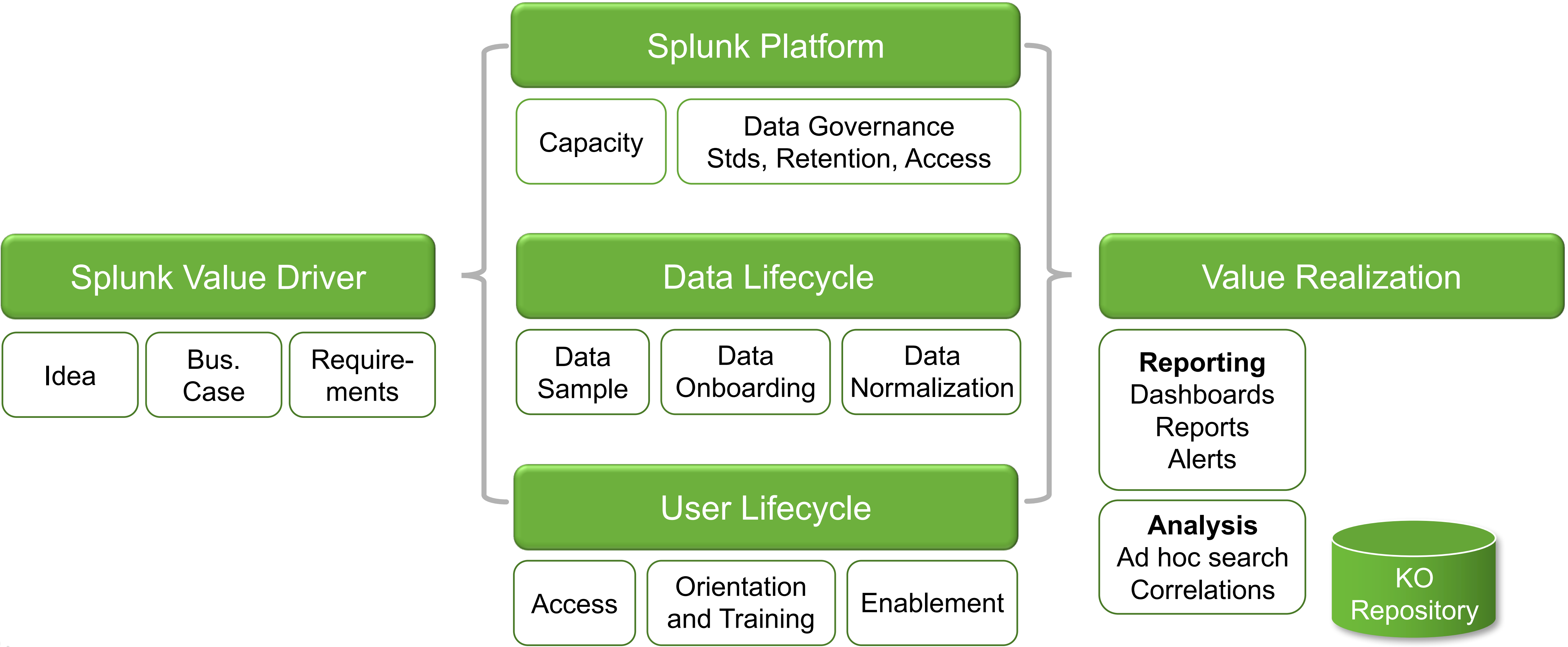
	Supporting Competencies				
CoE Foundation Services	Business Value	Governance	Operational Excellence	Enablement	Collaboration
Platform Mgmt.	▪ ROI/TCO ▪ Cost mgmt.	▪ Change control ▪ Service levels ▪ Chargeback ▪ License mgmt.	▪ Design ▪ Capacity mgmt. ▪ Deployment ▪ Maintenance ▪ Staffing	▪ Support triage ▪ Help Desk	▪ Search peering
Data Lifecycle Mgmt.					
User Lifecycle Mgmt.					
KO and App Lifecycle Mgmt.					
Use Case Lifecycle Mgmt.					
Exec Interlock					
Program Mgmt.					

	Supporting Competencies				
CoE Foundation Services	Business Value	Governance	Operational Excellence	Enablement	Collaboration
Platform Mgmt.					
Data Lifecycle Mgmt.	▪ Data Source Assessment	▪ Retention policies ▪ Data access ▪ CIM compliance	▪ Data discovery ▪ Data on-boarding ▪ Data security	▪ OOTB KOs ▪ Sandbox	▪ Correlations ▪ Data availability announcement
User Lifecycle Mgmt.					
KO and App Lifecycle Mgmt.					
Use Case Lifecycle Mgmt.					
Exec Interlock					
Program Mgmt.					

	Supporting Competencies				
CoE Foundation Services	Business Value	Governance	Operational Excellence	Enablement	Collaboration
Platform Mgmt.					
Data Lifecycle Mgmt.					
User Lifecycle Mgmt.	▪ Adoption ▪ User KPIs	▪ Roles and Responsibilities ▪ Capability	▪ RBAC ▪ Account Creation	▪ Orientation ▪ Education	▪ User Group ▪ Community Portal
KO and App Lifecycle Mgmt.					
Use Case Lifecycle Mgmt.					
Exec Interlock					
Program Mgmt.					

For more: CoE@splunk.com

Using the CoE to streamline your Path to Production



Splunk Value Driver

Idea

Bus. Case

Require-ments

Splunk Platform

Capacity

Data Governance
Stds, Retention, Access

Data Lifecycle

Data Sample

Data Onboarding

Data Normalization

User Lifecycle

Access

Orientation and Training

Enablement

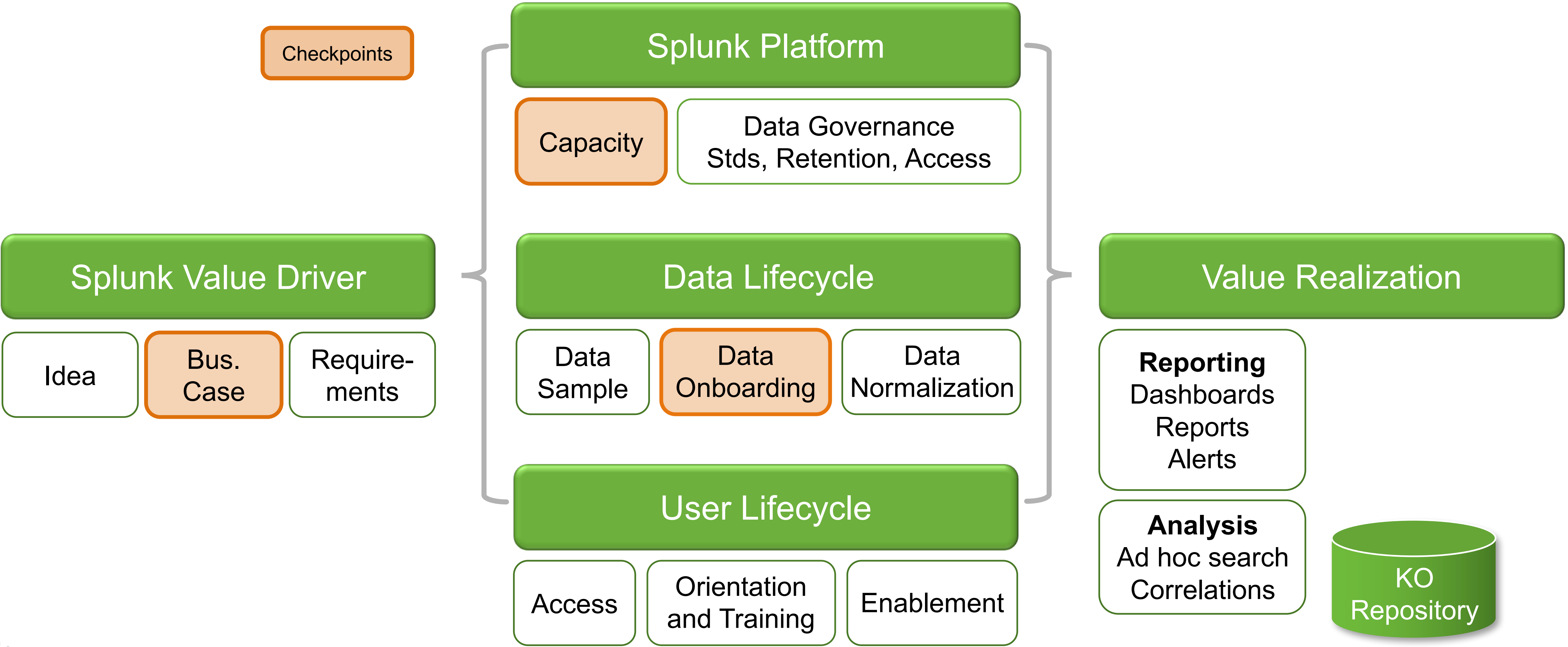
Value Realization

Reporting
Dashboards
Reports
Alerts

Analysis
Ad hoc search
Correlations

KO Repository

Using the CoE to streamline your Path to Production



Checkpoints

Splunk Value Driver

Idea

Bus. Case

Require-ments

Splunk Platform

Capacity

Data Governance
Stds, Retention, Access

Data Lifecycle

Data Sample

Data Onboarding

Data Normalization

User Lifecycle

Access

Orientation and Training

Enablement

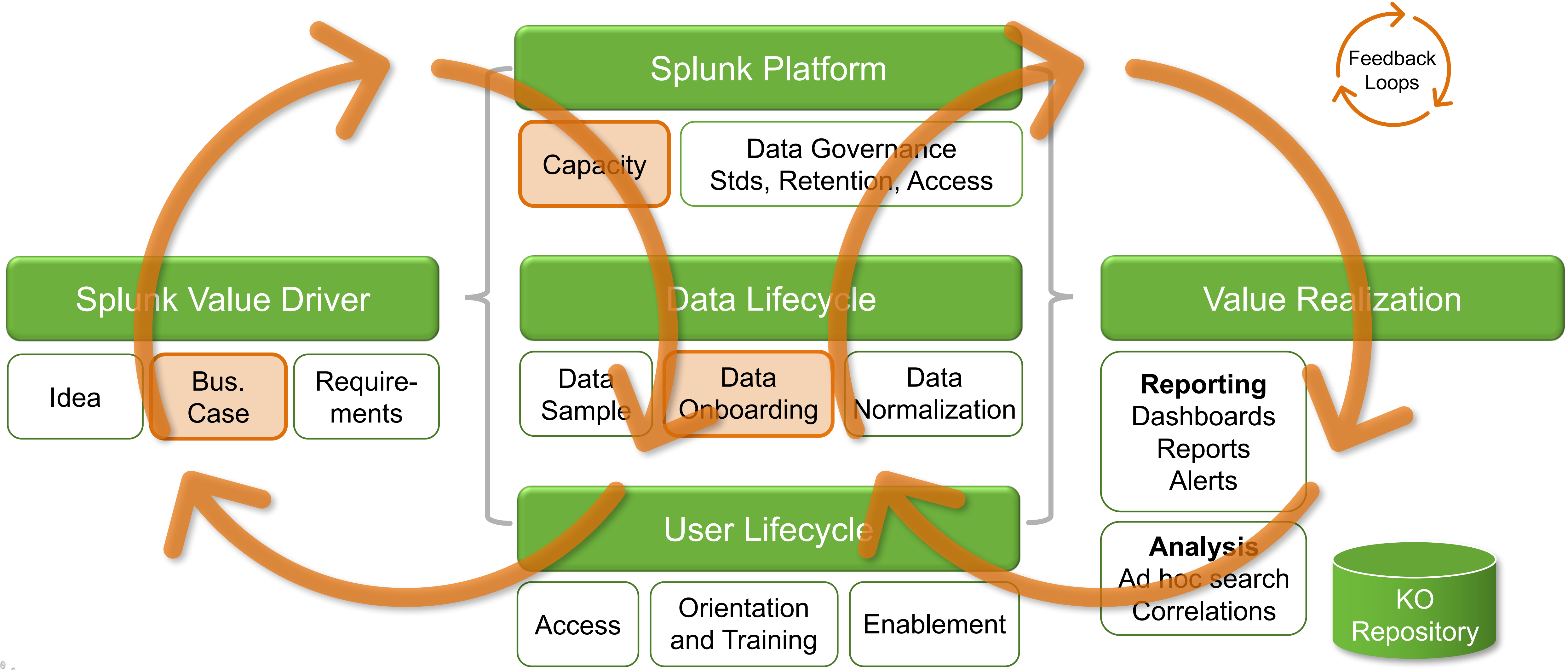
Value Realization

Reporting
Dashboards
Reports
Alerts

Analysis
Ad hoc search
Correlations

KO Repository

Using the CoE to streamline your Path to Production



Feedback Loops

Splunk Value Driver
- Idea
- Bus. Case
- Require-ments

Splunk Platform
- Capacity
- Data Governance Stds, Retention, Access

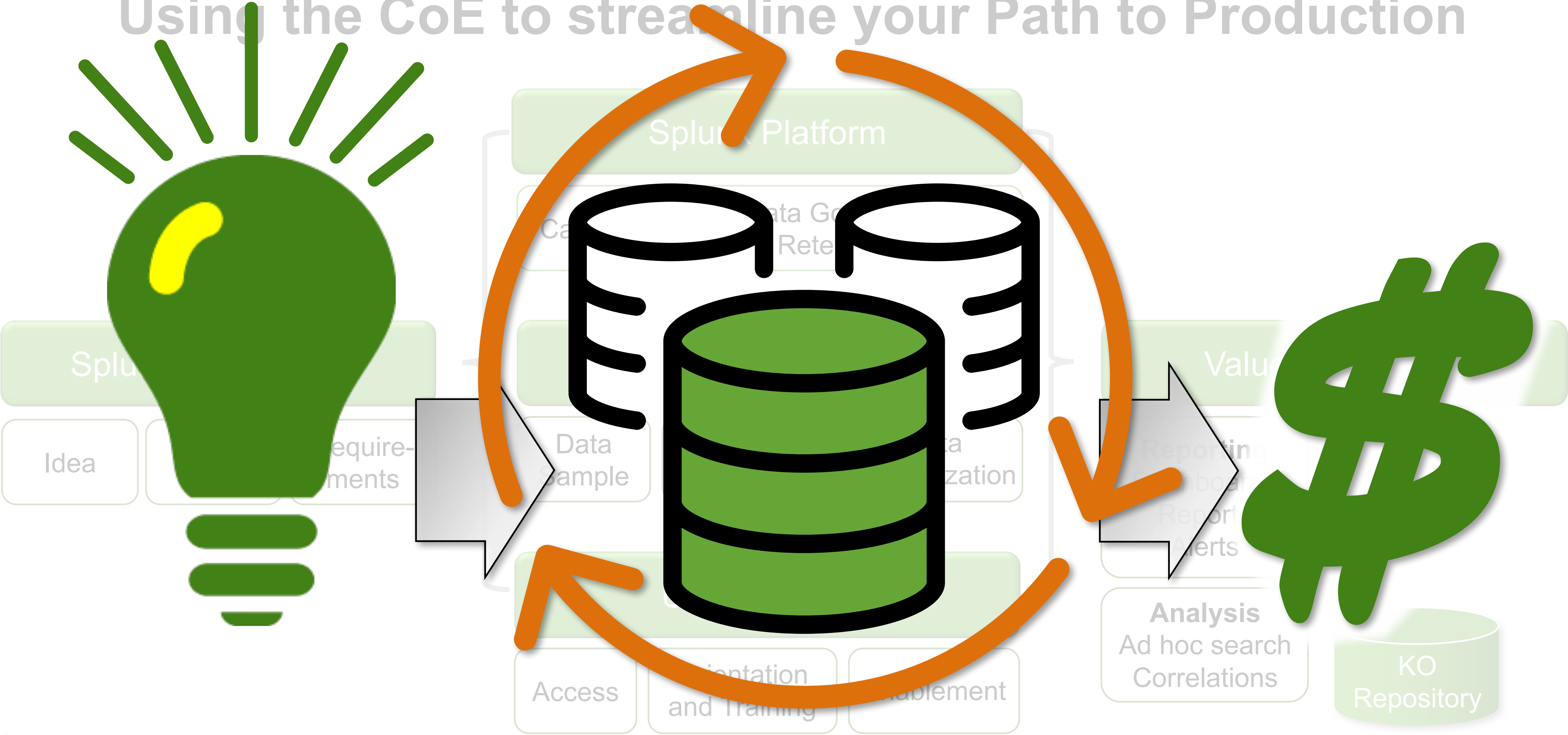
Data Lifecycle
- Data Sample
- Data Onboarding
- Data Normalization

User Lifecycle
- Access
- Orientation and Training
- Enablement

Value Realization
- **Reporting** Dashboards Reports Alerts
- **Analysis** Ad hoc search Correlations

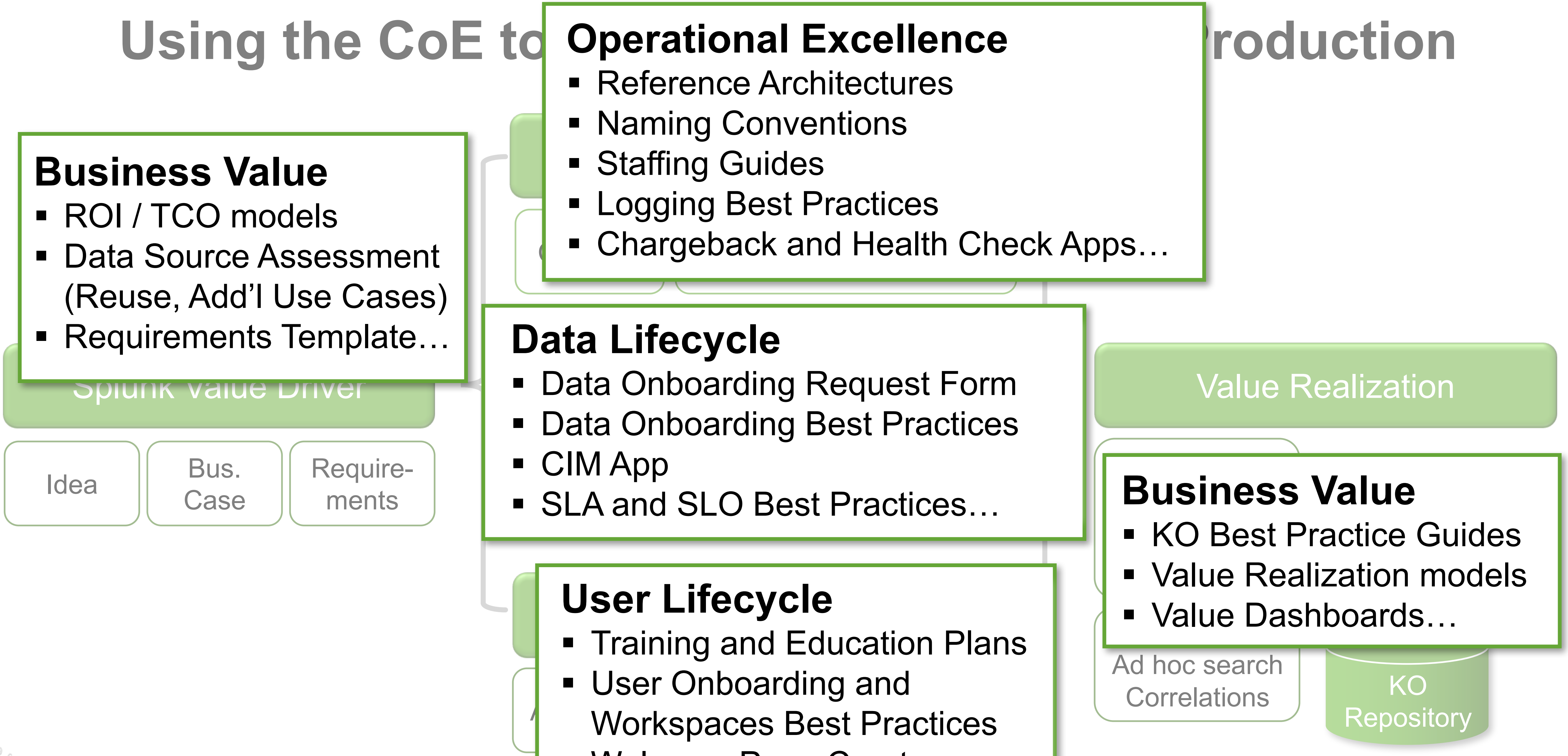
KO Repository

Using the CoE to streamline your Path to Production



Making machine data accessible, usable and (more quickly) valuable to your organization.

Using the CoE to … roduction



Business Value

- ROI / TCO models
- Data Source Assessment (Reuse, Add’l Use Cases)
- Requirements Template…

Operational Excellence

- Reference Architectures
- Naming Conventions
- Staffing Guides
- Logging Best Practices
- Chargeback and Health Check Apps…

Data Lifecycle

- Data Onboarding Request Form
- Data Onboarding Best Practices
- CIM App
- SLA and SLO Best Practices…

User Lifecycle

- Training and Education Plans
- User Onboarding and Workspaces Best Practices
- Welcome Page Creator
- Newsletter App…

Business Value

- KO Best Practice Guides
- Value Realization models
- Value Dashboards…

CoE Foundation

COE Foundational Components

Executive Sponsorship

- Owner
- Empowerment
- Aligned with business objectives

CoE Structure

- Centralized
- Federated
- Hybrid

CoE Operating Model

- Roles and responsibilities
- Communication
- Functional areas

Executive Charter

- Mission
- Roadmap

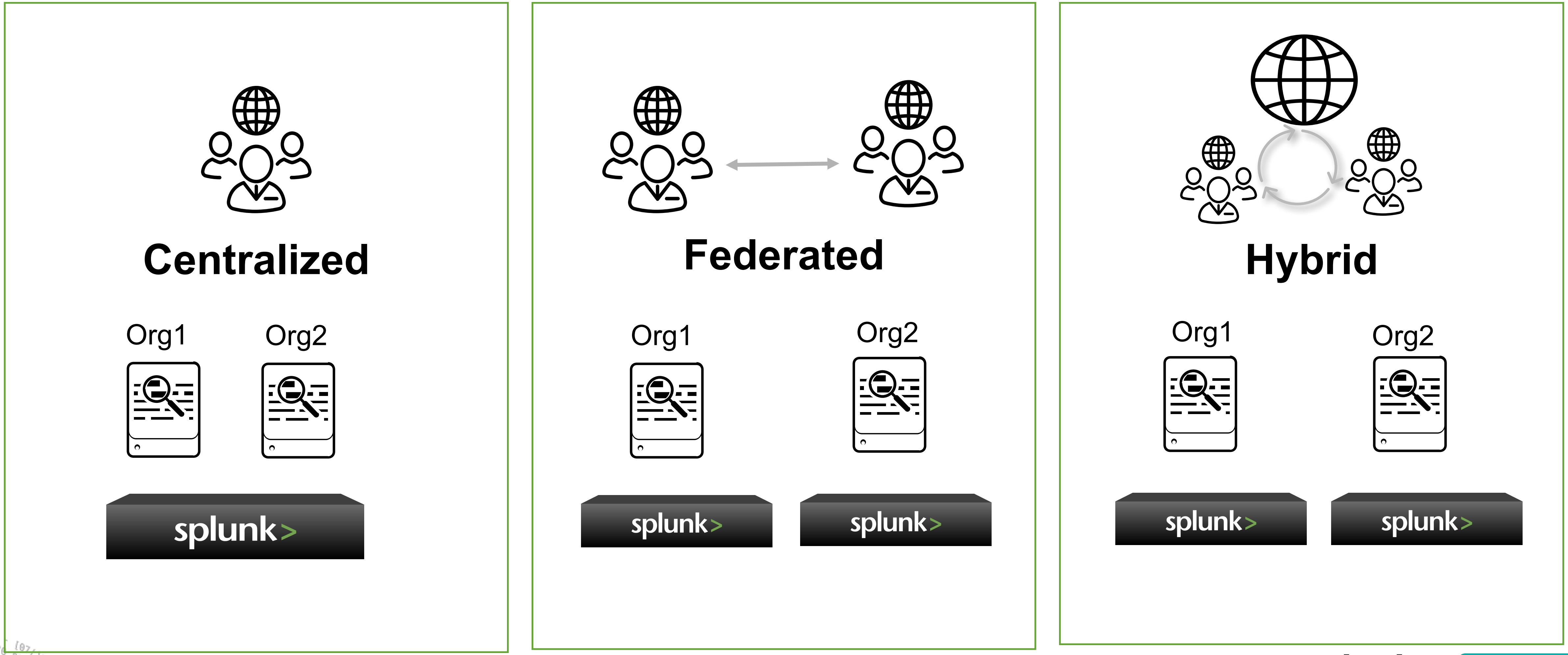
Program Management

- End-to-end oversight
- Priorities
- Governance
- Project Management

CoE Metrics

- Quantified success
- KPIs and SLAs
- Value dashboards

COE Structure



Centralized

Org1 Org2

splunk>

Federated

Org1 Org2

splunk> splunk>

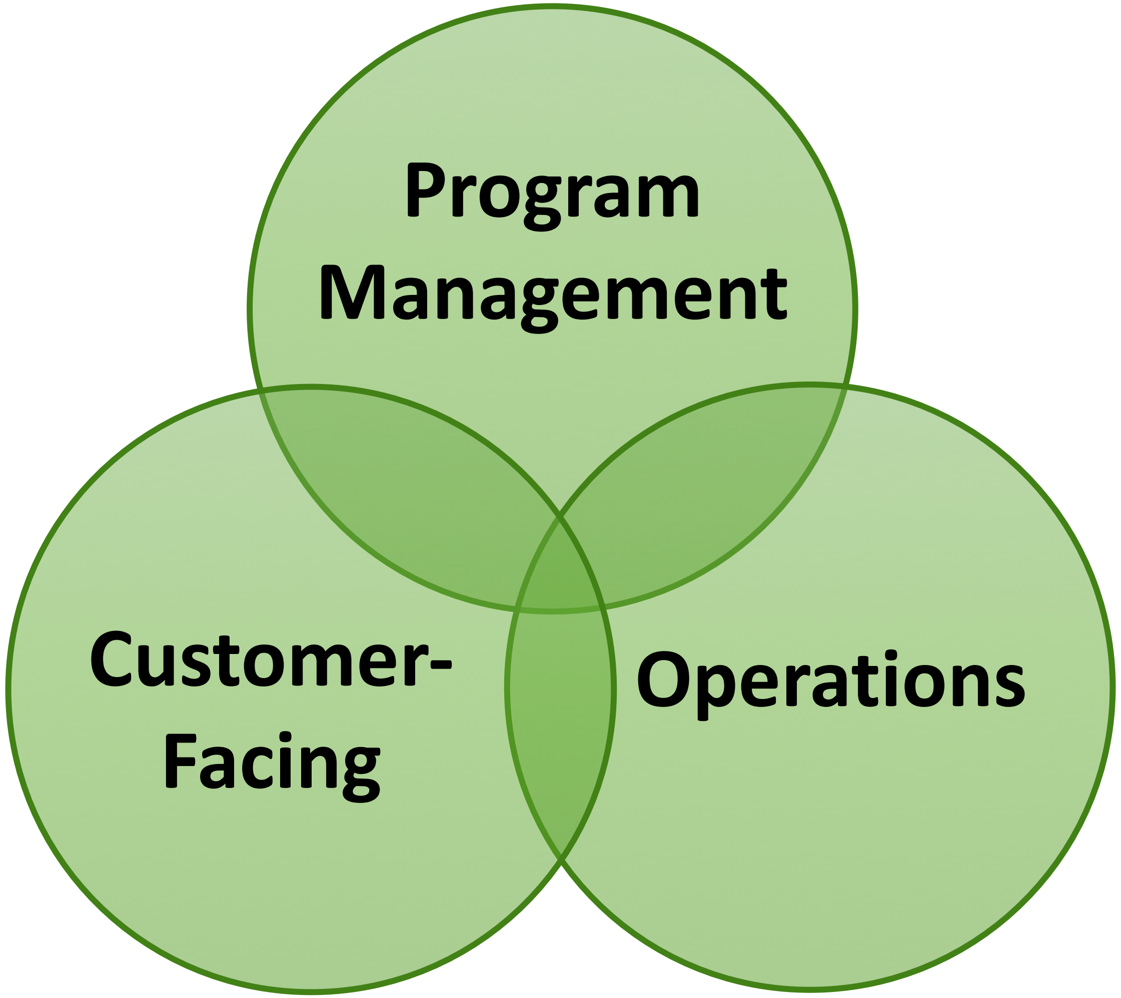
Hybrid

Org1 Org2

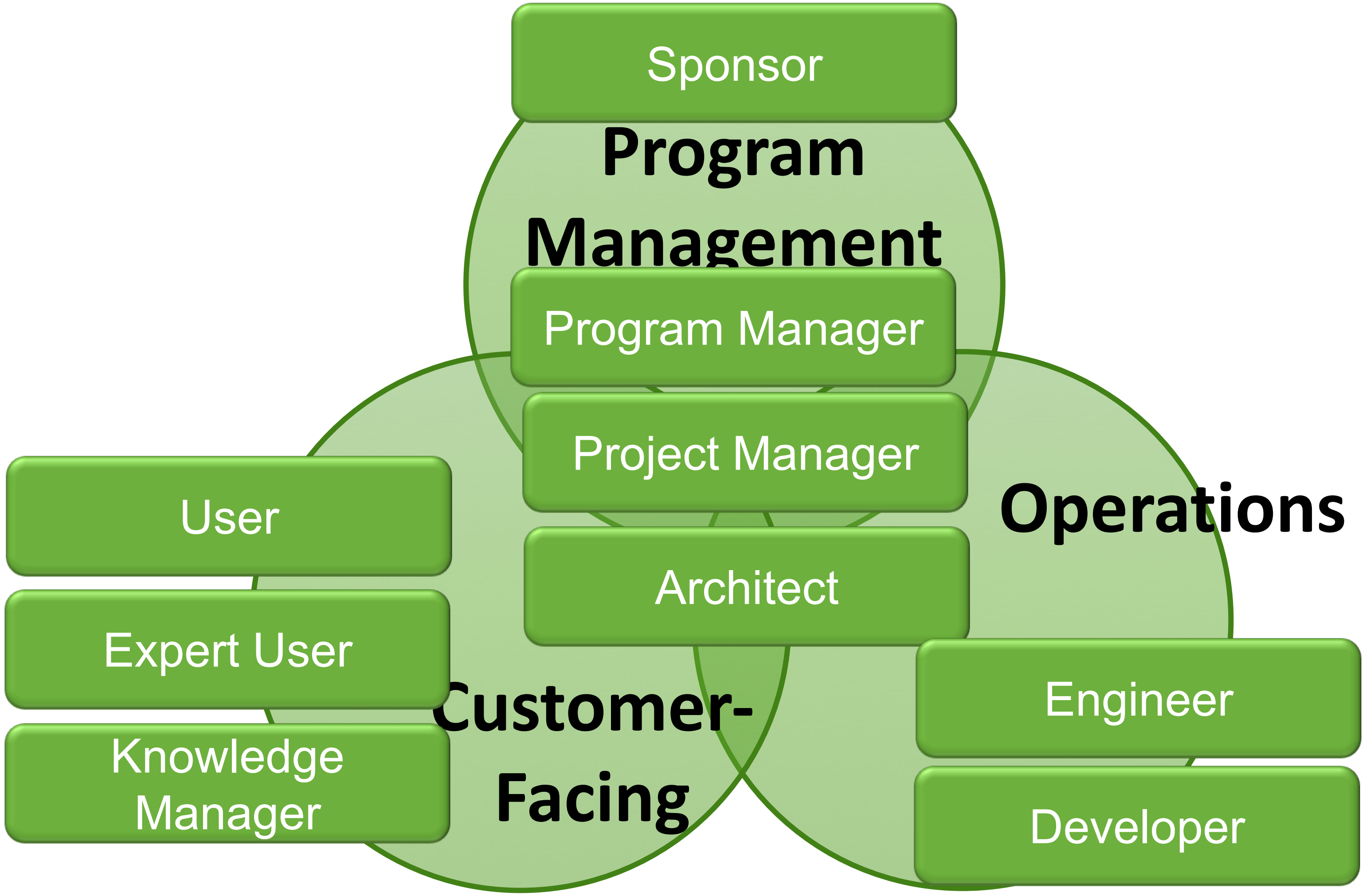
splunk> splunk>

Splunk CoE Operating Model

- Sponsor
- Program Manager
- Architect
- Engineer
- Developer
- Expert User
- User
- Knowledge Manager
- Project Manager



Splunk CoE Operating Model



Sponsor

Program Management

Program Manager

Project Manager

Architect

Operations

Engineer

Developer

User

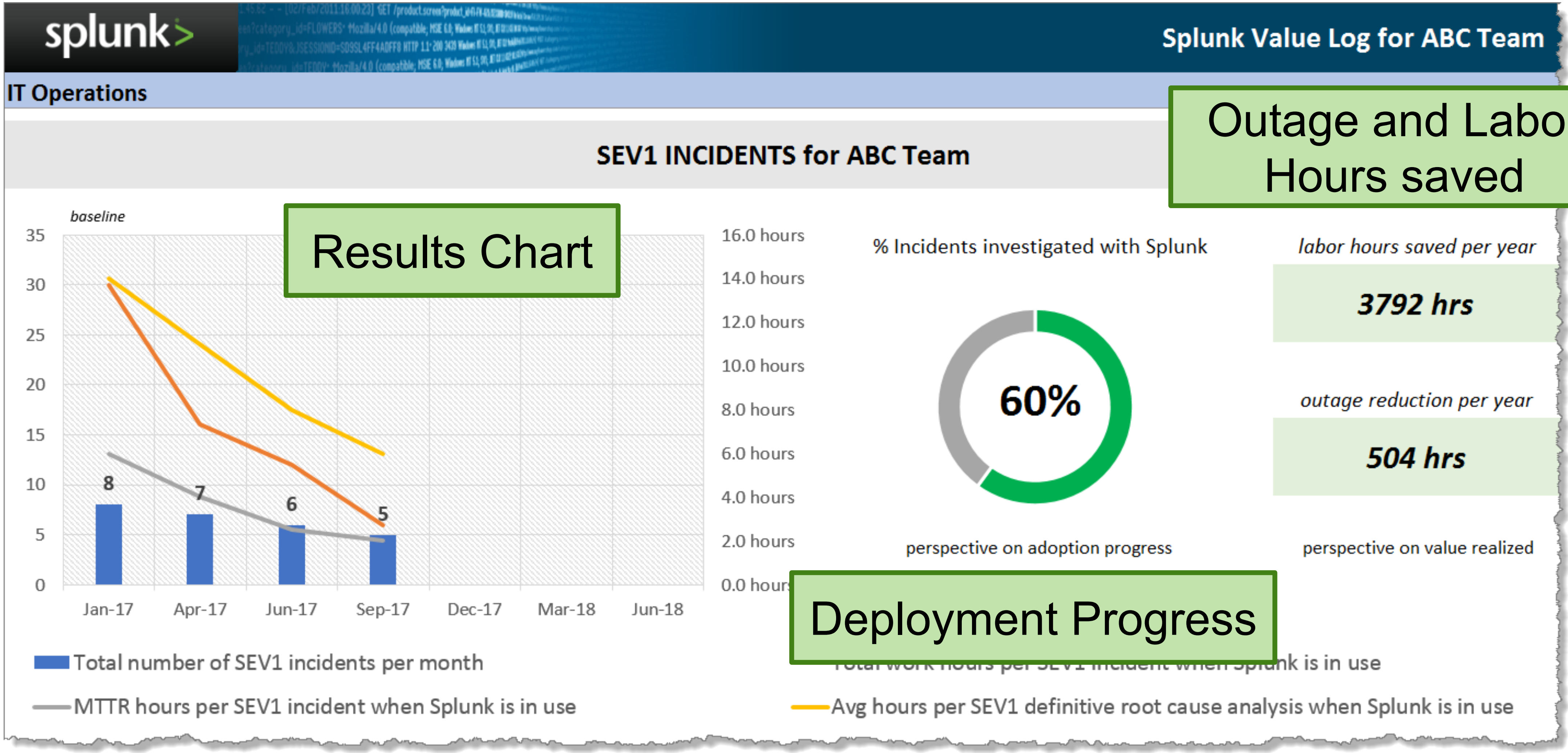
Expert User

Knowledge Manager

Customer-Facing

Tracking Value Realization

Value Dashboards provide visibility into progress and results



Splunk Value Log for ABC Team

IT Operations

SEV1 INCIDENTS for ABC Team

% Incidents investigated with Splunk

perspective on adoption progress

labor hours saved per year

3792 hrs

outage reduction per year

504 hrs

perspective on value realized

▬ Total number of SEV1 incidents per month

▬ Total work hours per SEV1 incident when Splunk is in use

▬ MTTR hours per SEV1 incident when Splunk is in use

▬ Avg hours per SEV1 definitive root cause analysis when Splunk is in use

Outage and Labor Hours saved

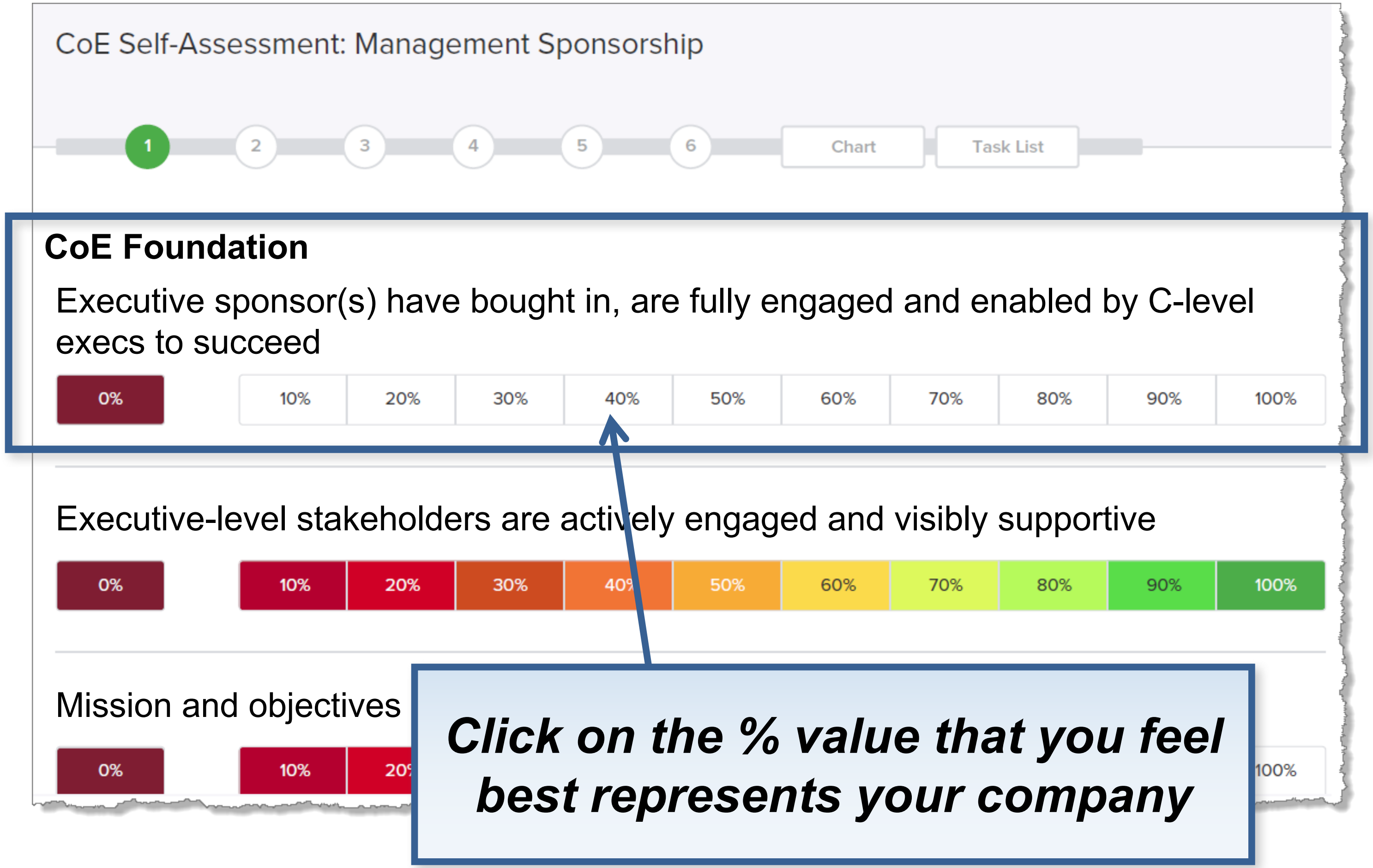
Results Chart

Deployment Progress

Building a CoE

CoE Self Assessment

Use this to learn more and establish a baseline for best practice-based improvement



CoE Self-Assessment: Management Sponsorship

CoE Foundation

Executive sponsor(s) have bought in, are fully engaged and enabled by C-level execs to succeed

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Executive-level stakeholders are actively engaged and visibly supportive

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Mission and objectives

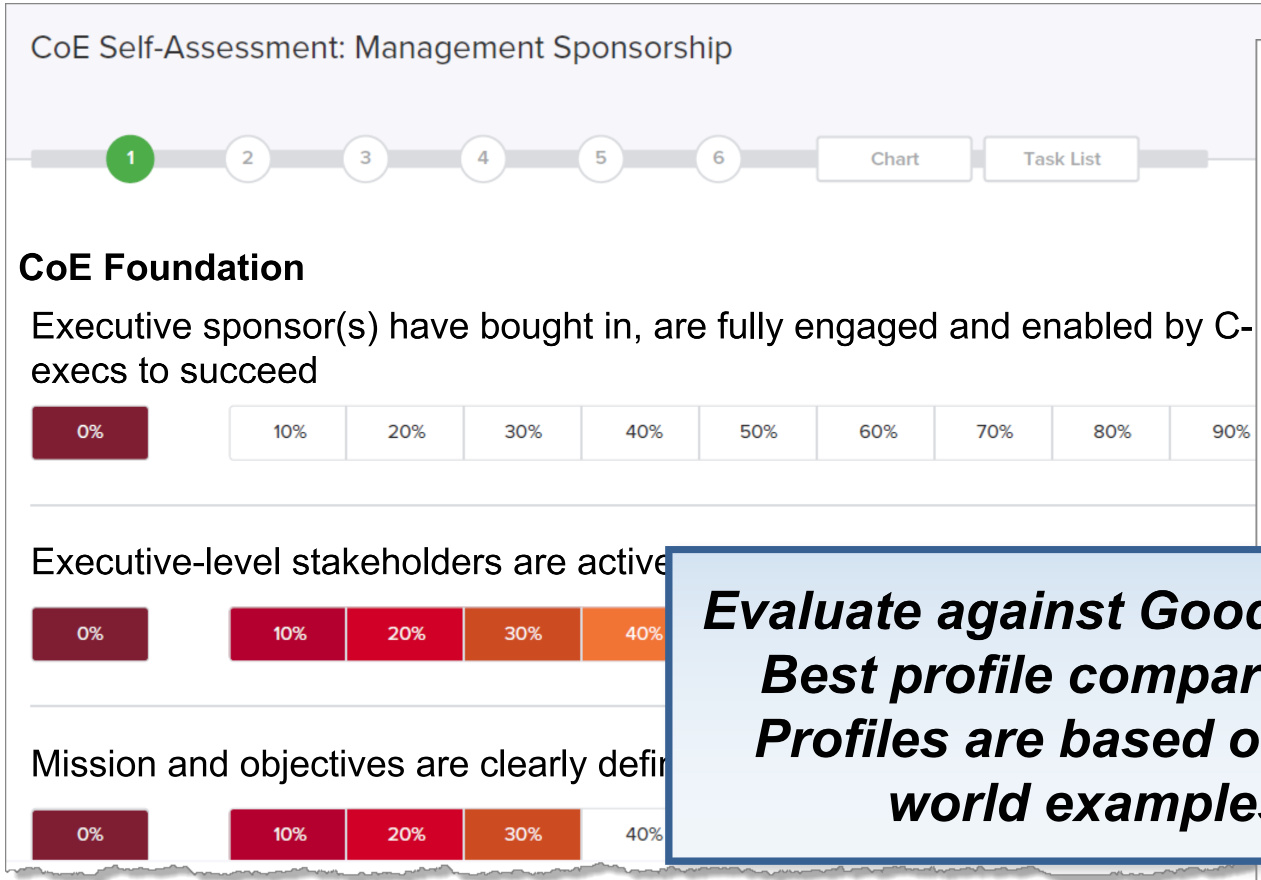
0% 10% 20% 100%

Click on the % value that you feel best represents your company

- 8-10 Questions in each competency area
- Questions map to successful best practices
- Establishes a baseline, gives visibility to gaps
- Helps identify your priorities to build an action plan

CoE Self Assessment

Use this to learn more and establish a baseline for best practice-based improvement



CoE Self-Assessment: Management Sponsorship

CoE Foundation

Executive sponsor(s) have bought in, are fully engaged and enabled by C-execs to succeed

0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90%

Executive-level stakeholders are active

0% | 10% | 20% | 30% | 40%

Mission and objectives are clearly defi

0% | 10% | 20% | 30% | 40%

Evaluate against Good, Better, Best profile comparisons. Profiles are based on real-world examples

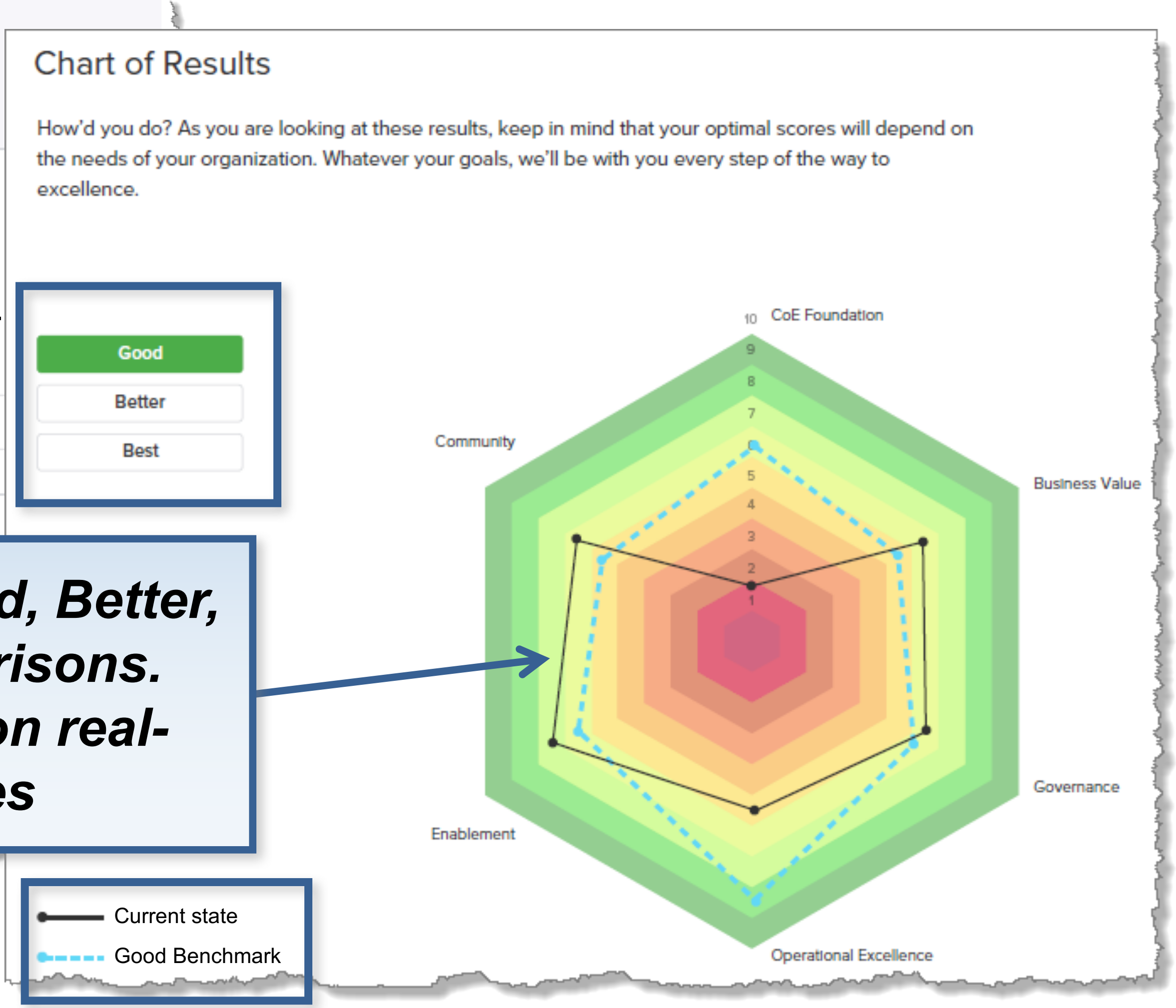
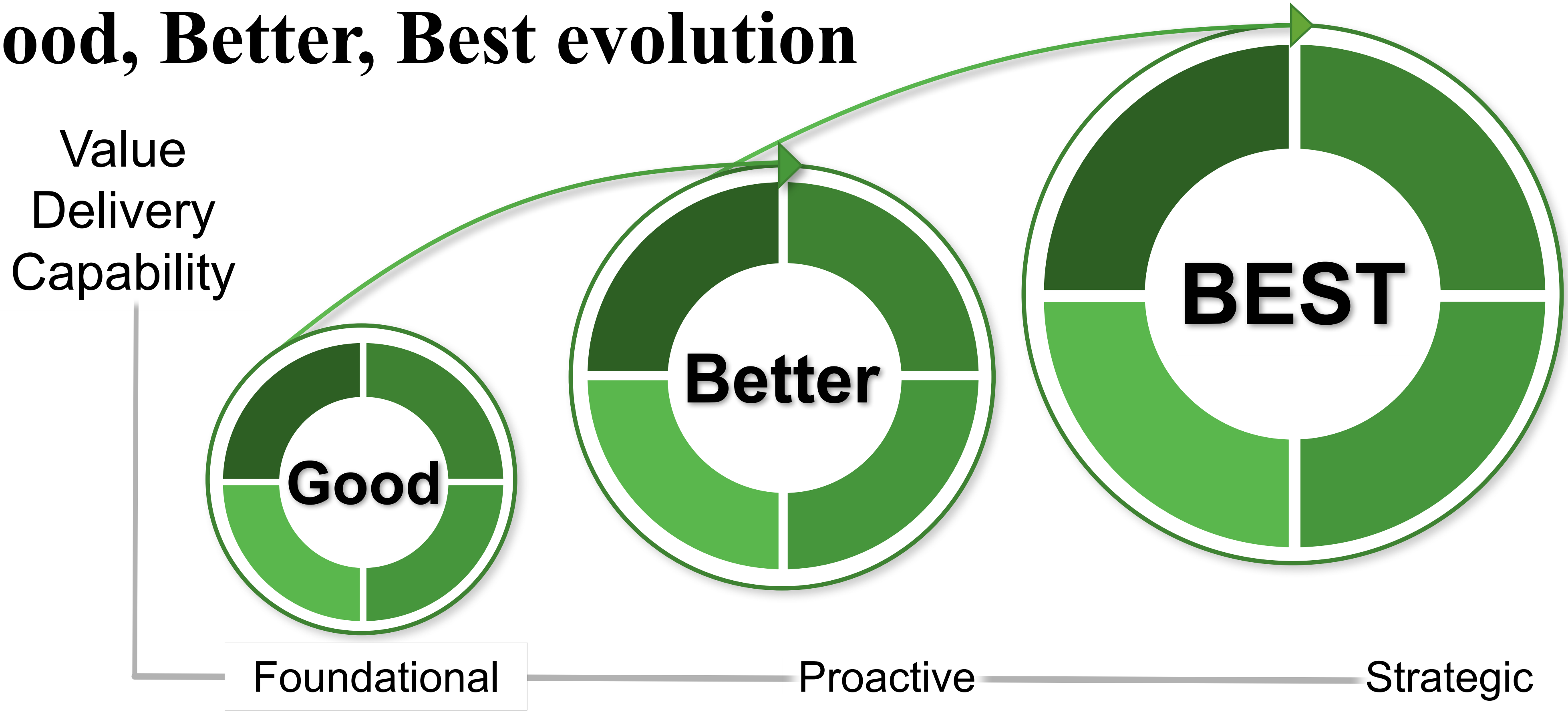


Chart of Results

How'd you do? As you are looking at these results, keep in mind that your optimal scores will depend on the needs of your organization. Whatever your goals, we'll be with you every step of the way to excellence.

Good, Better, Best evolution



Value Delivery Capability

Good

Better

BEST

Foundational

Proactive

Strategic

Data Onboarding

User Onboarding

Automation & Self-Service

Welcome Page Creator

Newsletter App

Business-Driven New Value Creation

KO Repository/User Groups

Customer Story

Splunk CoE Success Story

> 4TB Customer

Primary Use Cases: Security, IT Operations, Compliance

300+ Users

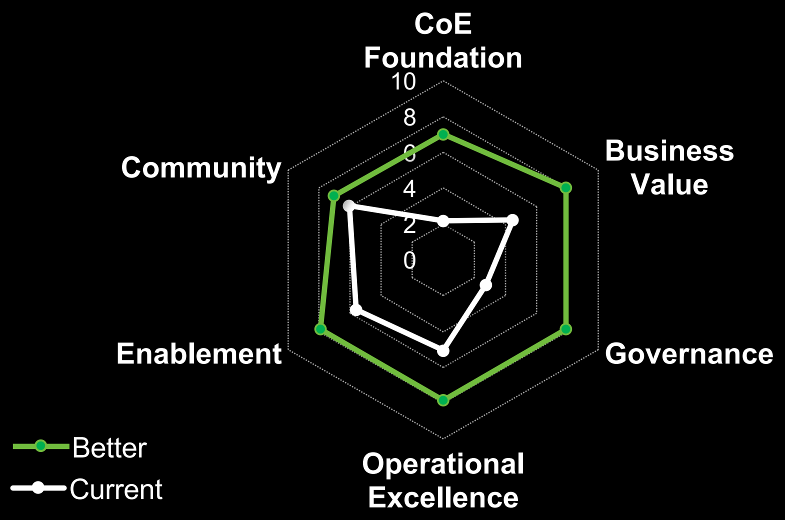
50 Clustered Indexers

500K Searches/Day

8 Search Heads

> Deployment Challenges

- Data Onboarding: Weeks/Months
  > Became Days
- Search Performance: Minutes
  > Became Seconds
- Notable Events
  > Became Actionable Alerts



● CoE: No Splunk Owner ***> Exec Sponsor, Program Mgr.***

● Business Value: Security posture ***> Priorities & Reqmts.***

● Governance: Data governance ***> CIM Compliance, Retention***

● Ops: Good staffing and platform resources

● Enablement: Good User onboarding and training plan

● Collaboration: Central repository and User Groups

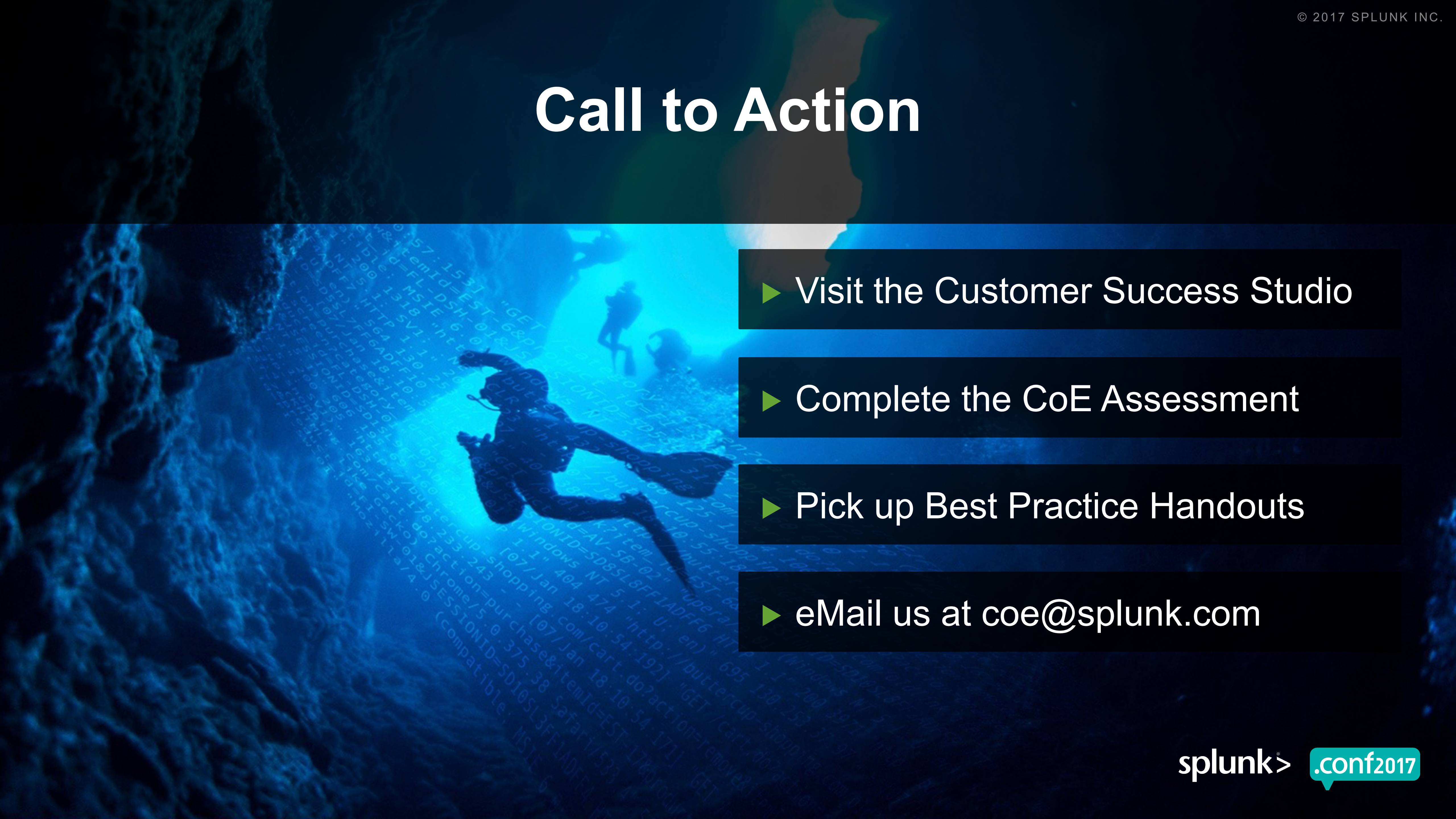
Making machine data accessible, usable and valuable to everyone.

splunk> .conf2017

What next?

splunk> listen to your data®

Call to Action

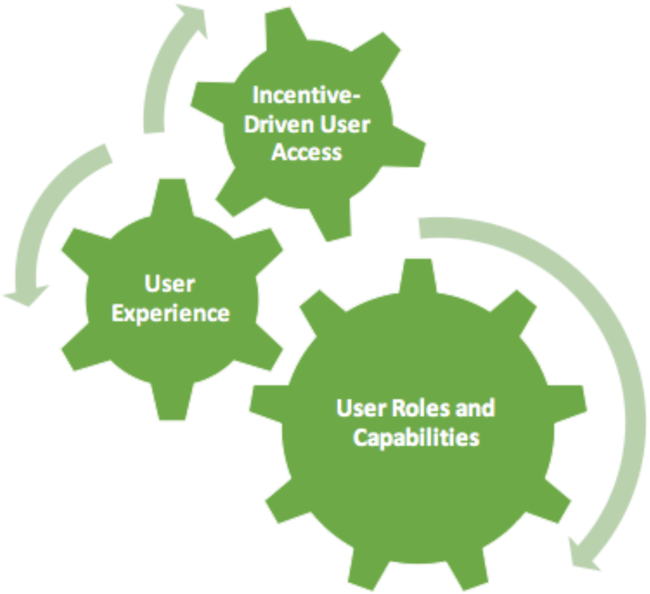


- Visit the Customer Success Studio
- Complete the CoE Assessment
- Pick up Best Practice Handouts
- eMail us at coe@splunk.com

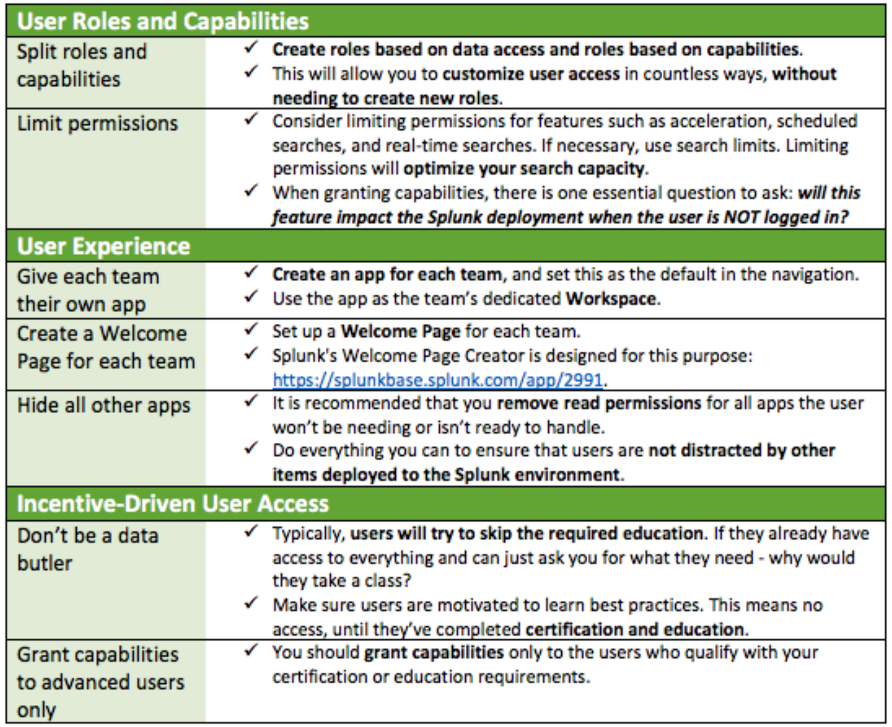
Customer Success Studio

CoE Best Practice: User Onboarding Handout

User Onboarding: Helping Users, So They Can Help Themselves



Basic Principles of User Onboarding: Things For Every Admin To Consider



User Roles and Capabilities	
Split roles and capabilities	✓ **Create roles based on data access and roles based on capabilities.** ✓ This will allow you to **customize user access** in countless ways, **without needing to create new roles.**
Limit permissions	✓ Consider limiting permissions for features such as acceleration, scheduled searches, and real-time searches. If necessary, use search limits. Limiting permissions will **optimize your search capacity**. ✓ When granting capabilities, there is one essential question to ask: ***will this feature impact the Splunk deployment when the user is NOT logged in?***
User Experience	
Give each team their own app	✓ **Create an app for each team**, and set this as the default in the navigation. ✓ Use the app as the team's dedicated **Workspace**.
Create a Welcome Page for each team	✓ Set up a **Welcome Page** for each team. ✓ Splunk's Welcome Page Creator is designed for this purpose: https://splunkbase.splunk.com/app/2991.
Hide all other apps	✓ It is recommended that you **remove read permissions** for all apps the user won't be needing or isn't ready to handle. ✓ Do everything you can to ensure that users are **not distracted by other items deployed to the Splunk environment.**
Incentive-Driven User Access	
Don't be a data butler	✓ Typically, **users will try to skip the required education.** If they already have access to everything and can just ask you for what they need - why would they take a class? ✓ Make sure users are motivated to learn best practices. This means no access, until they've completed **certification and education.**
Grant capabilities to advanced users only	✓ You should **grant capabilities** only to the users who qualify with your certification or education requirements.

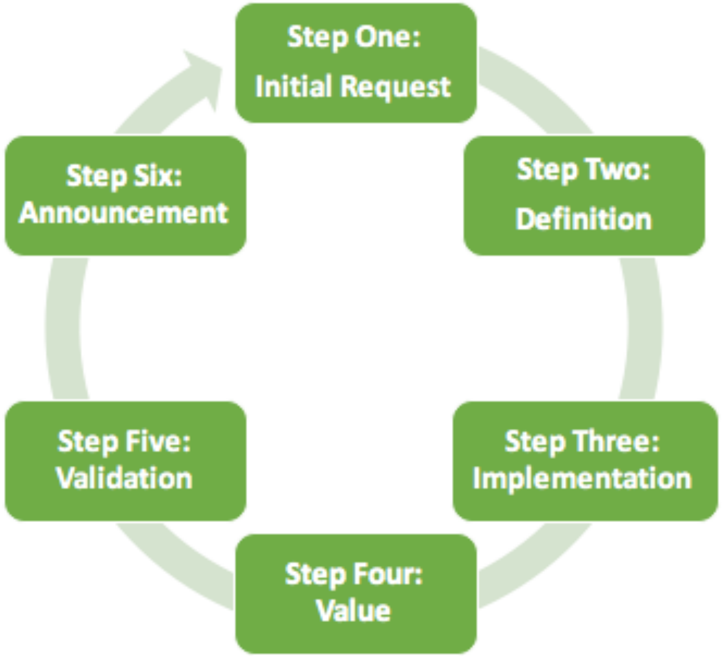
Determining Splunk Team Size

Variables	
Daily Ingest	Deployment Size
# of Users	# of Data Sources
# of Searches	# of Knowledge Objects
Service Level Objectives	Separation of Duties

Customer Success Studio

CoE Best Practice: Data Onboarding Handout

Data Onboarding: It's Iterative and Ongoing



Step One: Initial Request

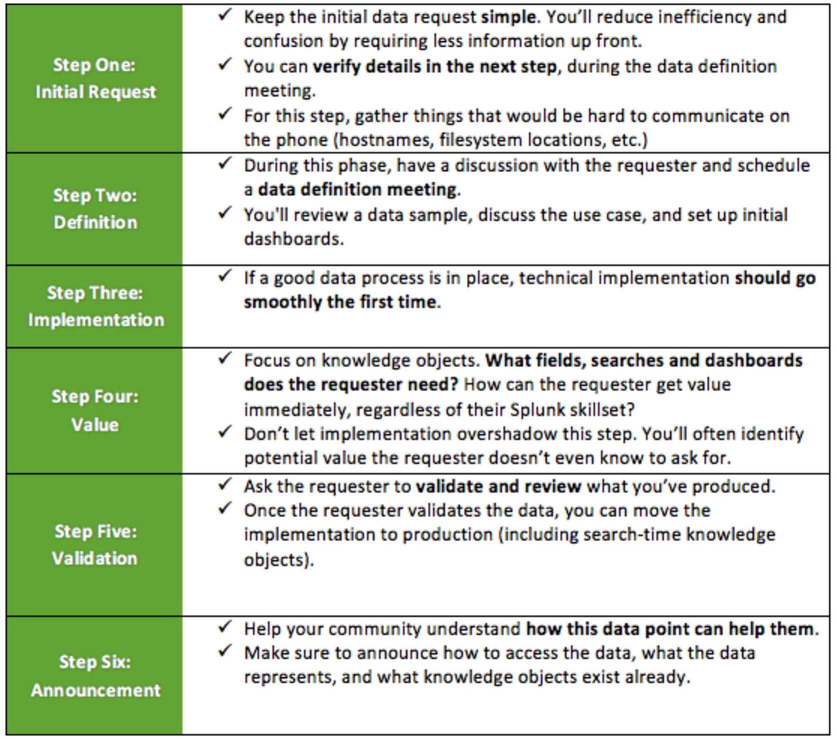
Step Two: Definition

Step Three: Implementation

Step Four: Value

Step Five: Validation

Step Six: Announcement

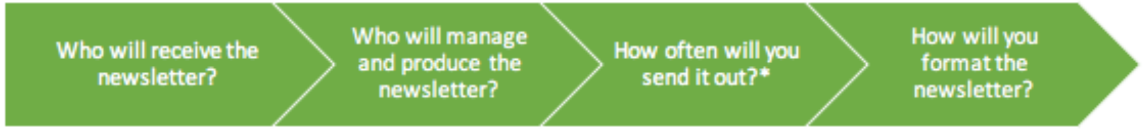


Step One: Initial Request	✓ Keep the initial data request **simple**. You'll reduce inefficiency and confusion by requiring less information up front. ✓ You can **verify details in the next step**, during the data definition meeting. ✓ For this step, gather things that would be hard to communicate on the phone (hostnames, filesystem locations, etc.)
Step Two: Definition	✓ During this phase, have a discussion with the requester and schedule a **data definition meeting**. ✓ You'll review a data sample, discuss the use case, and set up initial dashboards.
Step Three: Implementation	✓ If a good data process is in place, technical implementation **should go smoothly the first time**.
Step Four: Value	✓ Focus on knowledge objects. **What fields, searches and dashboards does the requester need?** How can the requester get value immediately, regardless of their Splunk skillset? ✓ Don't let implementation overshadow this step. You'll often identify potential value the requester doesn't even know to ask for.
Step Five: Validation	✓ Ask the requester to **validate and review** what you've produced. ✓ Once the requester validates the data, you can move the implementation to production (including search-time knowledge objects).
Step Six: Announcement	✓ Help your community understand **how this data point can help them**. ✓ Make sure to announce how to access the data, what the data represents, and what knowledge objects exist already.

Learn More

Customer Success Studio

CoE Best Practice: Creating a Newsletter



Who will receive the newsletter?

Who will manage and produce the newsletter?

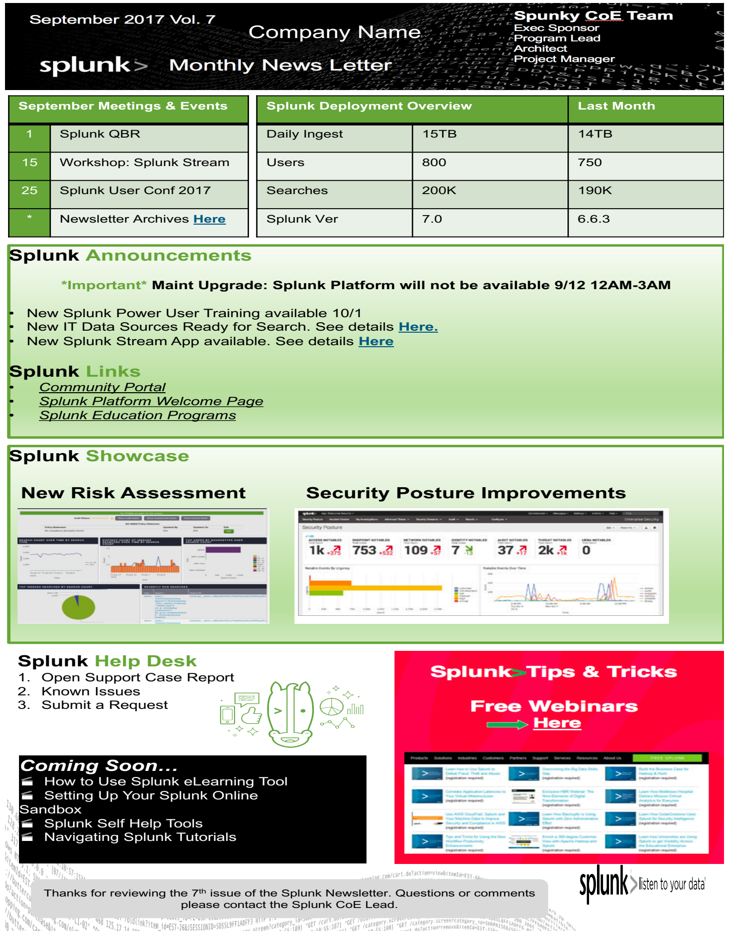
How often will you send it out?*

How will you format the newsletter?

* We recommend a monthly cadence.

What to Include in the Newsletter

- ✓ Calendar of events, such as workshops
- ✓ Announcements
- ✓ Platform and user stats, such as total number of users
- ✓ Splunk showcase and use case highlights
- ✓ Tips and tricks
- ✓ Important links
- ✓ Important messages, such as maintenance updates



September 2017 Vol. 7

Company Name

splunk> Monthly News Letter

Spunky CoE Team
Exec Sponsor
Program Lead
Architect
Project Manager

September Meetings & Events		Splunk Deployment Overview		Last Month
1	Splunk QBR	Daily Ingest	15TB	14TB
15	Workshop: Splunk Stream	Users	800	750
25	Splunk User Conf 2017	Searches	200K	190K
*	Newsletter Archives **Here**	Splunk Ver	7.0	6.6.3

Splunk Announcements

Important **Maint Upgrade: Splunk Platform will not be available 9/12 12AM-3AM**

- New Splunk Power User Training available 10/1
- New IT Data Sources Ready for Search. See details **Here.**
- New Splunk Stream App available. See details **Here**

Splunk Links

- *Community Portal*
- *Splunk Platform Welcome Page*
- *Splunk Education Programs*

Splunk Showcase

New Risk Assessment

Security Posture Improvements

Splunk Help Desk

1. Open Support Case Report
2. Known Issues
3. Submit a Request

Coming Soon…

- How to Use Splunk eLearning Tool
- Setting Up Your Splunk Online Sandbox
- Splunk Self Help Tools
- Navigating Splunk Tutorials

Splunk> Tips & Tricks

Free Webinars
→ **Here**

Thanks for reviewing the 7th issue of the Splunk Newsletter. Questions or comments please contact the Splunk CoE Lead.

splunk> listen to your data

Questions?

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

splunk> .conf2017