Saving the Nations Food Supply with Data-Driven Analytics

Sandy D. Voellinger
Engineering Practice Lead | Copper River ES

splunk> .conf19

Introduction

splunk> .conf19

Me, By The Numbers

20

Years in IT Automation, Engineering, & Security

10

Years working with Splunk

3

Years as Co-Lead DC Splunk'ers

5

Years supporting Public Sector

9

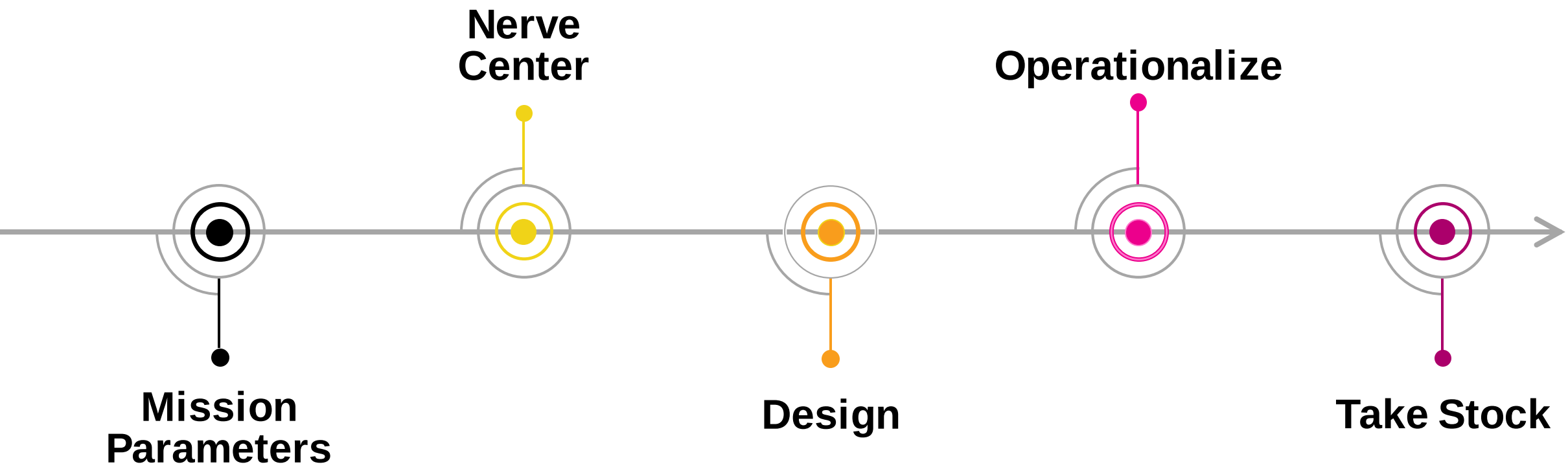
Number of Agencies my team currently supports

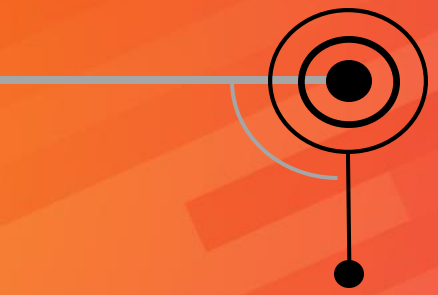
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Strategy





Mission Parameters

Understand the Mission

Information and Asset Protection

Federal Regulations & Mandates

FISMA
FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Mission / Business Services

PHI
PROTECTED HEALTH INFORMATION

Identify The Challenges

Mission Related Outages

- Communications
- Knowledge

Enterprise “Confusion”

- People
- Process
- Technology

Real World Impacts

Rotten Produce

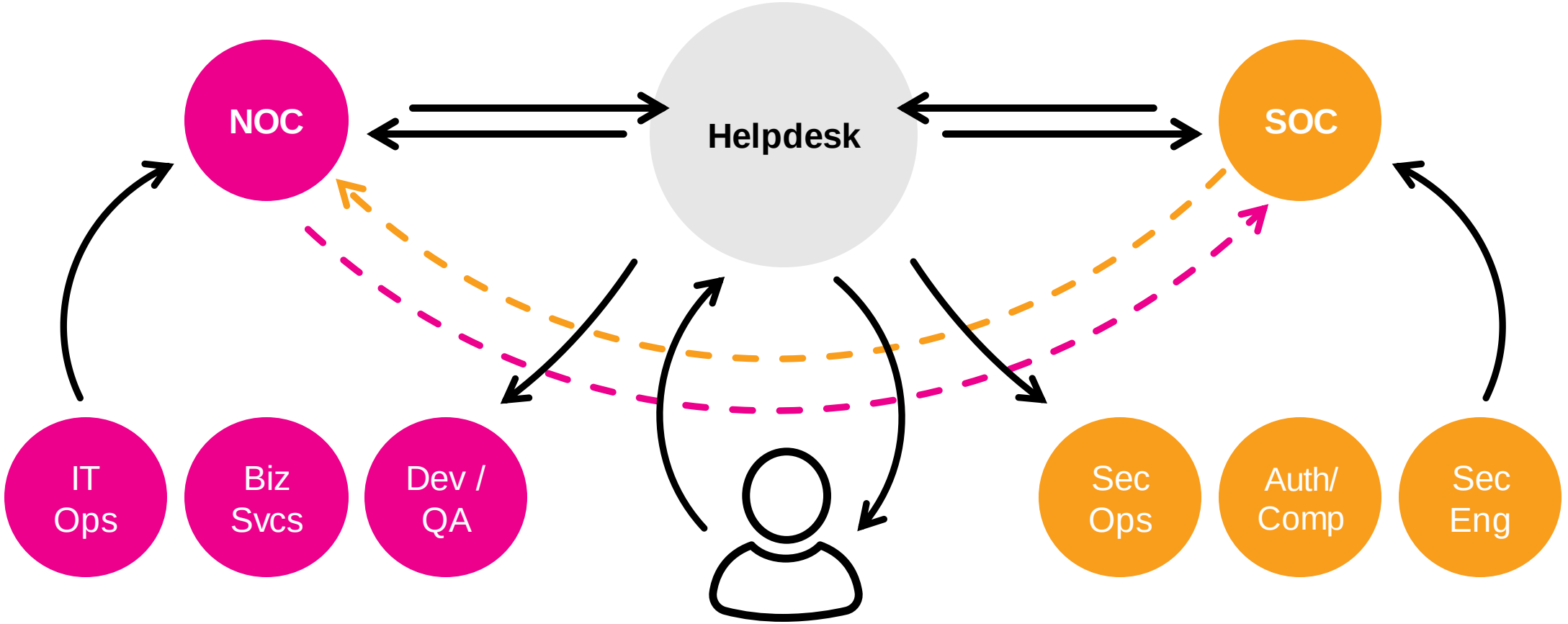
Consumer Market

Corporate Espionage

The Nerve Center

splunk> .conf19

Introspect

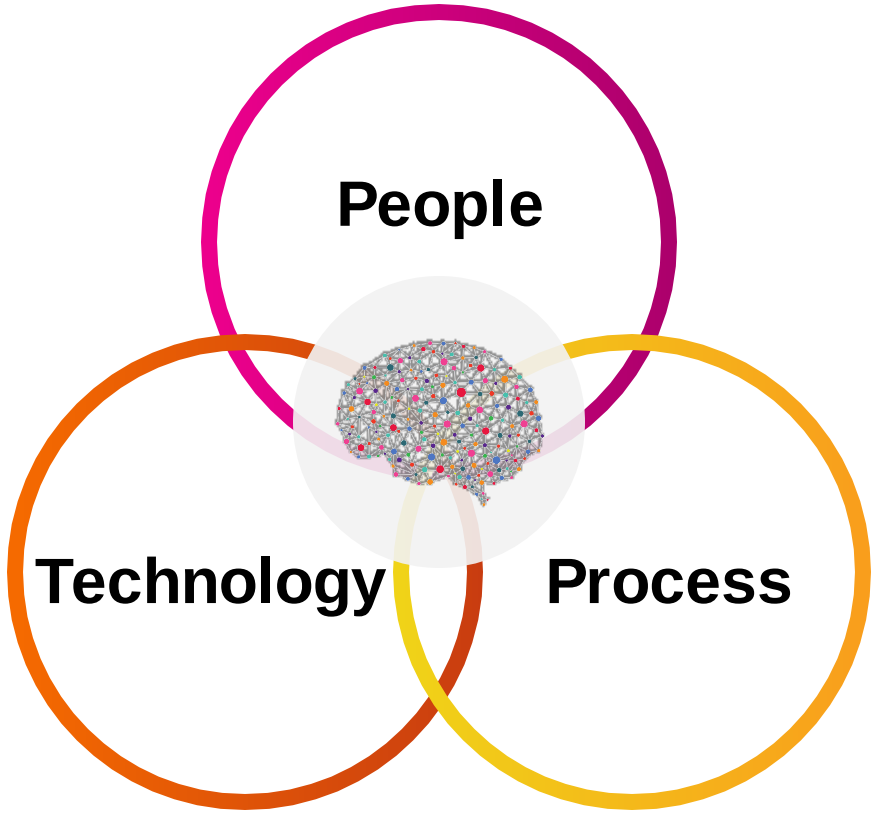


Nerve Center Composition

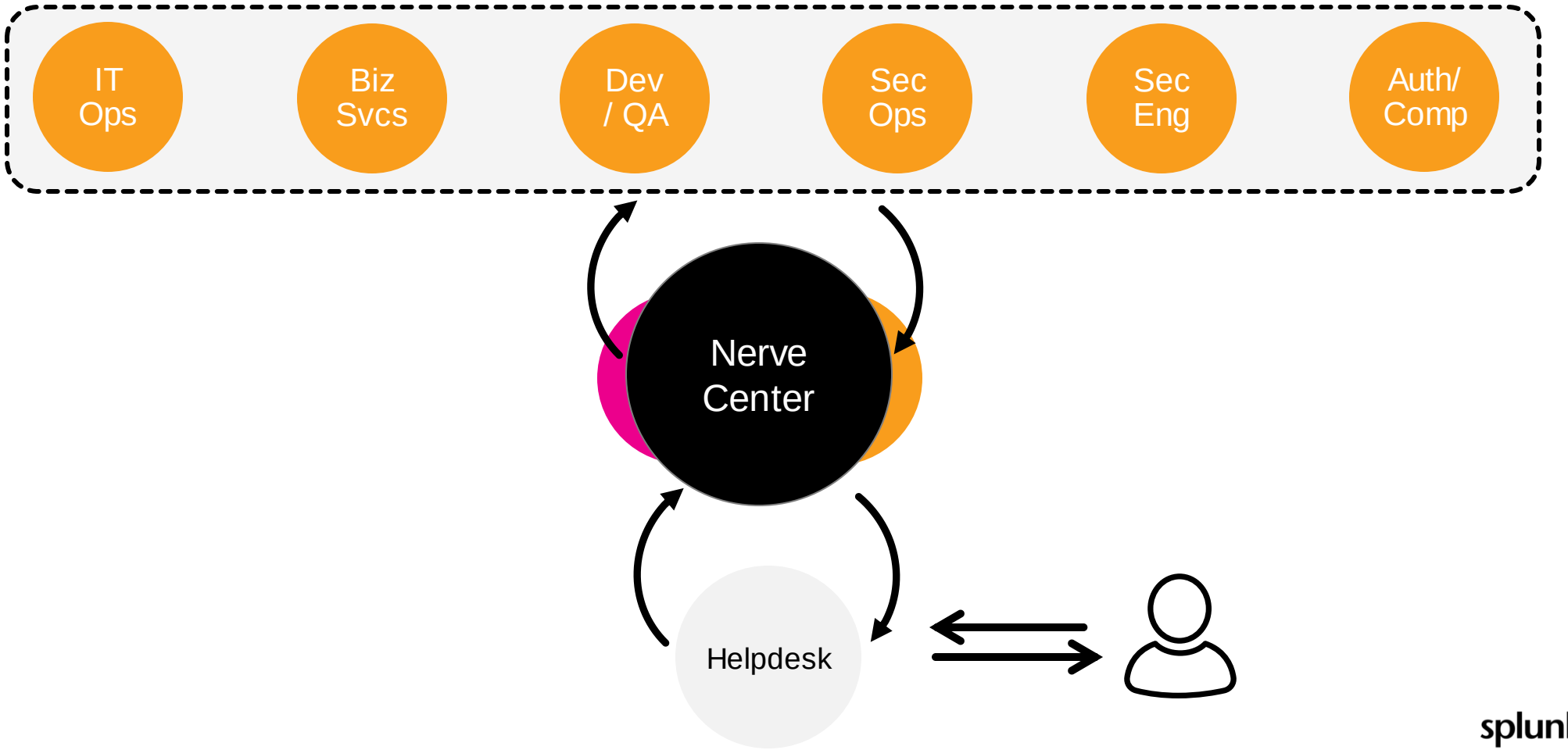
Organizational Structure
- Combine NOC/SOC

Technology / Application Rationalization
- Normalize behind Splunk

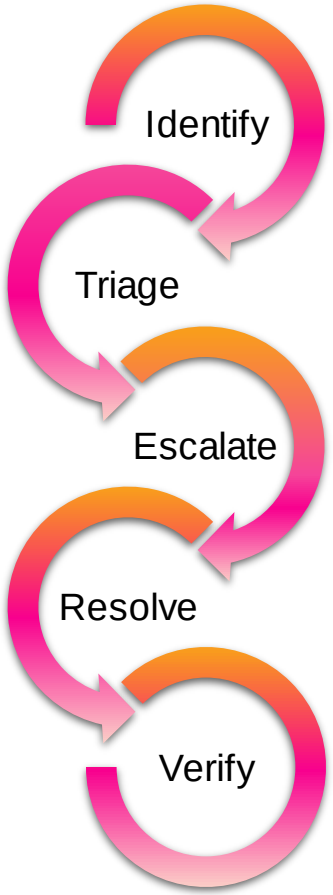
Processes and Workflows
- Orchestration/Automation



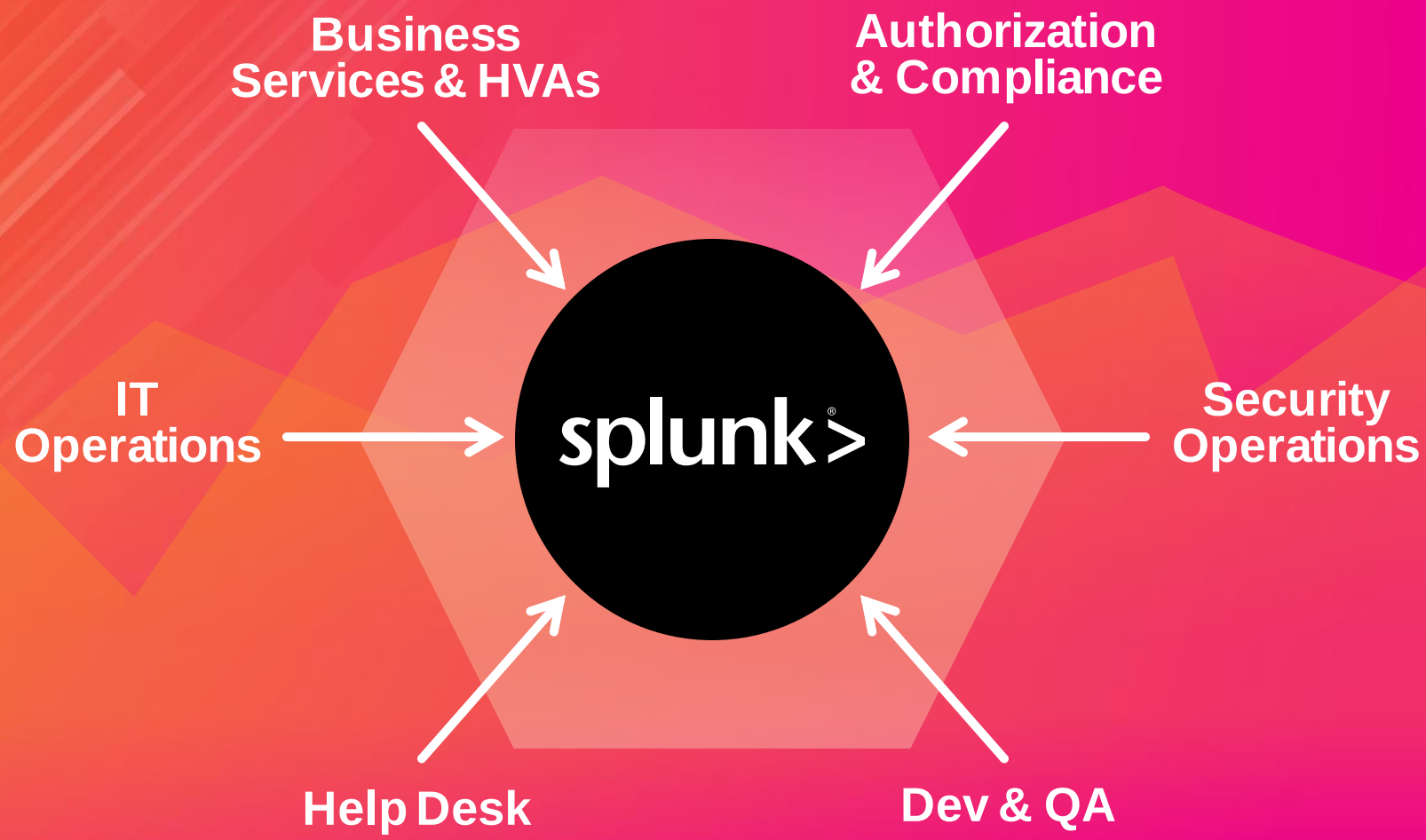
Organizational Alignment



Process Alignment



Technology Alignment

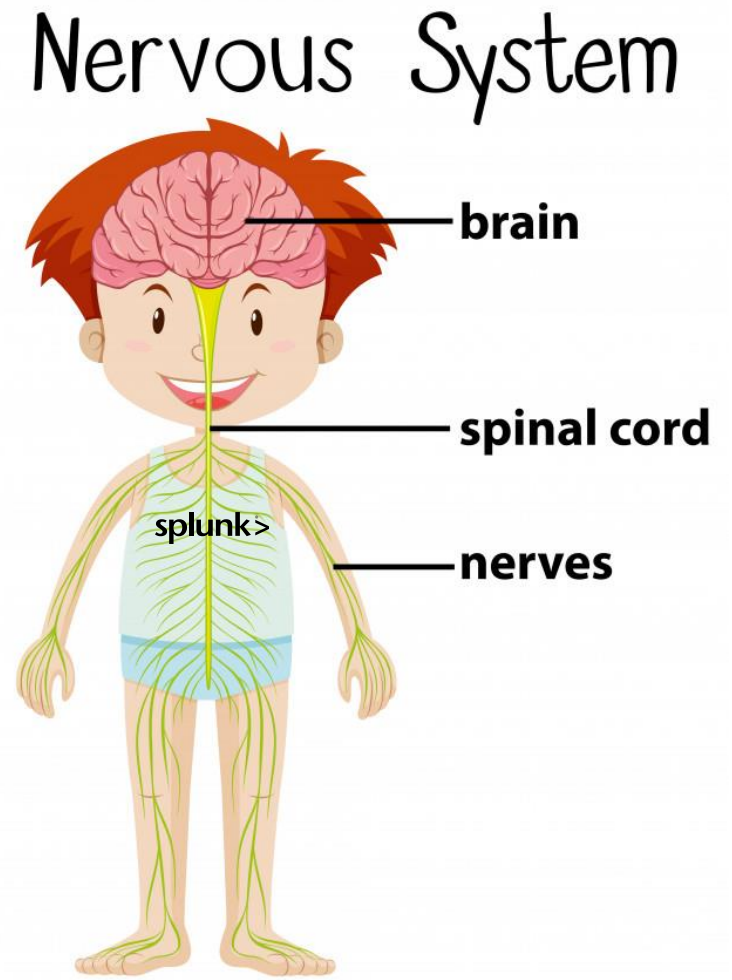


Splunk Anatomy 101

Brain = Reports, Alerts, Logic and Automation

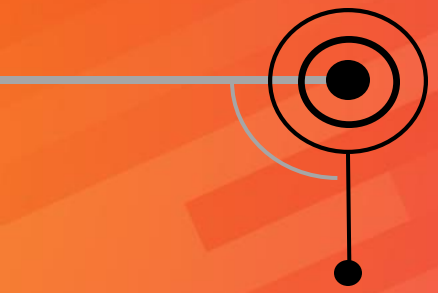
Spinal Cord = Forwarders and Data Collection

Nerves = Data Sources



“Take all our data, add a heavy splash of automation, and bring forth a strong stomach for change.”

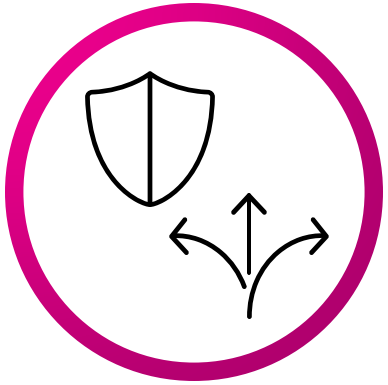
All data is relevant – Automation is Critical – Change is hard



Design

Design Questions

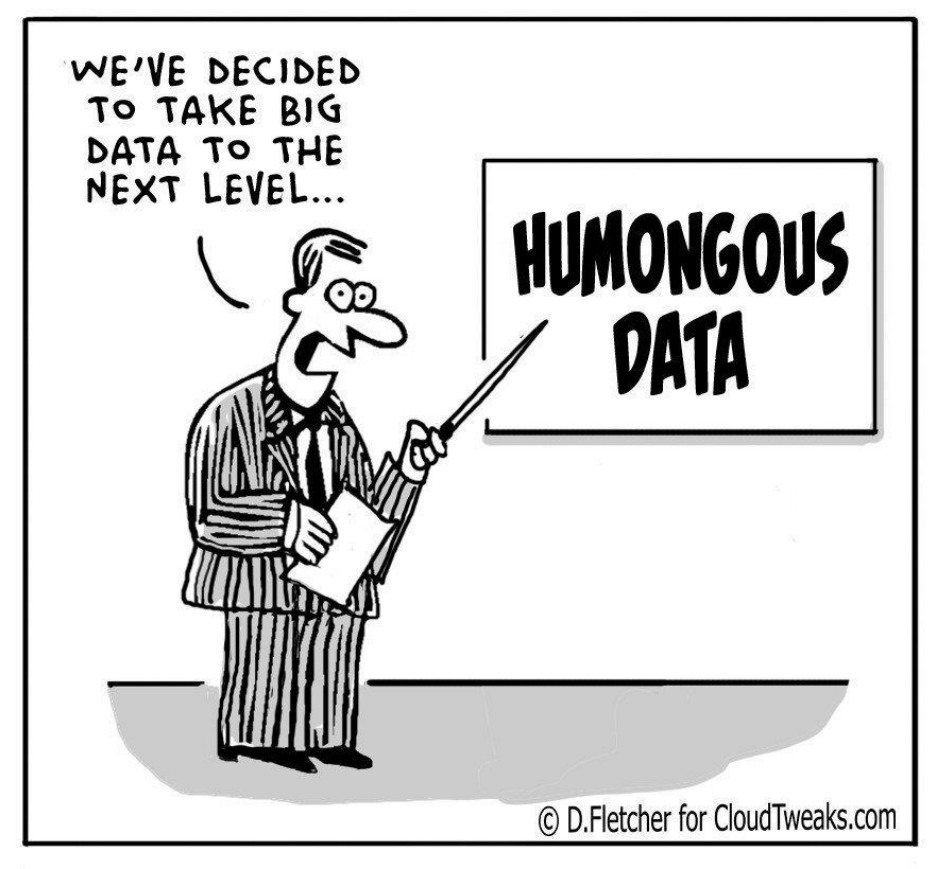
Desired outcomes will dictate the questions you answer



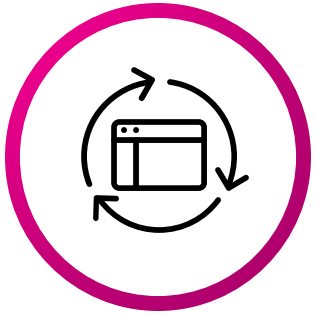
How do I keep my information **secure**, but make it **highly available**?

How do we get the **performance** we need, but make it **scalable** to all business verticals?

How do we **share** data between agencies, but maintain **control** of what is **shared**?



Splunk Design Requirements



Near Real-Time Correlation & Reporting

10+ TB Daily Ingestion with Multi-Site Index Clustering

~ 100 Concurrent Searches + ES & API Extensible

FIPS 140-2, PIV Integrated with RBAC

3 Years Searchable Retention, Hot & Warm Only

Build On A Solid Foundation

Converged Infrastructure

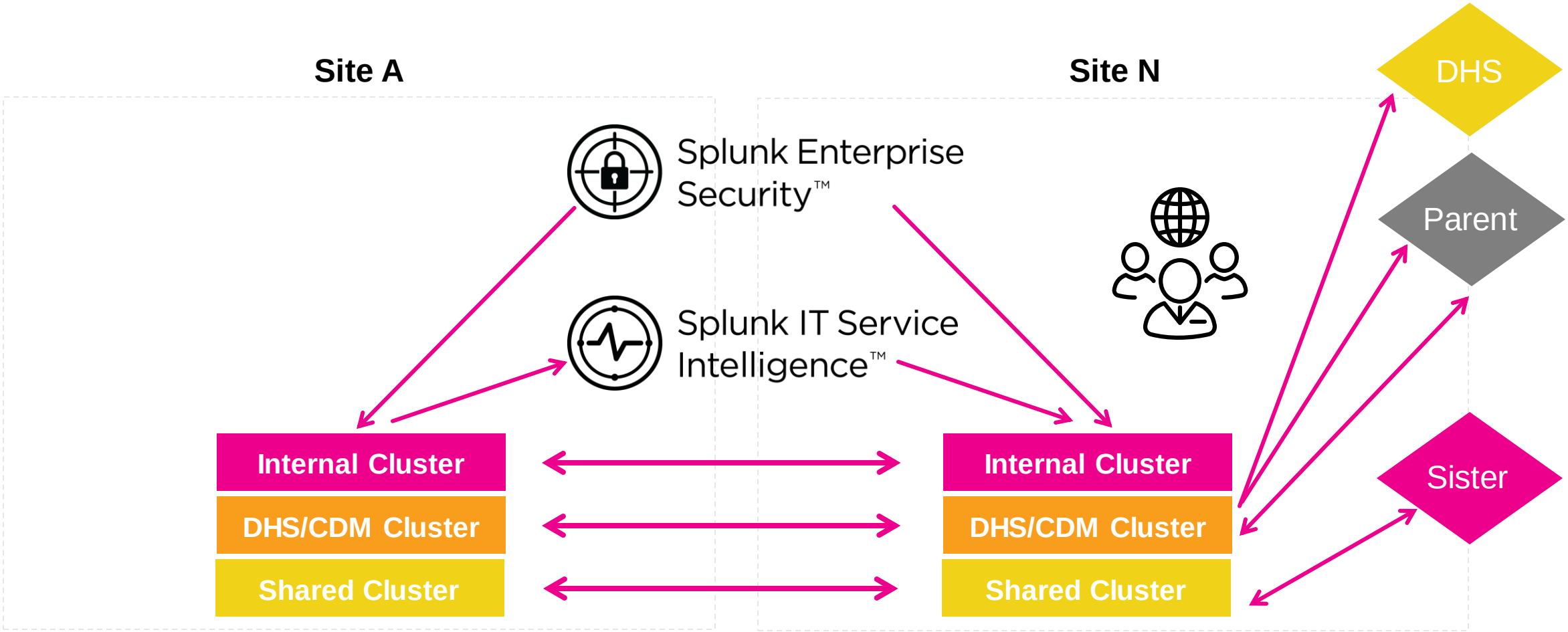
High Availability & Disaster Recovery

FIPS 140-2

Automation

Splunk Architecture

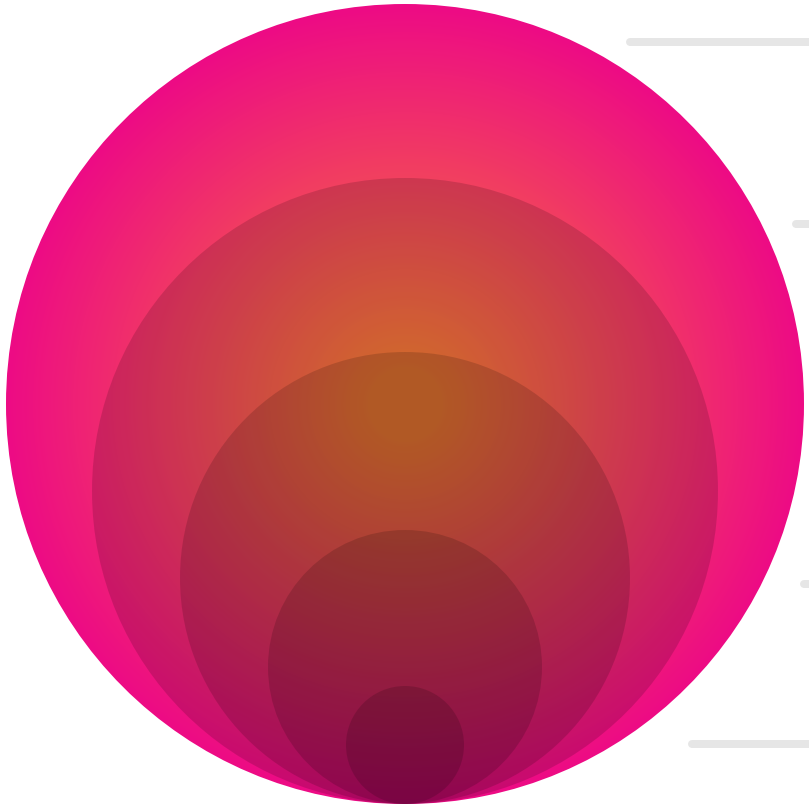
Multi-Agency Integrated Architecture

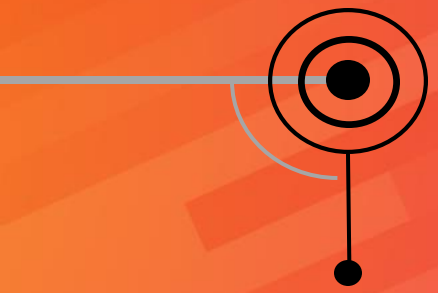


Environmental Statistics

Organize Your Data

- Align Use Case Registry & Data Sources
- Data Classifications & Restrictions
- One Data Source Per Index
- Map Index Enclave To Data Source
- Raw VS Summary





Operationalize

Where to Start?

Low Hanging Fruit

Frequency over Difficulty

Pace Yourself

Teach Others

Triage Workload

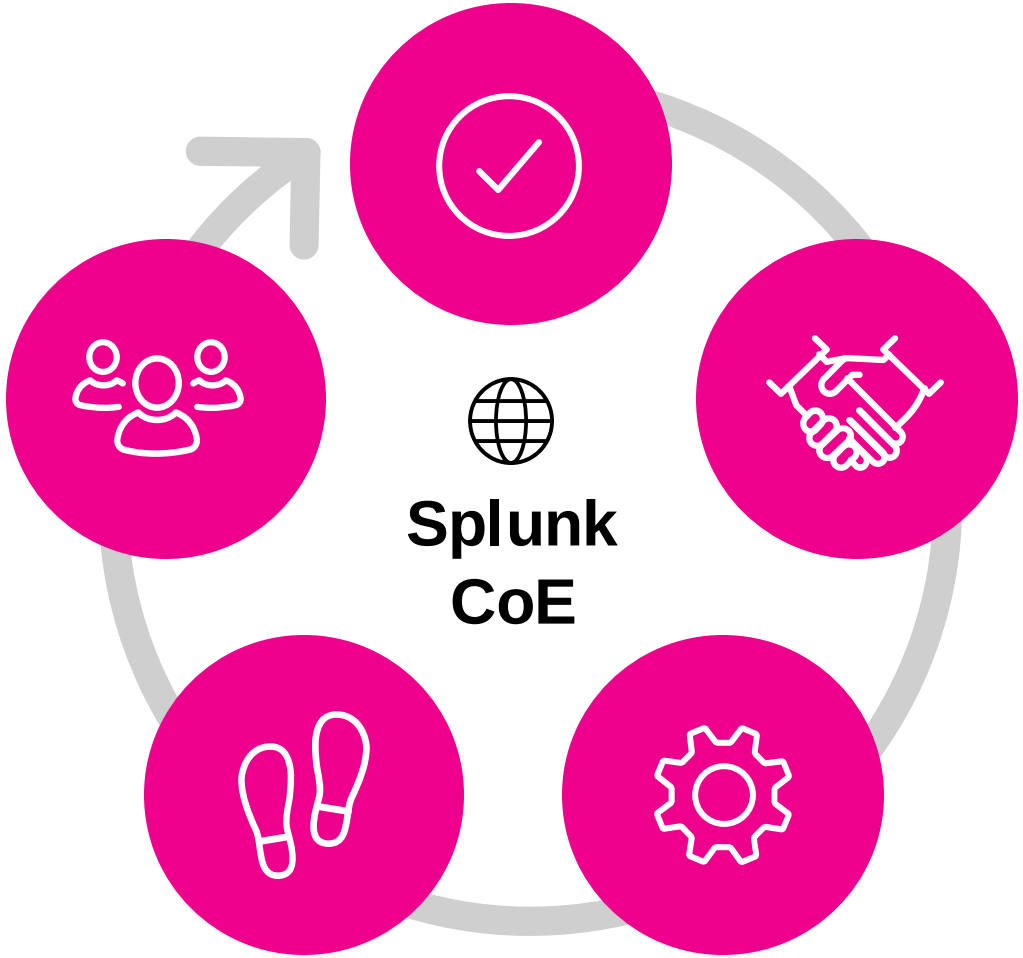
Use Case Registry

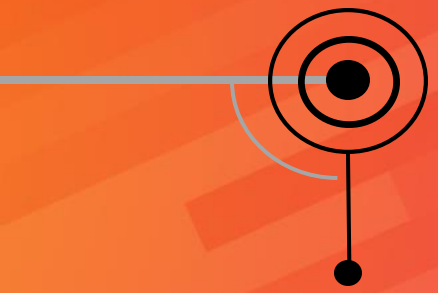
Group by Consumer or Function

- Mission Centric
- Security Operations
- Information Assurance
- Executives
- IT Operations
- Helpdesk

Center of Excellence

- Business Value
- Governance
- Operational Excellence
- Enablement
- Collaboration



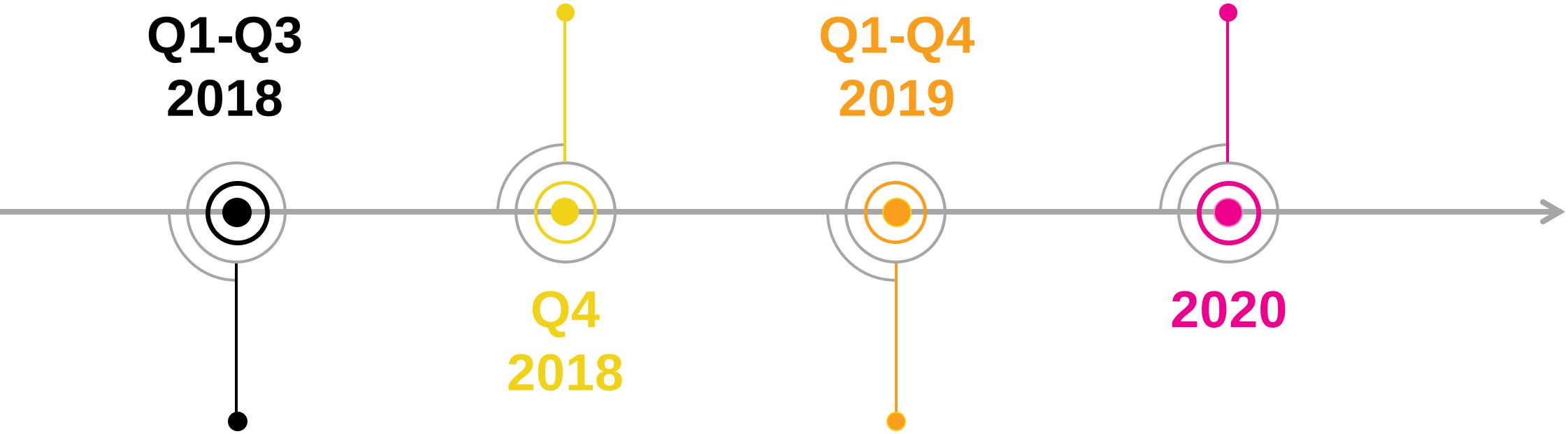


Take Stock

Timeline Review

splunk> .conf19

Timeline Review



Operational Results

12h 30m

Reduction in MTTD

16h 1h

Reduction in MTTR

68%

Reduction in overall outage times

2500+

Reduced “Man-Hours”

24

Custom Splunk Apps

Q&A

Sandy Voellinger | Engineering Lead

Copper River ES https://copperriveres.com

https://www.linkedin.com/in/sandy

Team = Splunk-UsersGroup : svoellinger

Sandy.Voellinger@copperriveres.com

splunk> .conf19

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION