© 2019 SPLUNK INC.



United Health Group:
Providing real-time visibility with Splunk IT Service Intelligence from the front end all the way to the mainframe

Ben Nolan
Splunk ITSI Administrator | Optum

Jacob Edelen
Splunk ITSI Administrator | Optum

© 2019 SPLUNK INC.

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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.





Ben Nolan
Splunk ITSI Administrator | Optum

Jacob Edelen
Splunk ITSI Administrator | Optum

splunk> .conf19

© 2019 SPLUNK INC.

Introductions

Jake Edelen

- Employed at Optum for over 4 years
- Specialized in end to end performance monitoring
- Splunking for 3.5 years – Certified Splunk ITSI Administrator
- Enjoy long walks on the beach.
- Favorite Splunk command: stats

Ben Nolan

- Over 10 years of industry experience
- Specialized in System Administration and Enterprise Monitoring
- Splunking for over 5 years – Certified Splunk Administrator
- Optum Employee since Feb 2017
- Enjoys solving technology problems and helping people
- Favorite Splunk command: rex

© 2019 SPLUNK INC.

Agenda

Splunk and ITSI at UHG/Optum

ITSI Instrumentation Approach

- Where we started
- Where we are now

Examples:

- Provider Applications
- Member Portal
- Online Pharmacy

Results and Lessons Learned

Next Steps

Q&A

© 2019 SPLUNK INC.

Splunk and ITSI at UHG/Optum

Core Splunk

- Hosted on Physical Hardware
- 10+ TB/Day
- 100+ Indexes
- 300+ Applications onboarded
- 2000+ Users
- Version: 7.1.7

Core Splunk Team

- 15 Dedicated on-shore resources
- 6 Dedicated off-shore resources
- 2 Dedicated Project Managers

IT Service Intelligence

- 2,400 + Services
- 10,000 + KPI's
- 15,000 + Entities
- 1600 Schedules Searches
- 150 + Alerts
- Version: 4.1.2

ITSI Team

- 7 Dedicated on-shore resources
- 1 Dedicated Project Manager

© 2019 SPLUNK INC.

I spend how much on war rooms?!?!

Problem:
Application teams have little to no visibility into the health of downstream dependencies.

Goal:
Provide insight into downstream dependencies and reduce MTTD and MTTR.

Solution:
Aggregate data, map dependencies, and provide visibility.

© 2019 SPLUNK INC.

The Initial Approach: Learning to Walk

Service Decomposition

- Compile Documentation
- Identify all critical components of front-end
- Identify all back-end supporting applications/systems
- Define Key Performance Indicators (KPI's)
- Pinpoint data gaps and fill

© 2019 SPLUNK INC.

Wait… This is Crawling not Walking!

Service Decomposition

- Compile Documentation Documentation always out of date
- Identify all critical components of front-end App teams knew their services well
- Identify all back-end supporting applications/systems Front-end teams do not know all backend systems
- Define Key Performance Indicators (KPI's) We've never monitored this before?
- Pinpoint data gaps and fill
  - – Internal processes restrict how quickly data can be added
  - – Most applications already onboarded to Splunk, were missing crucial data for some VBF components

© 2019 SPLUNK INC.

This is really really slow…

- Time and resource intensive service decompositions
- Siloed Monitoring
- Non-standardized KPI’s
- Peak Season?
- Messy Alerts

© 2019 SPLUNK INC.

Learning to Walk… For Real this Time

Service decomposition V2

- Onboard the data first!
- Limit scope of implementation
- Become an SME for widely used datasets
- Standardized KPI’s
- Improved Alerting

© 2019 SPLUNK INC.

Example of Improved Alerts

The alert condition for 'MPP (1) External User Select Organization, Corporate MPIN, TIN' was triggered.

Please review the corresponding ITSI Glass Table for additional context:

Alert: MPP (1) External User Select Organization, Corporate MPIN, TIN

View results in Splunk

service_name	Percent_Critical	Percent_High	Percent_Medium	Percent_Normal	Percent_Maintenance
MPP - Link Security - /corporates	46.67	0.00	0.00	53.33	0.00
MPP - Link Security - /provider_organizations	46.67	0.00	0.00	53.33	0.00
MPP - Link Security - /provider_tax_ids	46.67	0.00	0.00	53.33	0.00
MPP - User-Access - /organization	46.67	0.00	0.00	53.33	0.00
MPP - User-Access - /tins	46.67	0.00	0.00	53.33	0.00

© 2019 SPLUNK INC.

LINK Provider

What is it?

- Link Provider hosts access to several dashboards which contain a collection of applications for various healthcare providers and state agencies. Link supplies a jumping-off point for these applications and a consolidated user experience.

Who uses it?

- Health Care Providers [Doctors, Nurses, Hospitals …etc.]

Volume

- 1.5 Million Transactions per Day

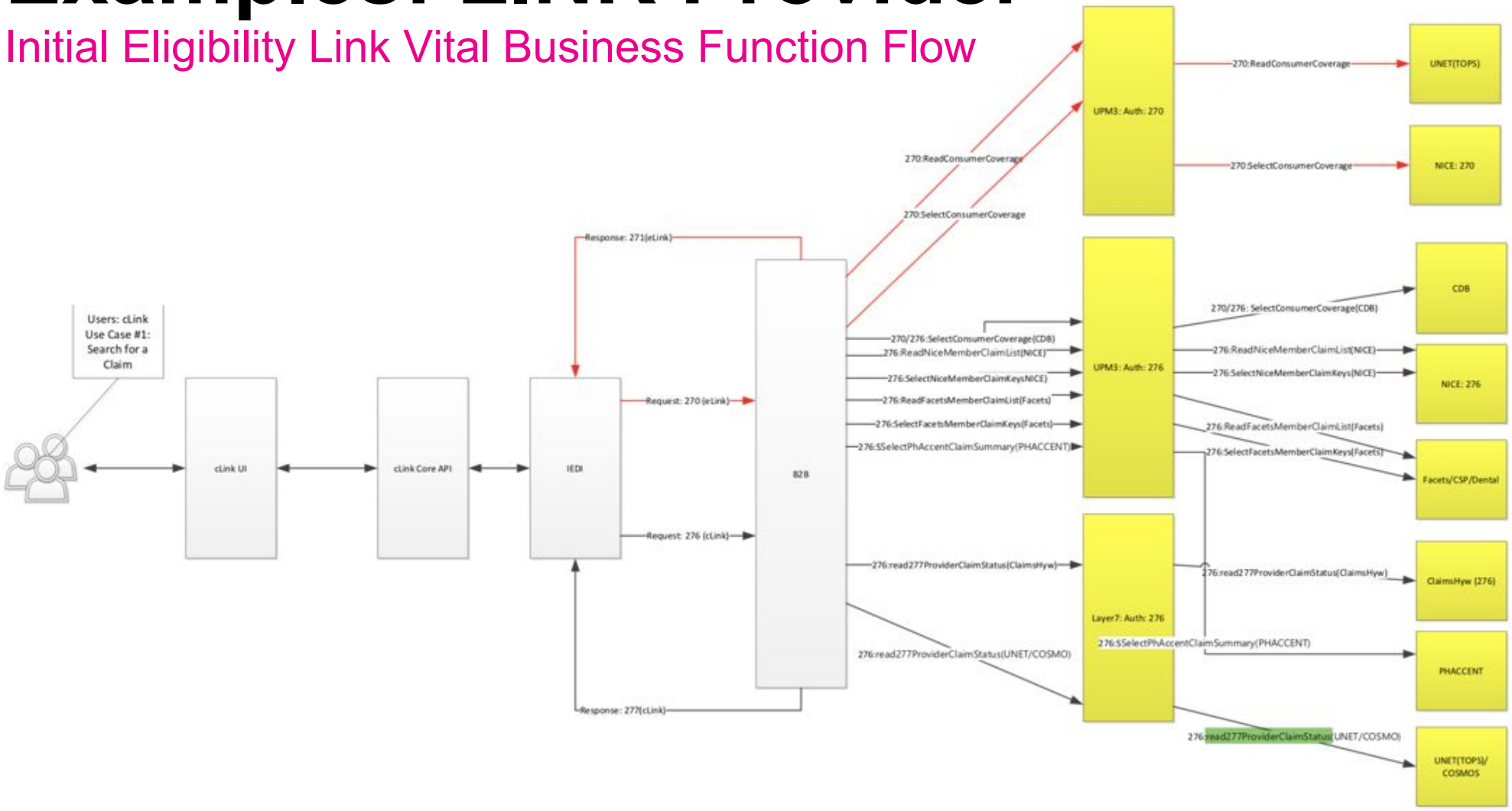
ITSI Stats

- 57 services across 15 different applications broke out into 6 Vital Business Functions
- 350 Key Performance Indicators
- 30+ alerts

© 2019 SPLUNK INC.

Examples: LINK Provider

Initial Eligibility Link Vital Business Function Flow



© 2019 SPLUNK INC.

Examples: LINK Provider

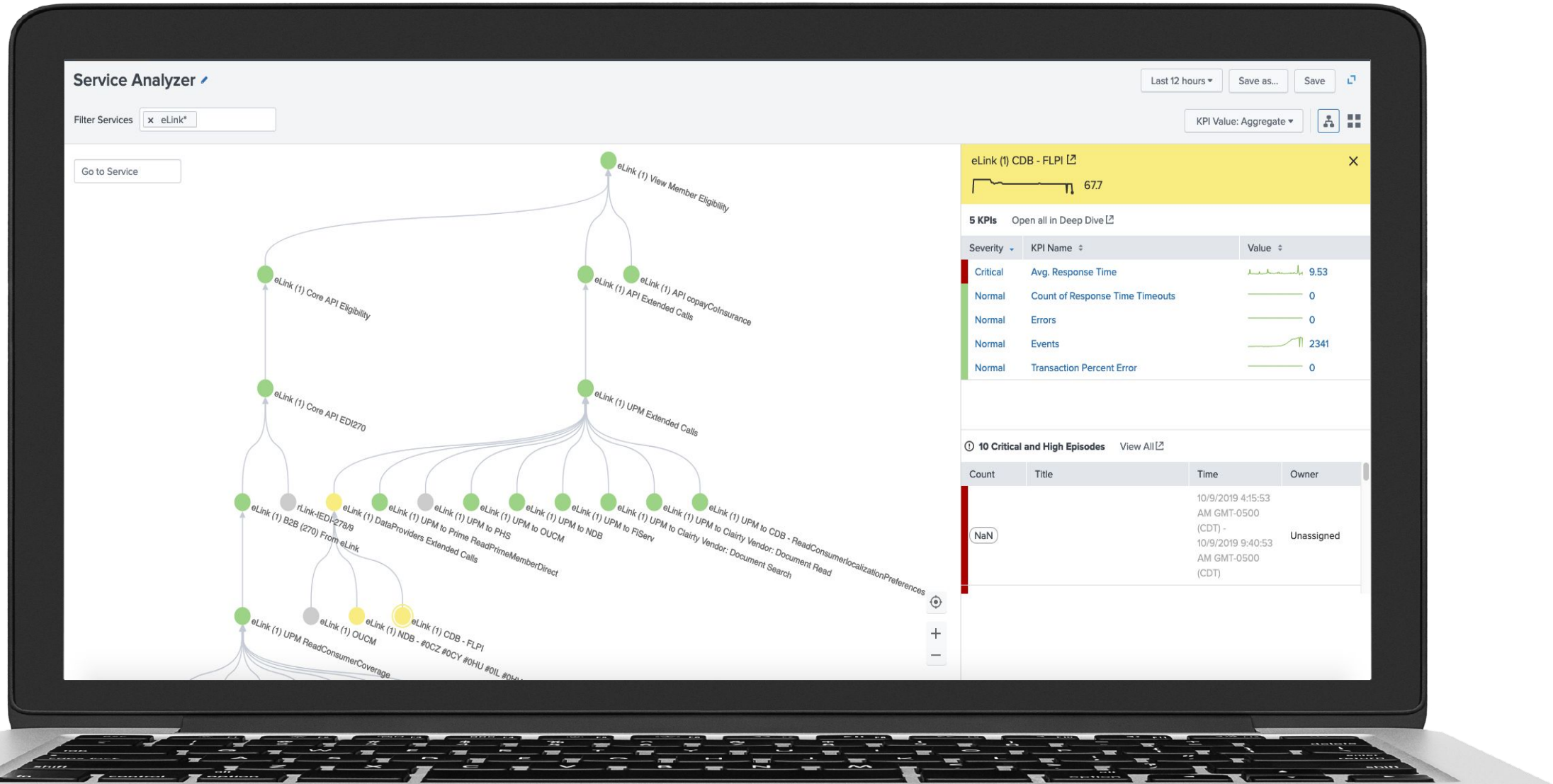
Example of Revised VBF Documentation



© 2019 SPLUNK INC.

Examples: LINK Provider

Example of Glass Table and Service Analyzer



© 2019 SPLUNK INC.

MyUHC - Login

MyUHC is the primary portal for customers to access their individual healthcare information. The customers are all of the people looking to access their healthcare information, and we have over 100,000 unique visitors to the site daily.

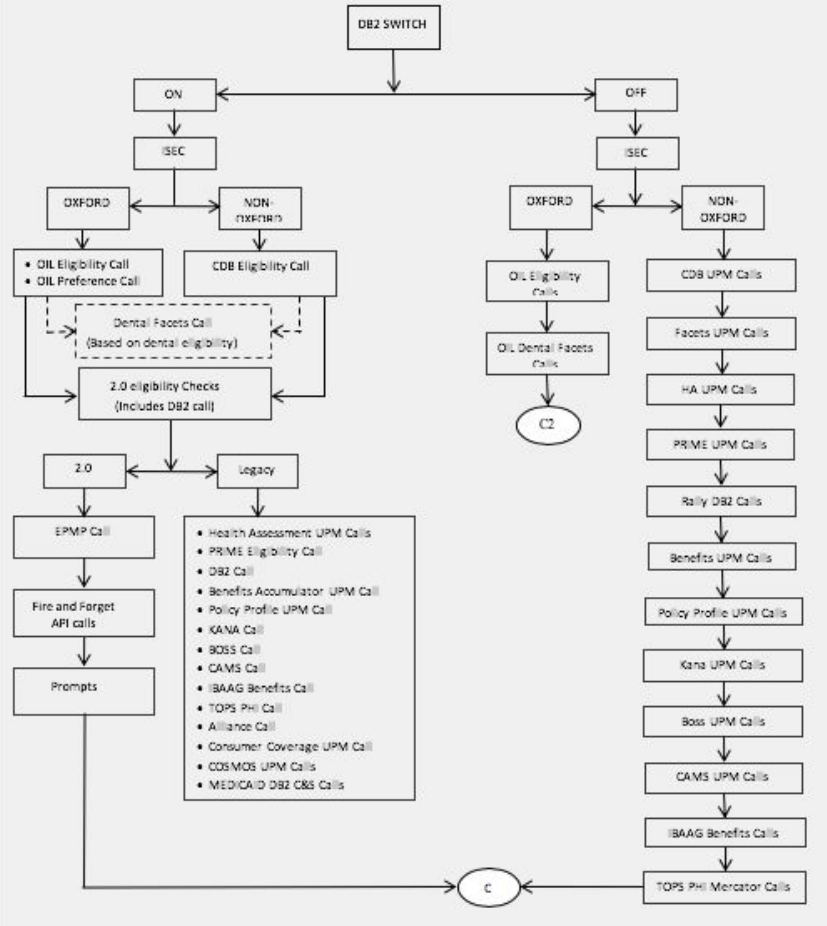
ITSI Stats

- 59 services across 7 different applications
- 350+ Key performance Indicators
- 10+ alerts

© 2019 SPLUNK INC.

Examples: MyUHC - Login

Example of Initial VBF Documentation

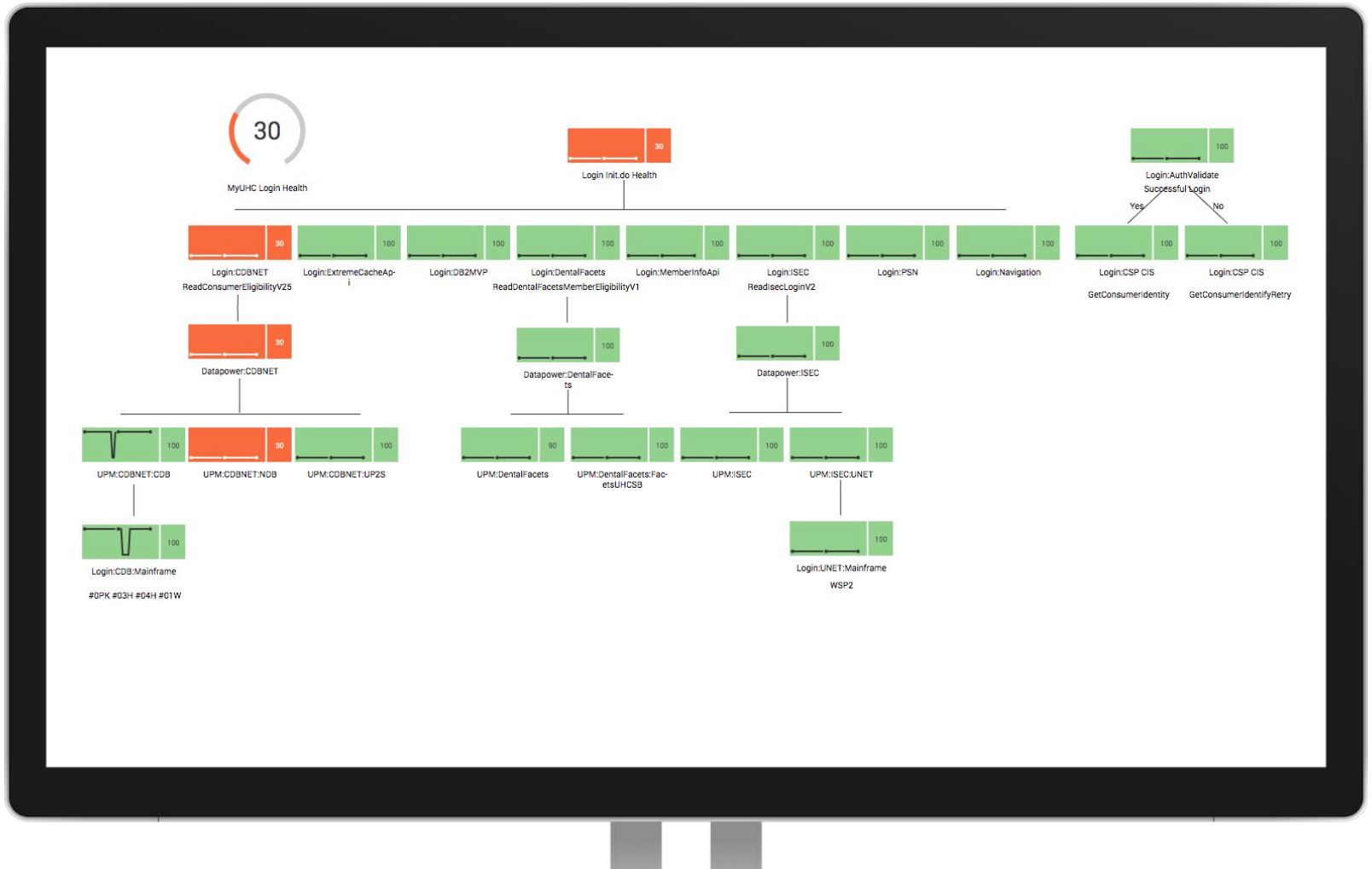


splunk> .conf19

© 2019 SPLUNK INC.

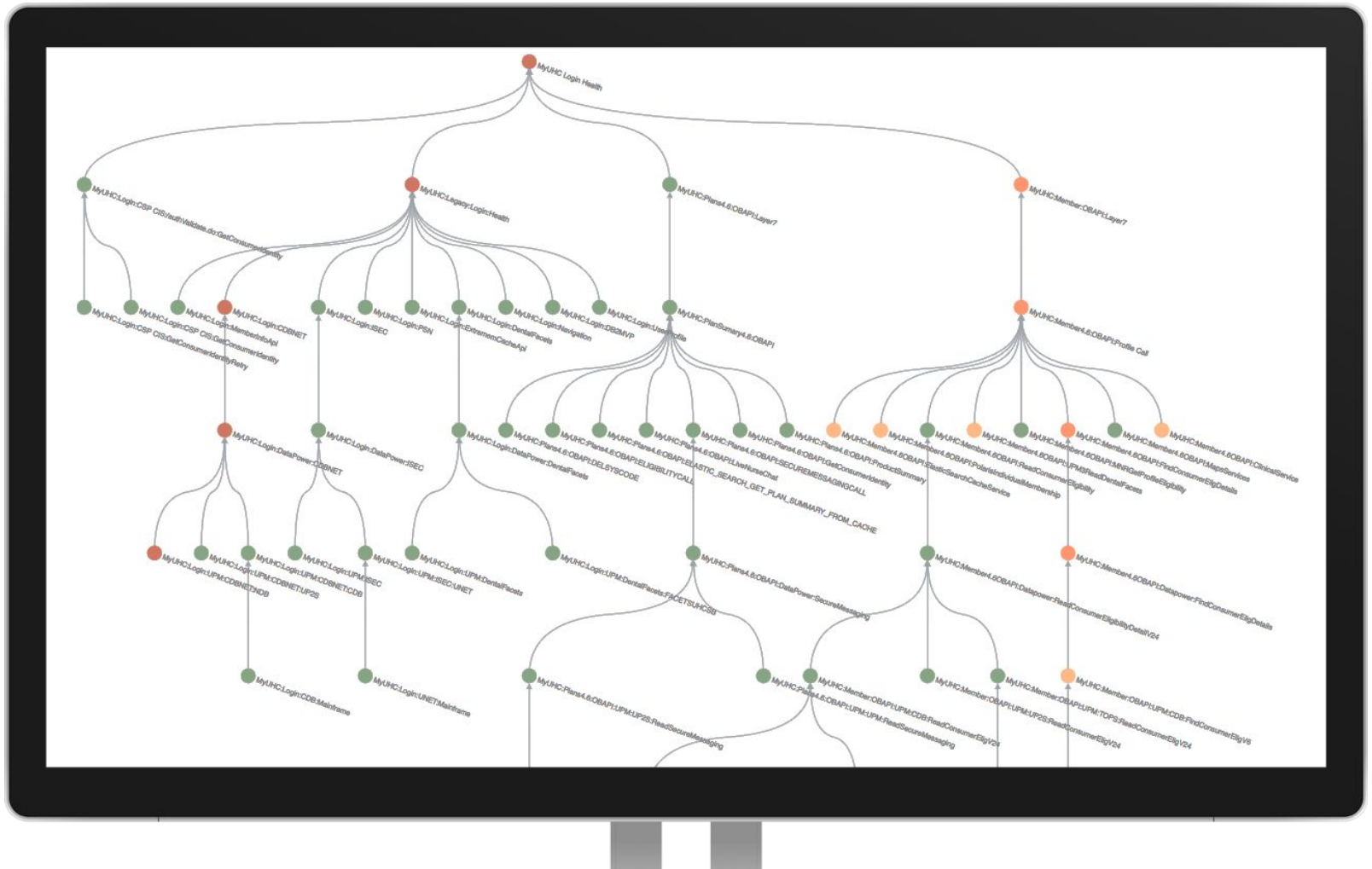
Examples: MyUHC

Example of Revised VBF Documentation



© 2019 SPLUNK INC.

Examples: MyUHC



splunk> .conf19

© 2019 SPLUNK INC.

Examples: MyUHC

Dive Deeper!



© 2019 SPLUNK INC.

Examples: OptumRX

The OptumRx Member portal provides members the ability to manage their maintenance medications online using a variety of self-service tools. Members have the ability to view and refill, renew or transfer prescriptions online. Members can also view their claim history, benefit information and order medical supplies.

ITSI Stats

- 350 services across 13 different applications broke out into 9 vital business functions
- 1500+ Key performance Indicators
- 45+ Alerts

© 2019 SPLUNK INC.

Examples: OptumRX

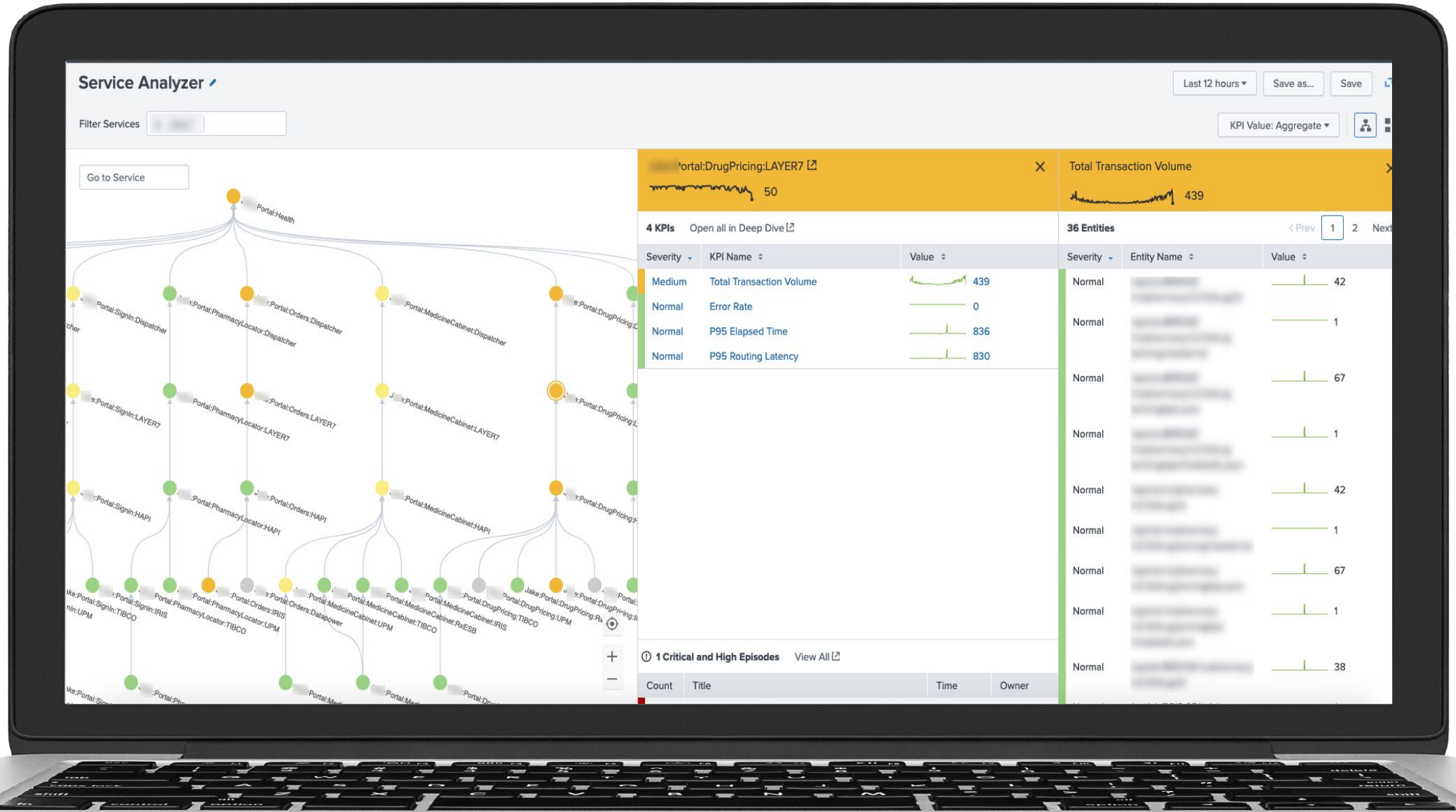


splunk> .conf19

© 2019 SPLUNK INC.

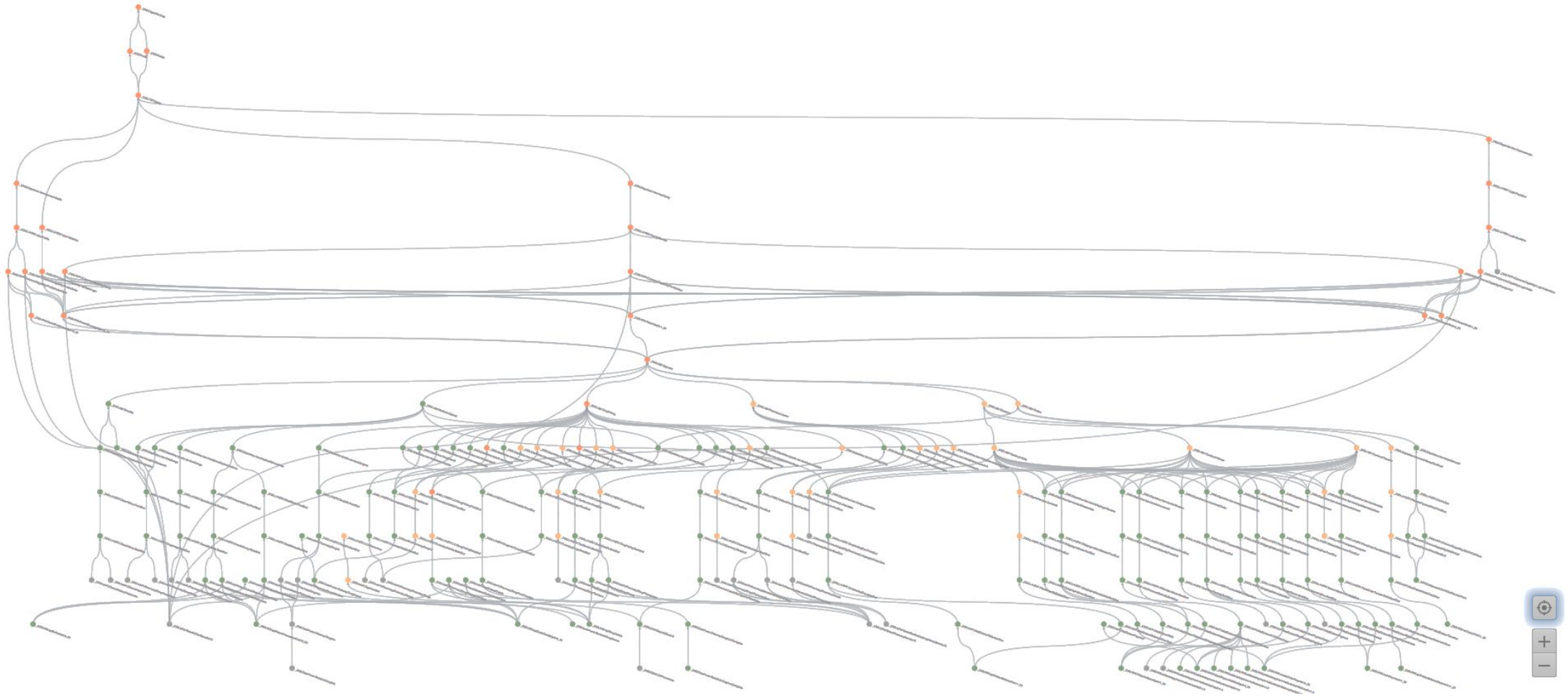
Examples: OptumRX

Ops teams can see where the problems are and drill down from there



© 2019 SPLUNK INC.

Examples: OptumRX



© 2019 SPLUNK INC.

Testimonials

LINK Provider

- "The fact that we can quickly see our dependent systems health (glass table) has helped reduce the time to identify issues resulting in faster remediation of war rooms"

– Andre, Link Provider Sr Tech Support Analyst

MyUHC

- "Splunk has become the primary tool our team uses for both triage and analysis of our systems. A year ago, war rooms opened with a variety of tools – now a days the first thing most people will see when the triage begins is a Splunk screen."

– Bharath, MyUHC Data Engineer

Optum Rx

- "Splunk helps us solve issues by providing a centralized log monitoring platform to be used by our operations group. We use Splunk ITSI to quickly monitor and identify customer impacting issues in our giant environment, which helps us with decreasing our impact resolution time."

– Sirisha, Optum Rx Software Engineer

© 2019 SPLUNK INC.

Key Takeaways

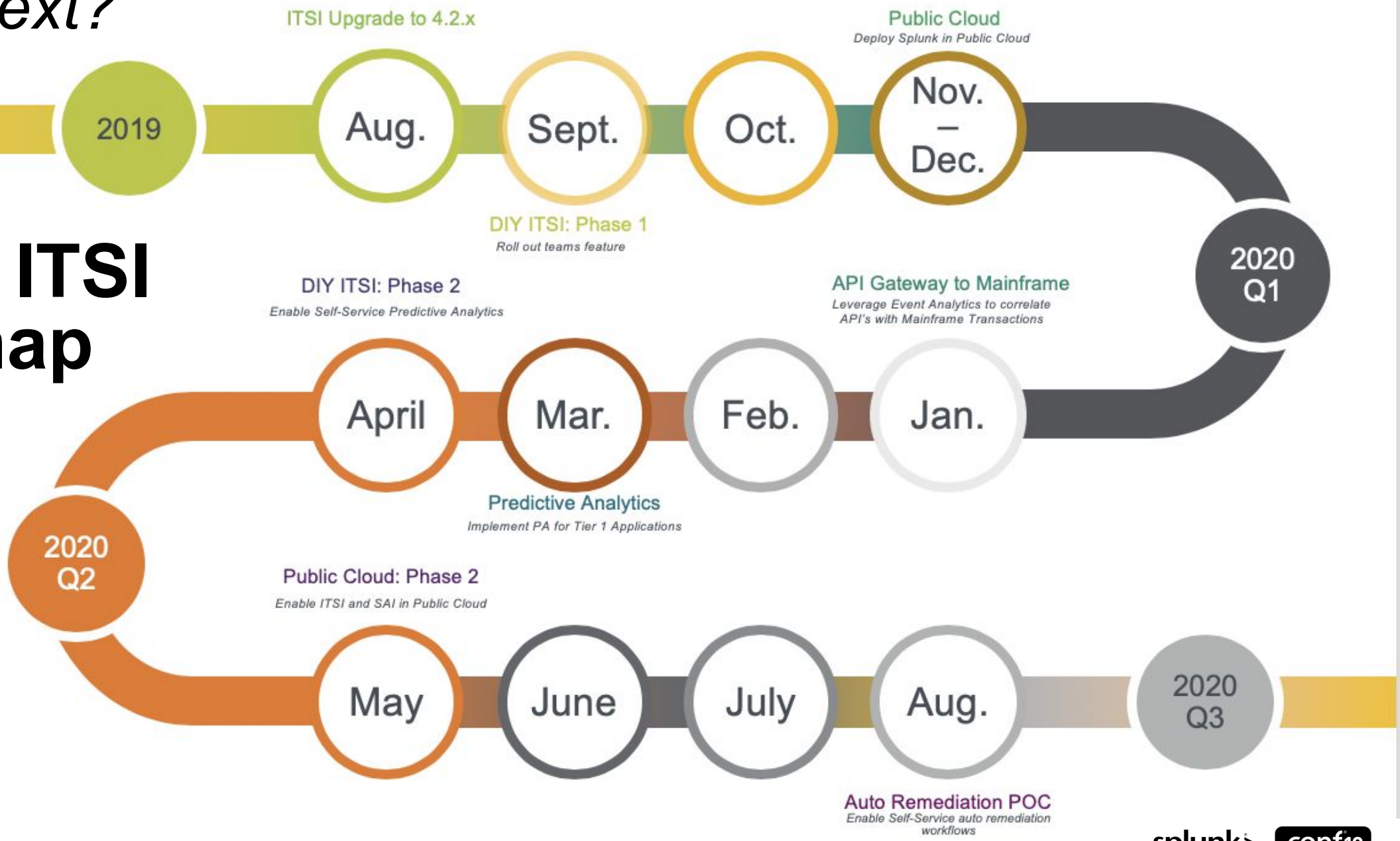
1. If you're onboarding your app logs, onboard the web server logs too!
2. Give them something they haven't had before
3. Knowledge transfer and training – Don't do everything for them
4. Use base searches!
5. Don't be a creep, follow scope!
6. Not everything needs to be built in ITSI
7. Re-use what you already have

What's Next?

Optum ITSI Roadmap

2019-2020

1 Year Plan



OPTUM

splunk> .conf19

© 2019 SPLUNK INC.



Q&A

splunk> .conf19

© 2019 SPLUNK INC.

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION

