Scaling for Success

Addressing Organizational Skill Gaps

Gregory Poniatowski | Information Security Lead

October 2018 | Version 1.0

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.

Supply and Demand

Expectation versus Reality

History

In the beginning

- Splunk Cloud was originally purchased as a SIEM.
- Modest infrastructure, small footprint
- Very little time spent on administration
- Several small scale efforts at optimization

Sudden Demand Static Supply

Spinning plates

- To drive adoption of the platform and increase security visibility an effort was made to demonstrate its capabilities to various operations groups.

- Selling the value proposition of Splunk internally was really successful
  - This is a good thing
    - The platform has enormous potential to benefit the company
  - This is also a bad thing
    - The team was still the same size (1)

The Problem

In the beginning

- Surge in demand stressed capacity in three key areas
- Static team size (1)
- Difficult to locate talent for temporary capacity
- No clear strategic solution

Three Legged Stool

Where does all the time go?

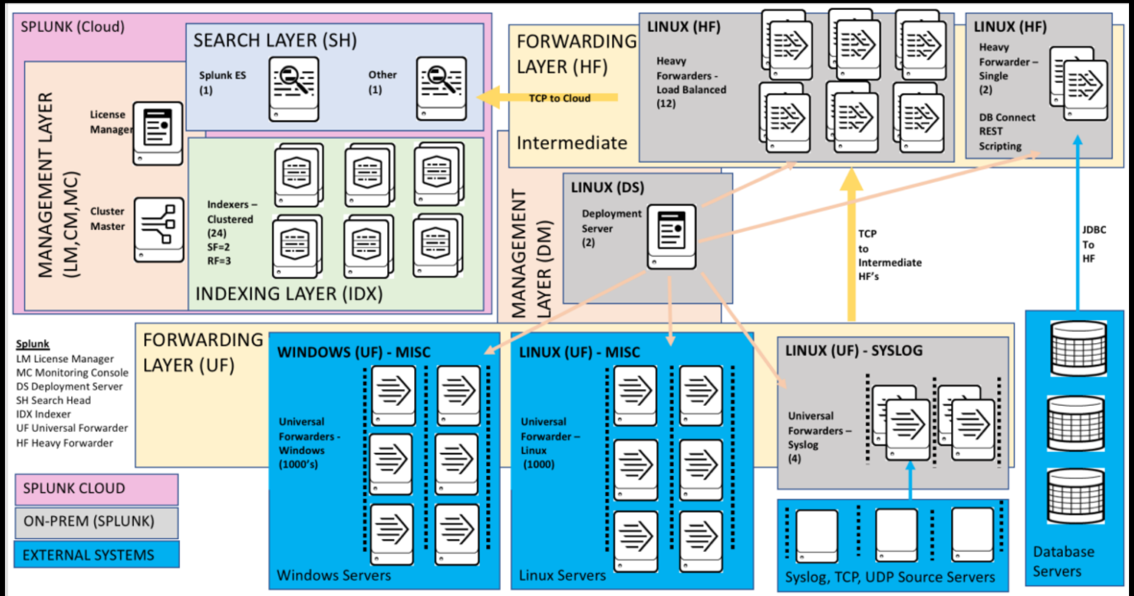
- Platform Support
  - The larger and more successful your deployment the more of this there is to do.
- Data Onboarding
  - Some data is well structured. Some data is easily portable. Some is neither.
- Content Creation
  - This is occasionally where a user’s story starts, but sometimes the page is left intentionally blank.

There are two fundamentally important components missing from the above, but these you will hardly notice when your deployment is living hand to mouth. You will notice them however when your deployment goes catastrophically wrong.

Platform Support

A stable service for all your users’ various needs

- Splunk is only the first technology in your stack
- As requirements (and technologies) get added to the infrastructure the skills required to keep it operating get more advanced
- A partial list of technologies we maintain to keep the data flowing and support development
  - rsyslog
  - HA Proxy
  - Docker
  - Python, Bash, and PowerShell Scripts
  - Gitlab
  - Atlassian Stuff
  - Puppet
  - PagerDuty

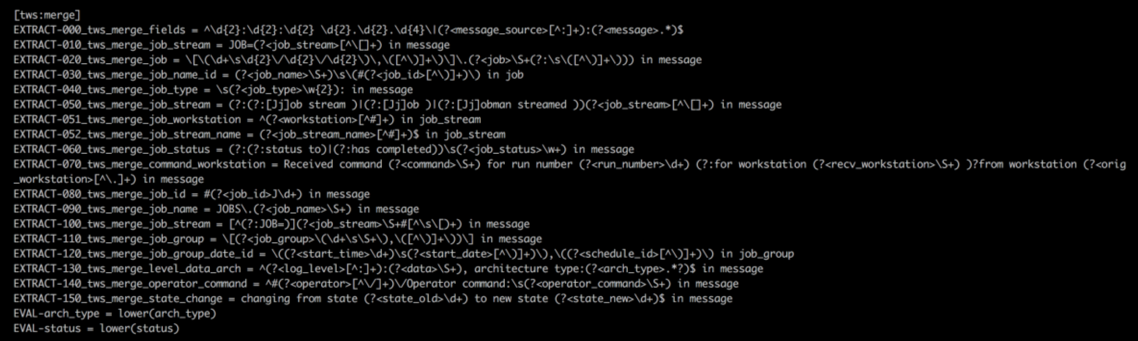


Data Onboarding

“standard syslog”

- Complexity is highly variable.
  - Sometimes you just push out a TA directly from Splunk Base and it works
  - Sometimes you have to cook up a TA yourself.

Almost anyone can be trained in a day to do the former, far fewer can be handed the specification for an obscure log type and turn it around into a custom TA



```
[tws:merge]
EXTRACT-000_tws_merge_fields = ^\d{2}:\d{2}:\d{2} \d{2}.\d{2}.\d{4}\|(?<message_source>[^:]+):(?<message>.*)$
EXTRACT-010_tws_merge_job_stream = JOB=(?<job_stream>[^\□+) in message
EXTRACT-020_tws_merge_job = \[\(\d+\s\d{2}\/\d{2}\/\d{2}\)\,\([^\)]+\)\]\.(?<job>\S+(?:\s\([^\)]+\))) in message
EXTRACT-030_tws_merge_job_name_id = (?<job_name>\S+)\s\(#(?<job_id>[^\)]+)\) in job
EXTRACT-040_tws_merge_job_type = \s(?<job_type>\w{2}): in message
EXTRACT-050_tws_merge_job_stream = (?:(?:[Jj]ob stream )|(?:[Jj]ob )|(?:[Jj]obman streamed ))(?<job_stream>[^\□+) in message
EXTRACT-051_tws_merge_job_workstation = ^(?<workstation>[^#]+) in job_stream
EXTRACT-052_tws_merge_job_stream_name = (?<job_stream_name>[^#]+)$ in job_stream
EXTRACT-060_tws_merge_job_status = (?:(?:status to)|(?:has completed))\s(?<job_status>\w+) in message
EXTRACT-070_tws_merge_command_workstation = Received command (?<command>\S+) for run number (?<run_number>\d+) (?:for workstation (?<recv_workstation>\S+) )?from workstation (?<orig
_workstation>[^\.]+) in message
EXTRACT-080_tws_merge_job_id = #(?<job_id>J\d+) in message
EXTRACT-090_tws_merge_job_name = JOBS\.(?<job_name>\S+) in message
EXTRACT-100_tws_merge_job_stream = [^(?:JOB=)](?<job_stream>\S+#[^\s\[)+) in message
EXTRACT-110_tws_merge_job_group = \[(?<job_group>\(\d+\s\S+\),\([^\)]+\))\] in message
EXTRACT-120_tws_merge_job_group_date_id = \((?<start_time>\d+)\s(?<start_date>[^\)]+)\),\((?<schedule_id>[^\)]+)\) in job_group
EXTRACT-130_tws_merge_level_data_arch = ^(?<log_level>[^:]+):(?<data>\S+), architecture type:(?<arch_type>.*?)$ in message
EXTRACT-140_tws_merge_operator_command = ^#(?<operator>[^\/]+)\/Operator command:\s(?<operator_command>\S+) in message
EXTRACT-150_tws_merge_state_change = changing from state (?<state_old>\d+) to new state (?<state_new>\d+)$ in message
EVAL-arch_type = lower(arch_type)
EVAL-status = lower(status)
```

Content Creation

After years of gathering first hand anecdotal data

While some users became skilled content creators, most new demand fell into two categories

- Demand of the 1st Type
  - Phase One: “We should get the data into Splunk”
  - Phase Two: ????
  - Phase Three: Insight!

- Demand of the 2nd Type
  - ” I need a dashboard that monitors all hardware and application errors everywhere in real time.”

Both cases require two very different approaches and require a deep understanding of the potential that Splunk has as well as key architectural considerations that can impact:

- License Utilization
- Search Performance
- Availability

The Anna Karenina Principle

Few right ways and many wrong ways to manage demand

Everyone basically has access to everything Backend supported as a best effort.

- The first approach we tried was also the easiest to implement.
  - On the plus side, users had ready access to the platform.
  - All operations were single threaded through one person.
  - Lifestyle that was supported by high interest technical debt.

Bolster the ranks with occasion professional services. Pay down the principle on some of the debt.

- The second approach was better resourced but not scalable or sustainable
  - Operations were no longer single threaded but with additional overhead
  - Best practice is a moving target when resources going through a revolving door.

Moment of Truth

From the smoldering ashes of a search head and some heavy forwarders

- What it was that we need to be successful and stay that way
- Near total neglect of user enablement and product management
- Available talent pool externally was not very deep, and it would take time to build skills internally
- We needed a strategic approach

“You’re gonna need a bigger team.”

– *Every Professional Services Consultant*

Exploring the COE Concept

Early draft to serious proposal

- Began research into staffing models and best practices
- Use of Splunk’s COE model to design staffing plan
- Still unsure how to fill vacant roles adequately

A New Service Offering

Partnering with Accenture to adapt the Splunk COE concept

- Establish Partnership
  - Viewed as a key step to ensure access to a large pool of talent
- Build a Shared Service
  - Economies of scale deepen the bench
- Develop Service Strategy
  - How would the service be developed and deployed
- Baseline Current Capacity

Baseline

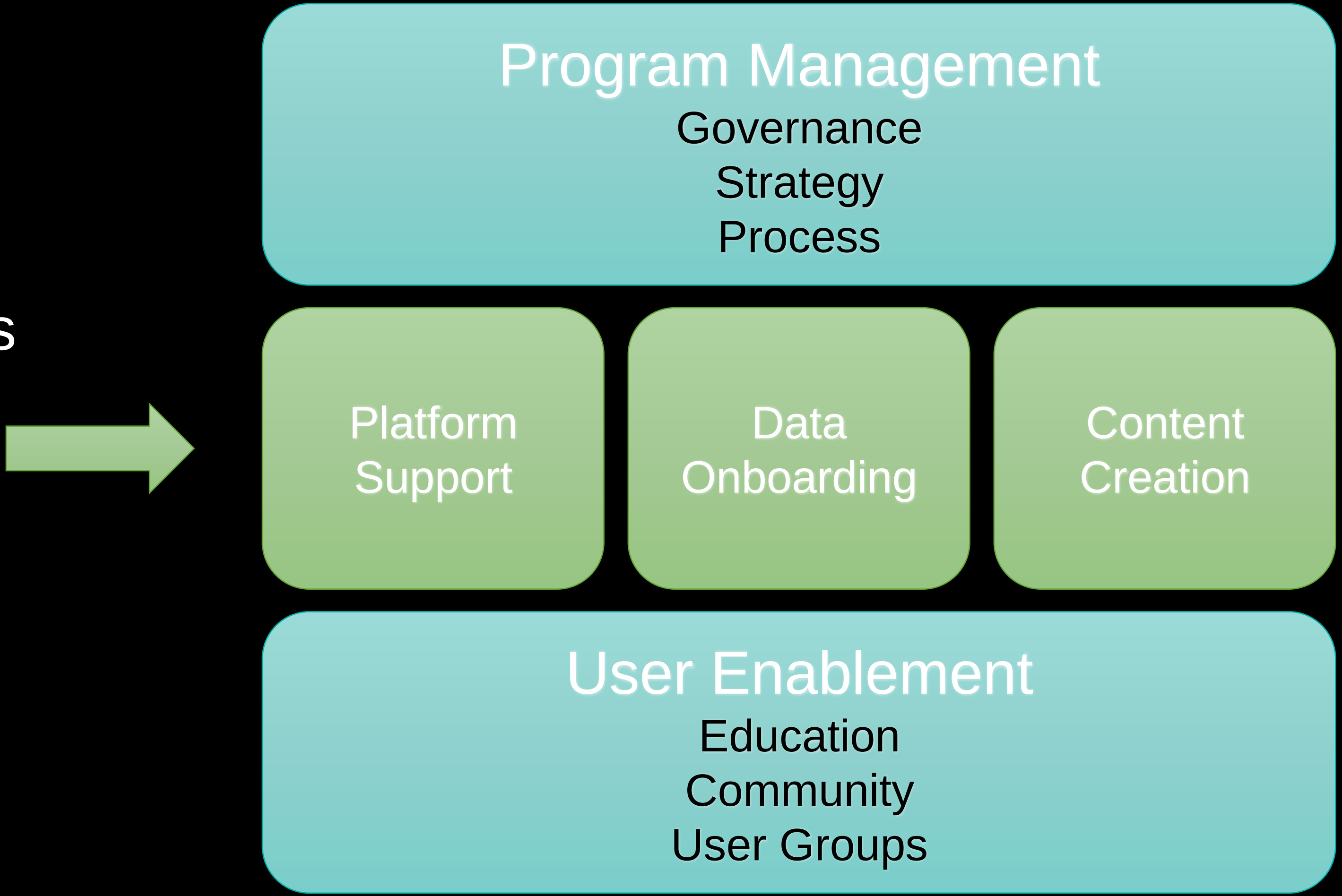
COE Evaluation Score – March 2018

Capability	Initial
Gap	6
Good	12
Better	1
Best	2
Score	20

Delivery Service

On the factory floor

At its most basic, the structure was developed to provide a scalable service for supporting the key components of the platform while freeing up resources internally for program management and user enablement.



Program Management
Governance
Strategy
Process

Platform Support

Data Onboarding

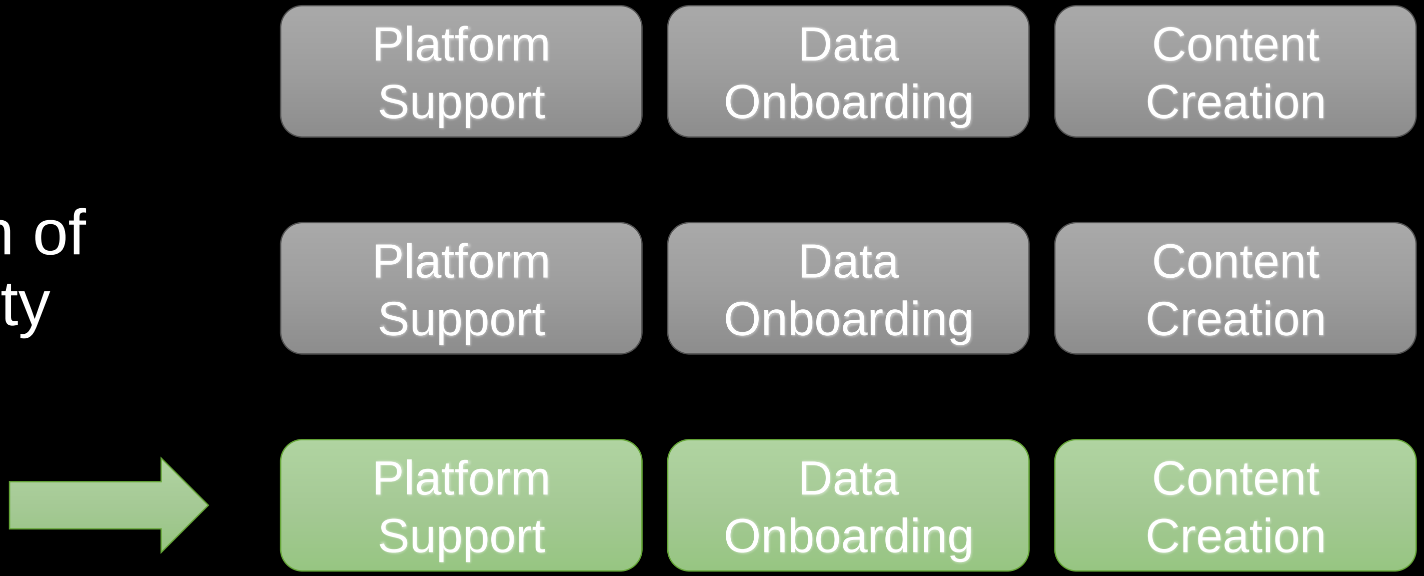
Content Creation

User Enablement
Education
Community
User Groups

Scalable Delivery Service

On the factory floor

- The service scales by offering a baseline capacity with the option of including additional burst capacity
- Resources in reserve are periodically cycled through to shadow dedicated resources so that less time is lost in spinning up additional lines.

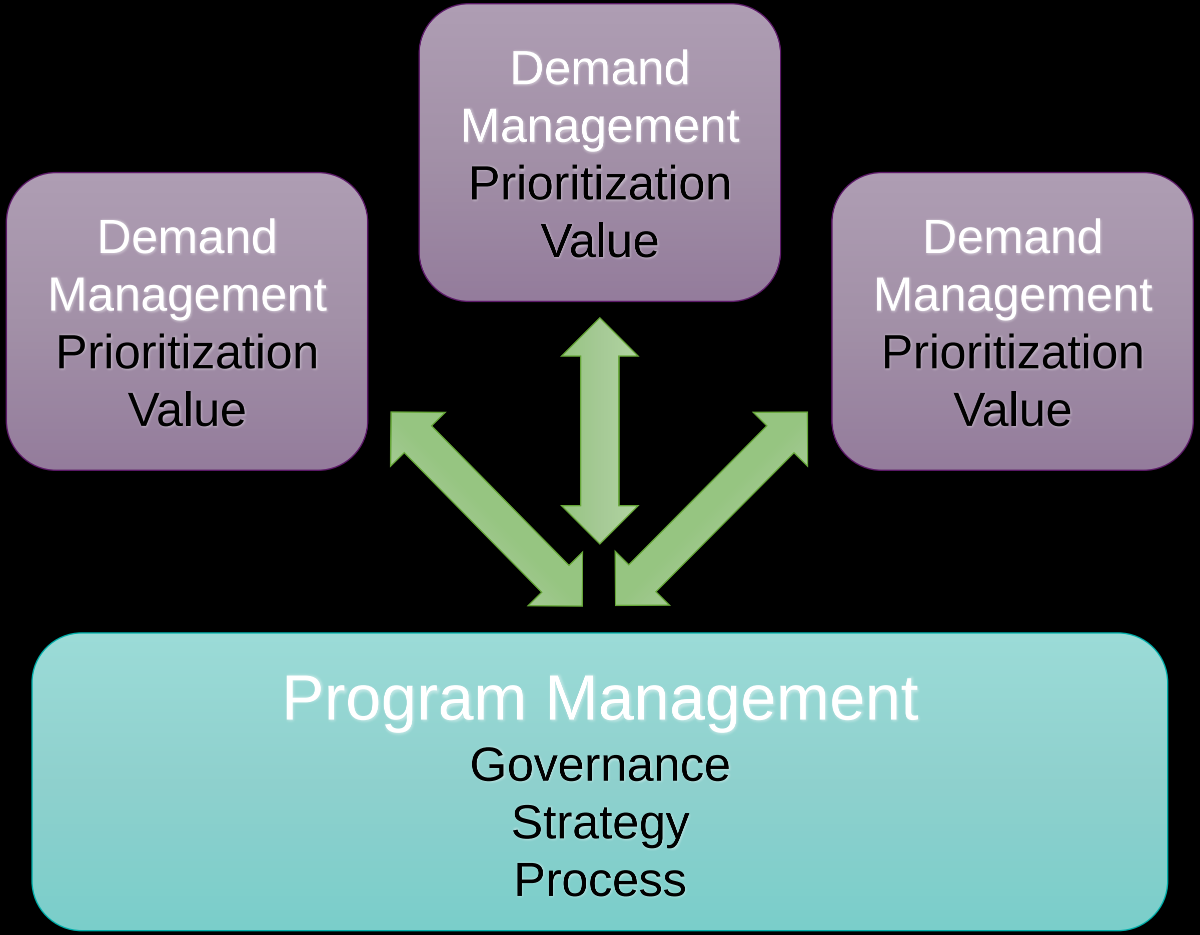


Platform Support	Data Onboarding	Content Creation
Platform Support	Data Onboarding	Content Creation
Platform Support	Data Onboarding	Content Creation

Program Management

Deputize your way to success

- Different areas of the organization have wildly different means of measuring value and setting priorities
- The relationship between the value of a byte and the cost to index is a complex problem.
- How can demand be prioritized and value be calculated?
  - Functional experts in different areas handle demand from similar groups in the organization
  - COE reconciles priorities between different groups and their own estimations of effort and feasibility



Demand Management Prioritization Value

Demand Management Prioritization Value

Demand Management Prioritization Value

Program Management

Governance

Strategy

Process

Tooling & Training

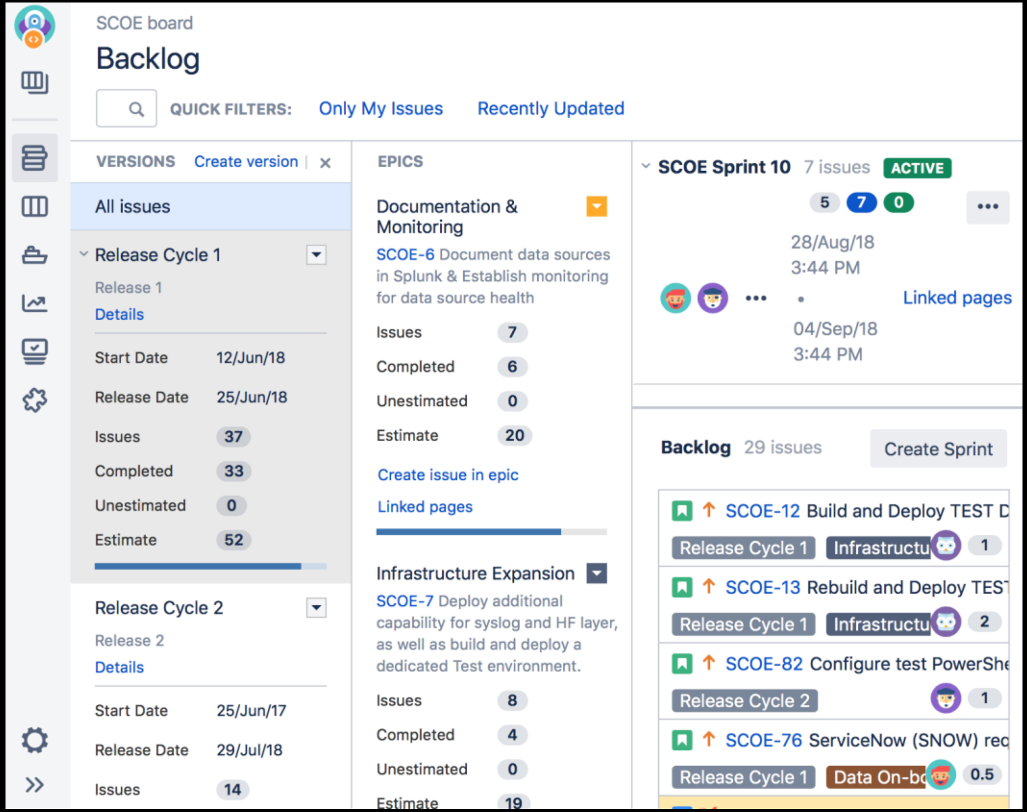
Helping users to ask for and receive help

- Making it easy for users to raise demand
- Delivery tracking
- User education

Access & Availability

Gatekeeping

- The first generation of project management tooling we used was email and shouting over the phone.
- For the COE, more organization was required.



SCOE board

Backlog

QUICK FILTERS: Only My Issues Recently Updated

VERSIONS Create version | ×

All issues

Release Cycle 1

Release 1

Details

Start Date	12/Jun/18
Release Date	25/Jun/18
Issues	37
Completed	33
Unestimated	0
Estimate	52

Release Cycle 2

Release 2

Details

Start Date	25/Jun/17
Release Date	29/Jul/18
Issues	14

EPICS

Documentation & Monitoring

SCOE-6 Document data sources in Splunk & Establish monitoring for data source health

Issues	7
Completed	6
Unestimated	0
Estimate	20

Create issue in epic

Linked pages

Infrastructure Expansion

SCOE-7 Deploy additional capability for syslog and HF layer, as well as build and deploy a dedicated Test environment.

Issues	8
Completed	4
Unestimated	0
Estimate	19

SCOE Sprint 10 7 issues ACTIVE

5 7 0 •••

28/Aug/18 3:44 PM • 04/Sep/18 3:44 PM

Linked pages

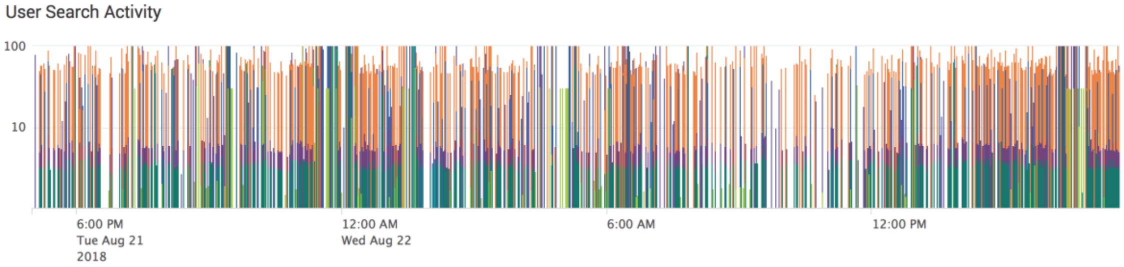
Backlog 29 issues Create Sprint

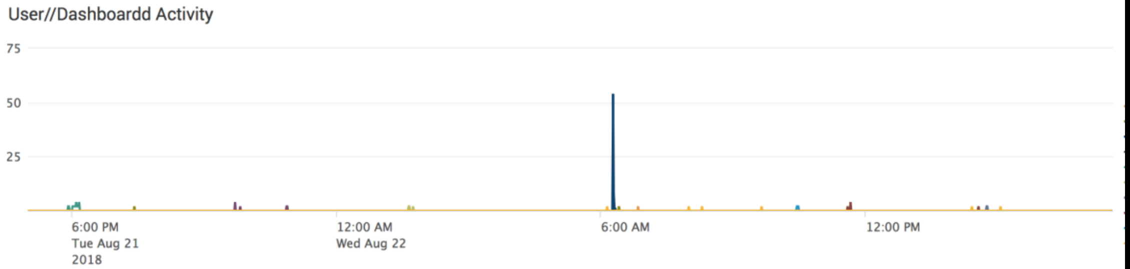
SCOE-12 Build and Deploy TEST D	Release Cycle 1	Infrastructu	1
SCOE-13 Rebuild and Deploy TES	Release Cycle 1	Infrastructu	2
SCOE-82 Configure test PowerShe	Release Cycle 2		1
SCOE-76 ServiceNow (SNOW) req	Release Cycle 1	Data On-bo	0.5

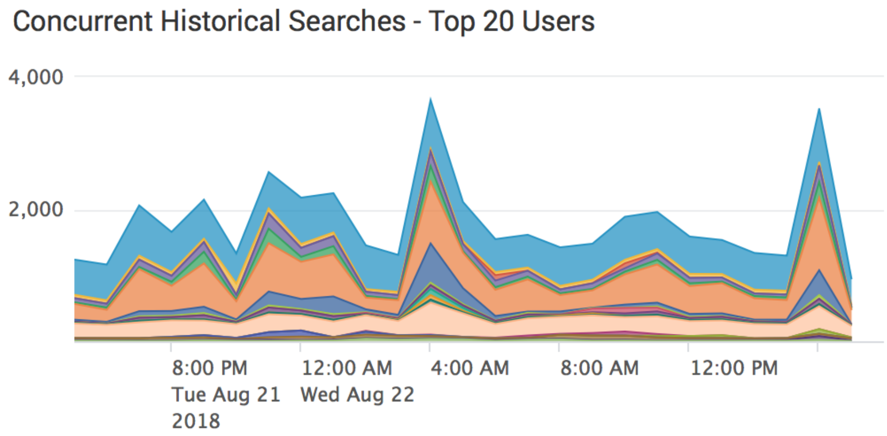
User Enablement

Helping users help themselves help us

- Many users want to create for themselves.
- This sort of self service delivery is in turn monitored by the COE.
- This model allows users to learn the platform and develop their skills while also making efficient use of the COE.


User Search Activity

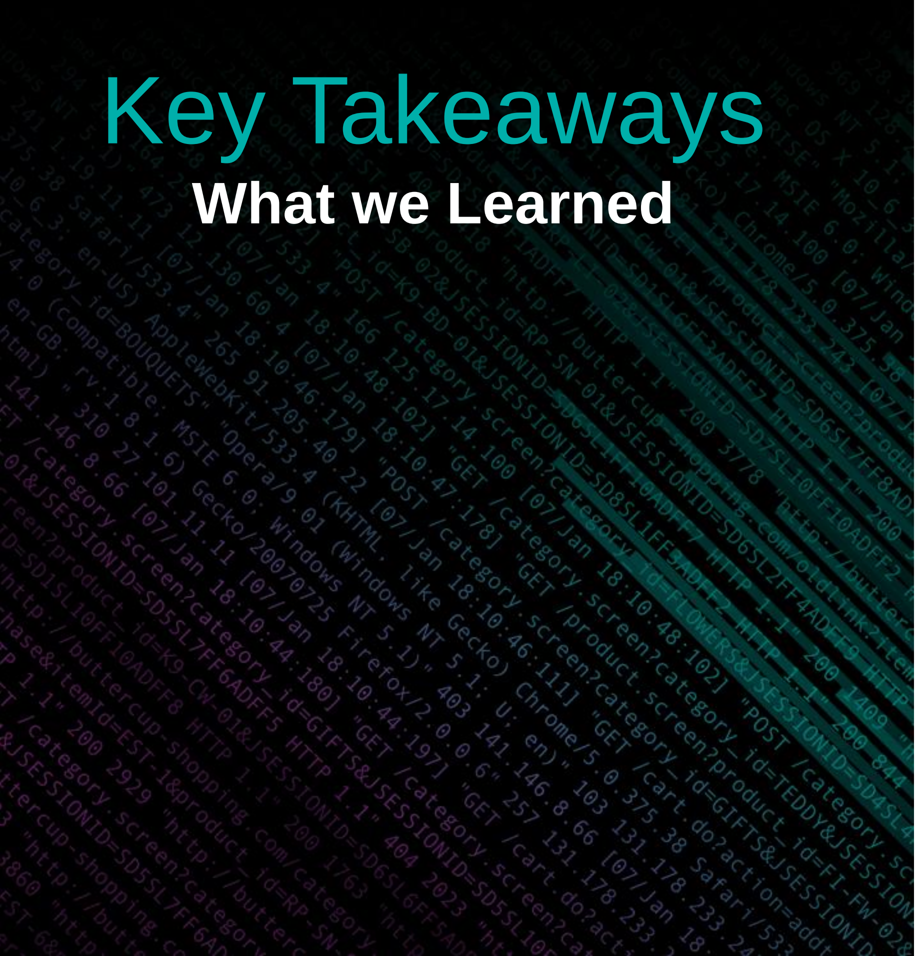

User//Dashboardd Activity


Concurrent Historical Searches - Top 20 Users

Where are we now?

COE Evaluation Score – March to September

Capability	Initial	Current
Gap	6	0
Good	12	9
Better	1	7
Best	2	5
Score	20	38



Key Takeaways

What we Learned

1. To be successful you need a deliberate and well resourced operation

2. Talent can take time to build. In the meantime partnering made scaling more immediate and sustainable.

3. Supporting the COE with processes and tooling enables them to be effective.

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>