



splunk®

Operational Intelligence

Decoding the Code of Your Applications

Aaron Garcia – Capital Group Companies

Nate Smalley – Splunk Inc.

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.

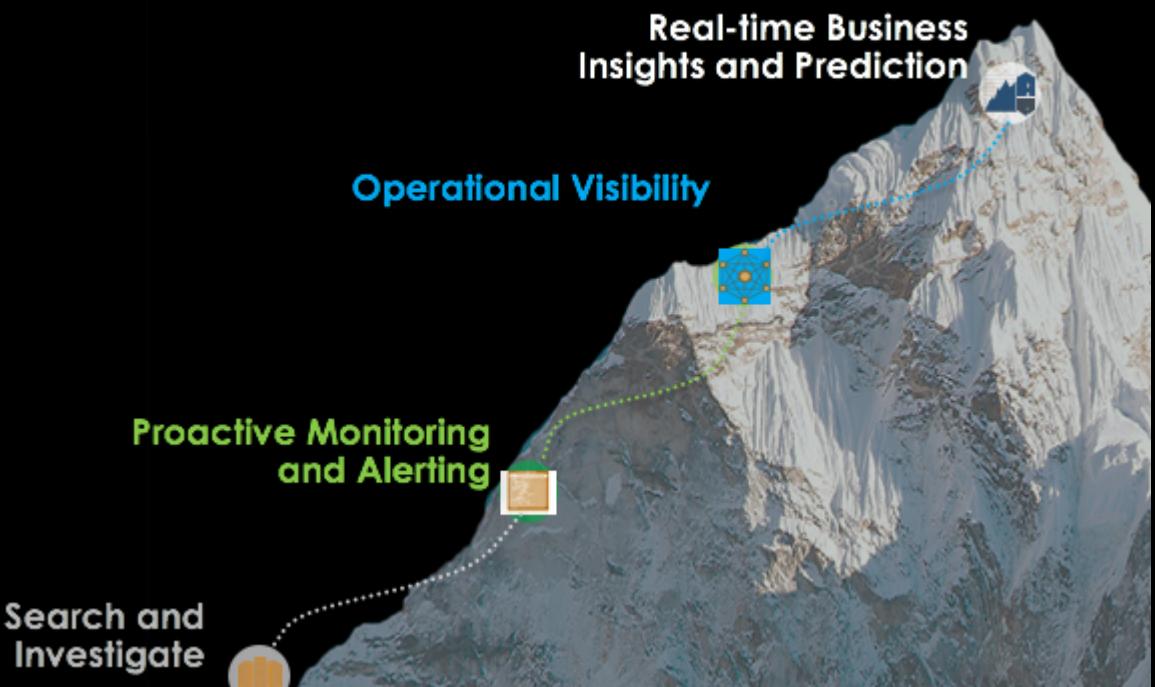
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements 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.

Splunk, Splunk>, Listen to Your Data, 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. © 2018 Splunk Inc. All rights reserved.

Agenda

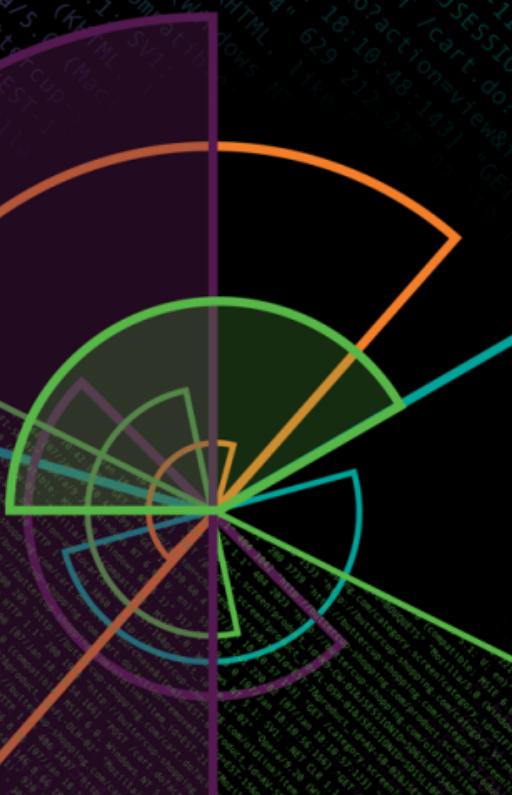
Are we in the right room?

- ▶ Who are these People?
 - ▶ Who is Capital Group Companies
 - ▶ The Journey of Application Insight
 - OI Level 1 – Basic Search
 - OI Level 2 – Splunk App
 - OI Level 3 – IT Service Intelligence
 - ▶ Moving into the Future

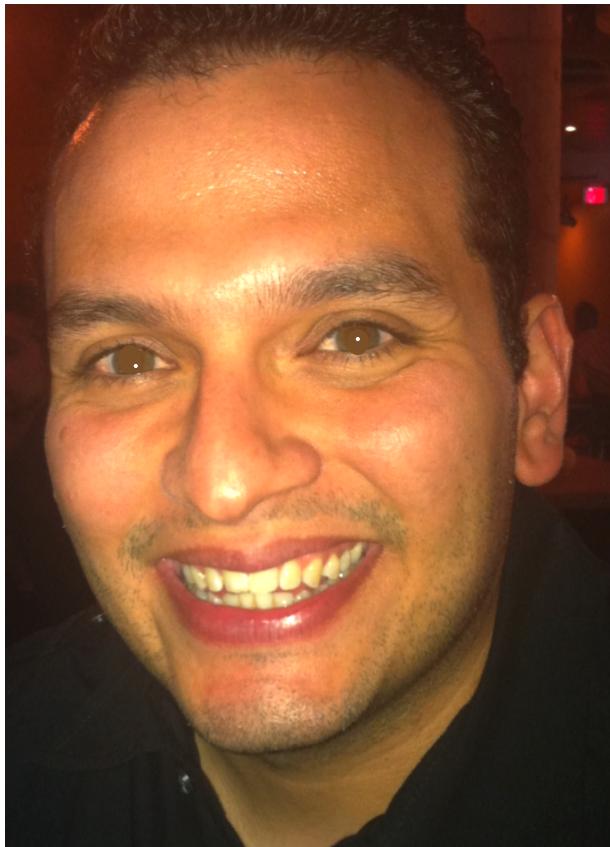


Who Are these Speakers?

Introductions



Aaron Garcia



- ▶ Technology Engineer with The Capital Group Companies
 - ▶ 15 Years in various support/engineering roles
 - ▶ Currently focused on workload automation and operational intelligence

Nate Smalley



- ▶ IT Operations Technologist (Reformed Security Guy)
- ▶ Former Technical Director of Security & Monitoring Tools Team – Apollo Group (University of Phoenix)
- ▶ Currently Splunk Sales Engineer Manager supporting the Largest Splunk Customers
- ▶ Enjoy Long walks across SNMP and Candle light dinners while fighting Operational Outages

Capital Group Companies

- ▶ Founded in 1931
- ▶ One of the oldest and largest investment management organizations in the world
- ▶ Relentless focus on delivering superior, consistent results for long-term investors using high-conviction portfolios, rigorous research and individual accountability.
- ▶ Offices worldwide



CAPITAL
GROUPSM

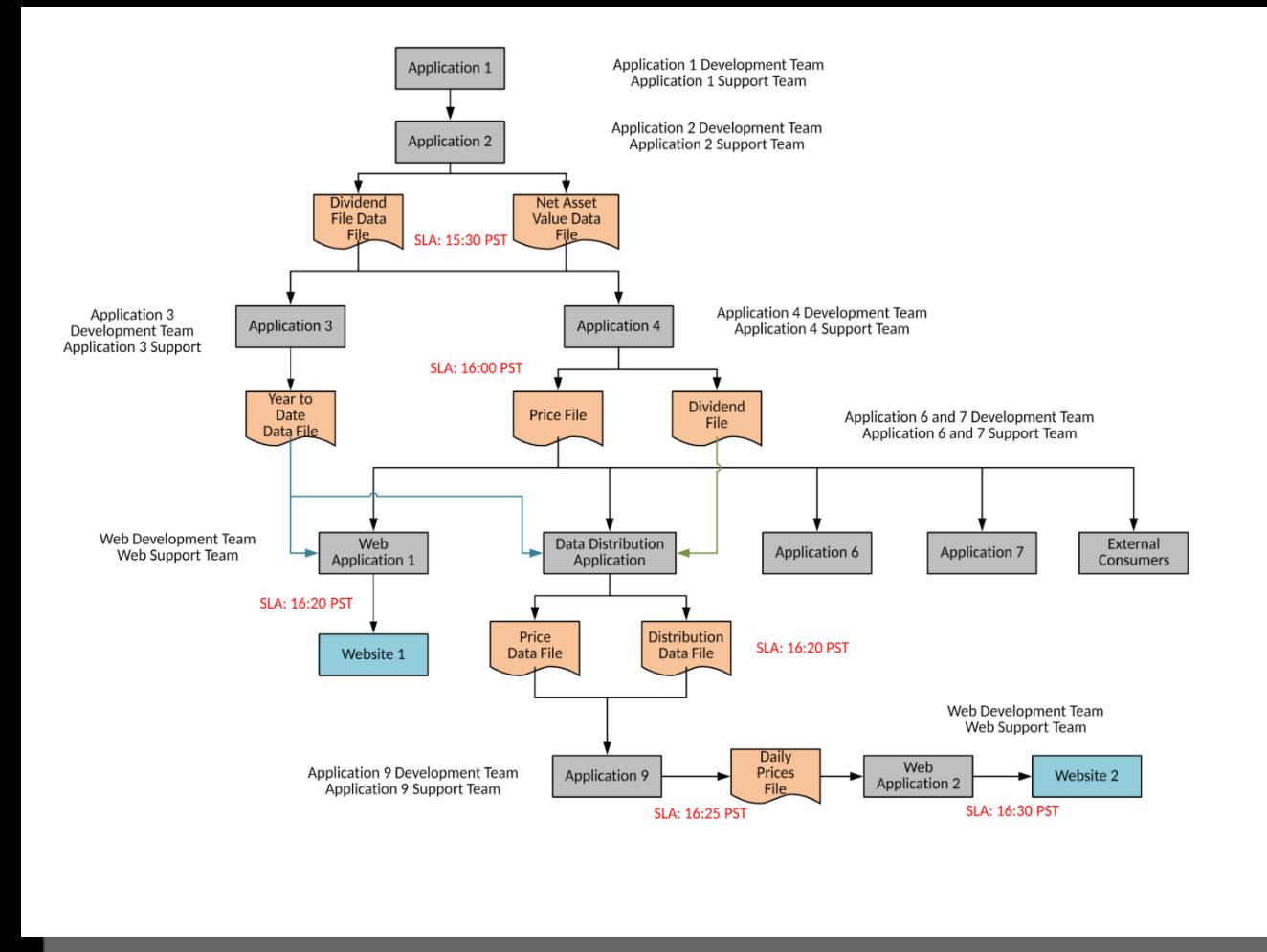
The Start: Pricing Process

Operation Level 1



The Pricing Process

- ▶ Price distribution is a key responsibility and heavily regulated
- ▶ Distribution consists of multiple applications and processes
- ▶ Traditional monitoring tools were focused mainly on the hardware running the applications
- ▶ Zero visibility into the file transfers

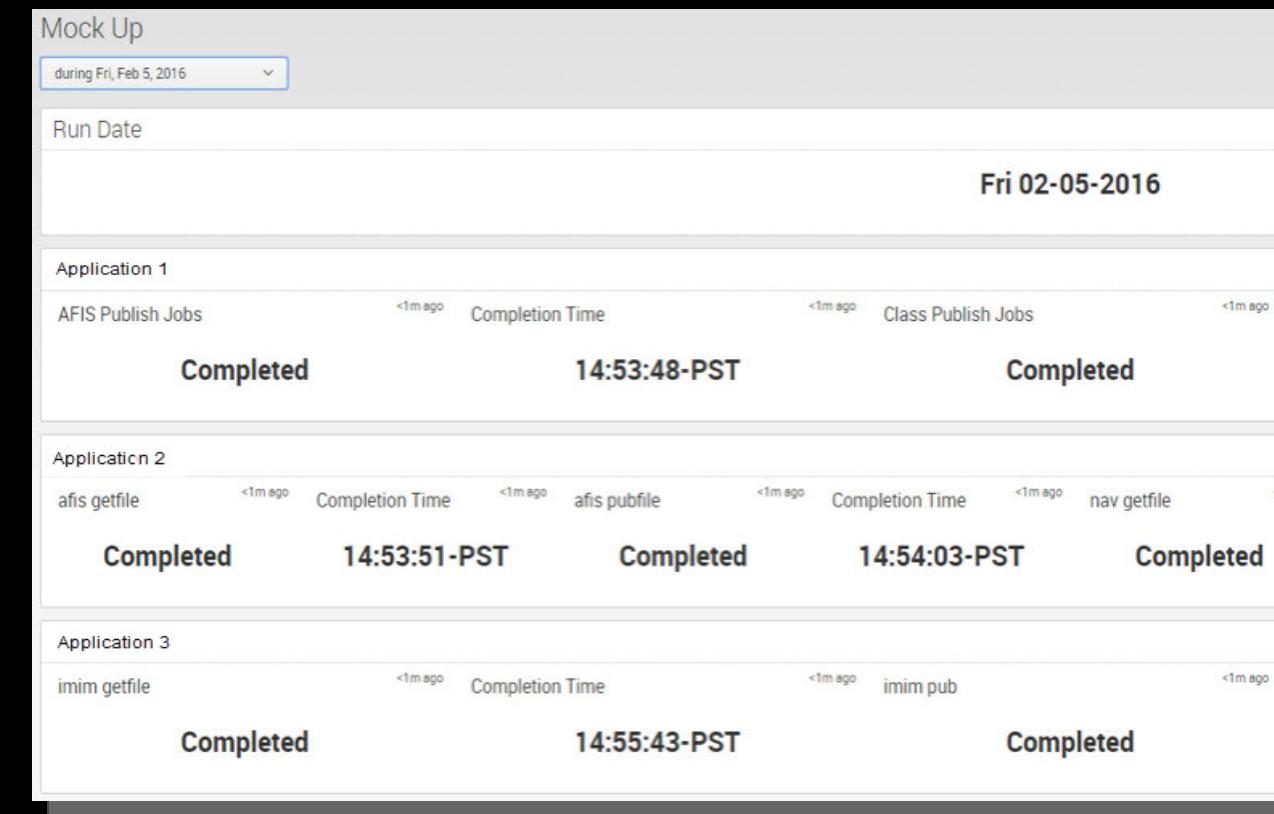


The Problem With Pricing

Where we started

- ▶ Call anyone and everyone who works on the applications
 - ▶ Create specific call out procedures in hopes of getting the right associates faster
 - ▶ All hands on deck during the process
 - ▶ Too much reliance on application developers and SMEs
 - ▶ Support calls were usually chaotic since there was never clear indication where the issue might be
 - ▶ Multiple callouts were often needed at times in order to find the right person

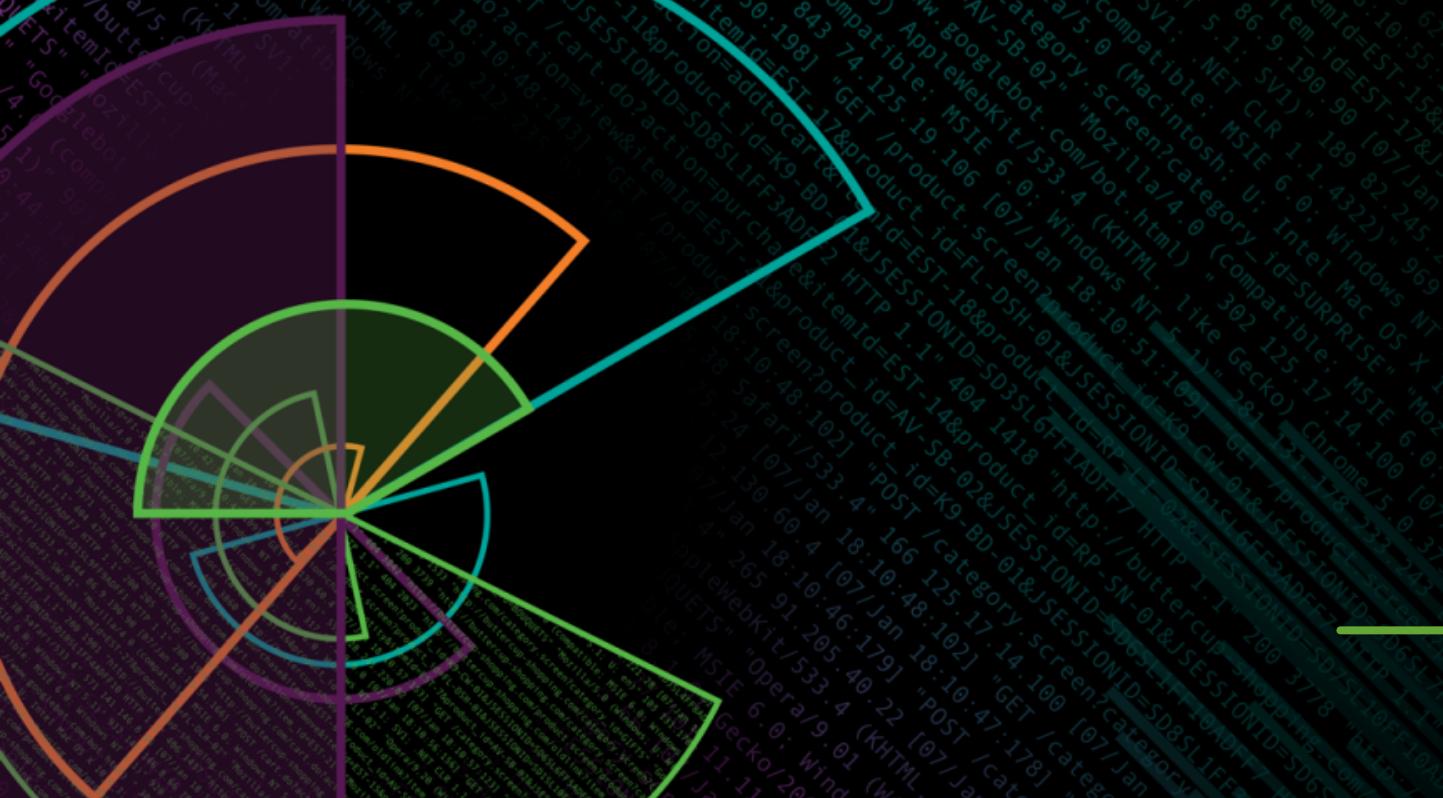
Early Prototypes Visualized Pricing



- ▶ Early prototypes were focused on if we could “see” what was happening in Pricing
 - ▶ The first prototypes proved that we could successfully translate Pricing into something anyone could understand
 - ▶ Rely less on specific domain knowledge and abstract the technology

The Middle: Splunk App

Operation Level 2



Transform Data Into Useful Views

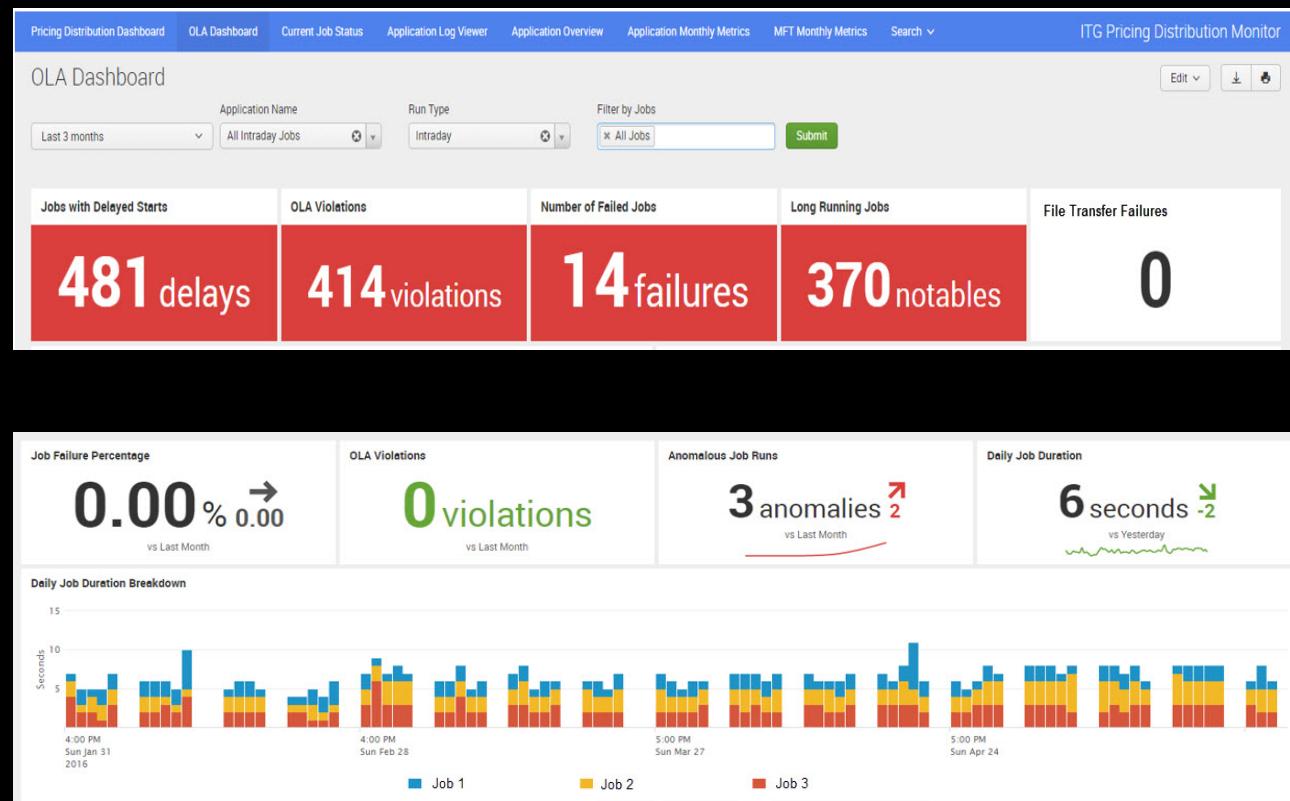
Codification of Use Case

- ▶ The goal was to consolidate and translate all the Pricing Data into something easy to understand
 - ▶ Service decomposition was done with each of the application teams in the pricing chain
 - ▶ The app was built in Splunk Core using out of the box knowledge objects

Pricing Distribution Dashboard	OLA Dashboard	Current Job Status	Application Log Viewer	Application Overview	Application Monthly Metrics	MFT Monthly Metrics	Search	ITG Pricing Distribution Monitor
Pricing Distribution Dashboard								
Job Period								
Yesterday	Intraday			Submit				
Job Completion								
Application 1	Application 2			Application 3			Application 4	
Completed: 3/3 jobs @ 14:58:06	Completed: 12/12 jobs @ 15:00:28			Completed: 5/5 jobs @ 15:13:57			Completed: 4/4 jobs @ 17:50:19	
Application 5	Application 6			Application 7			Web	
Completed: 4/4 jobs @ 15:10:42	Completed: 65/65 jobs @ 15:30:46			Completed: 5/5 jobs @ 15:15:36			Completed: 8/8 jobs @ 15:16:04	
Number Of Errors by Application								
Application 1	Application 2			Application 3			Application 4	
0 errors	0 errors			0 errors			0 errors	
Application 5	Application 6			Application 7			Web	
0 errors	0 errors			0 errors			0 errors	

Diving Deep

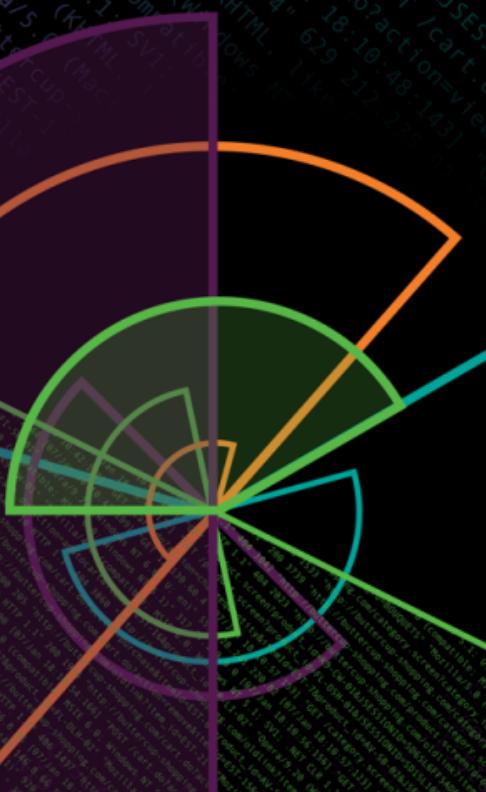
The Splunk Pricing App



- ▶ Issues can often be identified within seconds of opening the app
 - ▶ Identifying which application teams are needed to troubleshoot is extremely clear
 - ▶ SLA trending and metrics were finally available
 - ▶ Issues with file transfers could clearly be seen

Current State: Transitioning to Intelligence

Operation Level 3



Enter Splunk IT Service Intelligence

Predictive analytics for real-time insights, simplified operations and root cause analysis

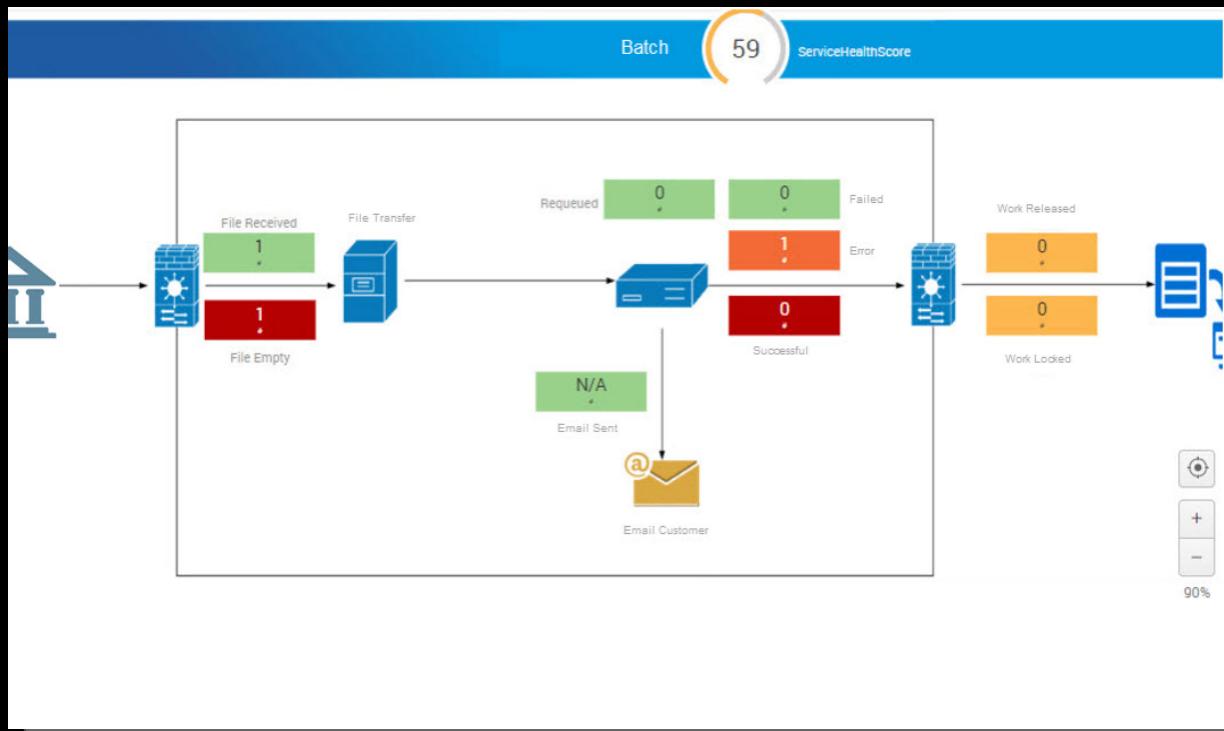
Dependency Mapping and more

- ▶ Faster delivery of value to our customers
- ▶ Creating meaningful visuals and alerting
- ▶ True correlation of application dependencies
- ▶ Elimination of alert fatigue



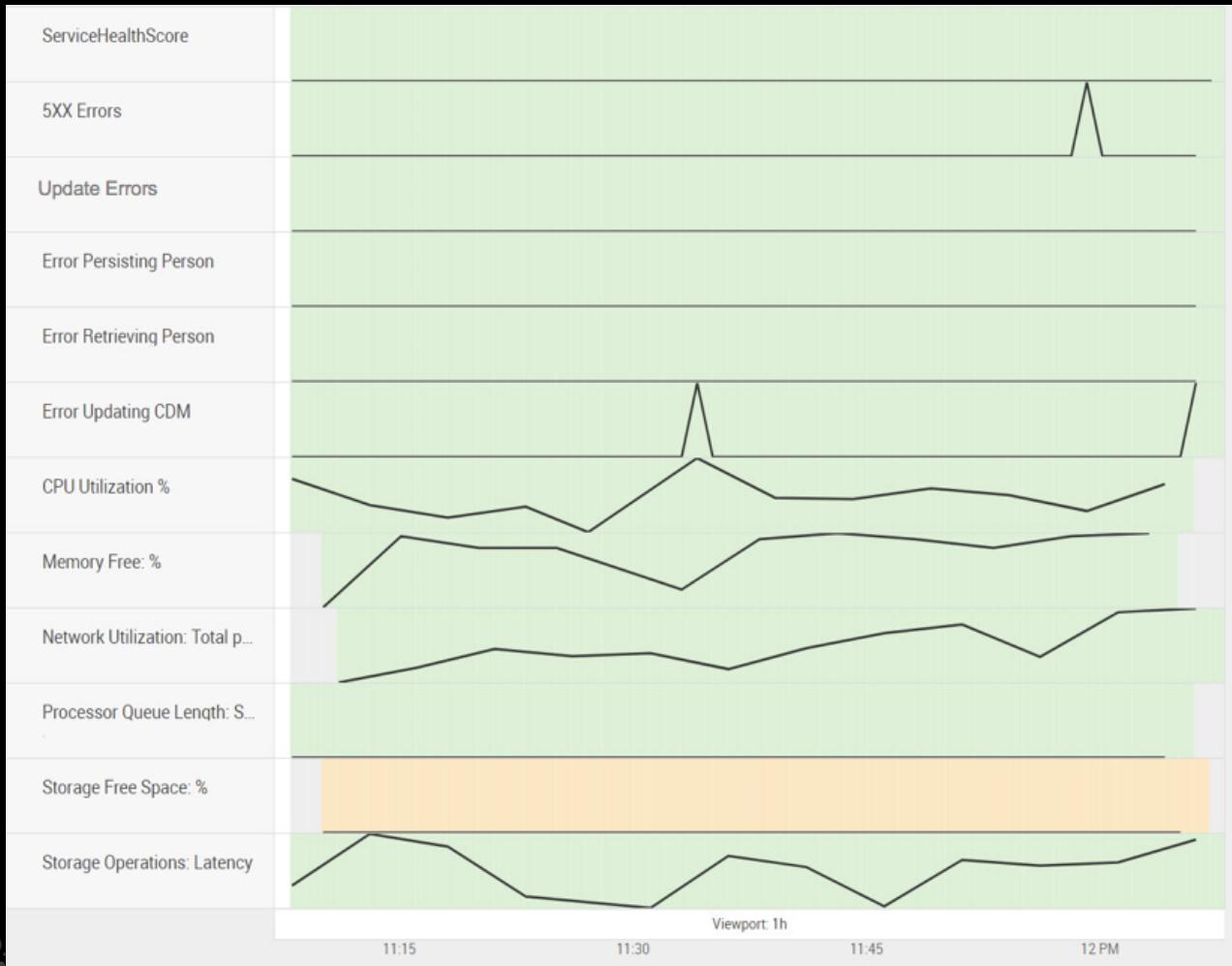
Adoption Through IT Service Intelligence

Everyone sharing a View



- ▶ Support teams and development teams can see the same thing
 - ▶ Faster decisions can be made on what needs to be looked at
 - ▶ One tool can be used for all aspects of troubleshooting
 - ▶ Alerting can be tailored to what matters

Data Driven Operations



- ▶ Machine and application insights on one view can greatly reduce the troubleshooting time
- ▶ In the past multiple tools were needed to deliver the complete picture
- ▶ System administrator knowledge was often needed to retrieve machine metrics

The Future: Moving Forward

Operation Level 3 and beyond



What Else is There?

Moving Forward

- ▶ Getting the right information to the right people faster
- ▶ Meaningful and actionable alerting
- ▶ Bi-directional Integration with ServiceNow
- ▶ Service templating
- ▶ Predictive Analytics

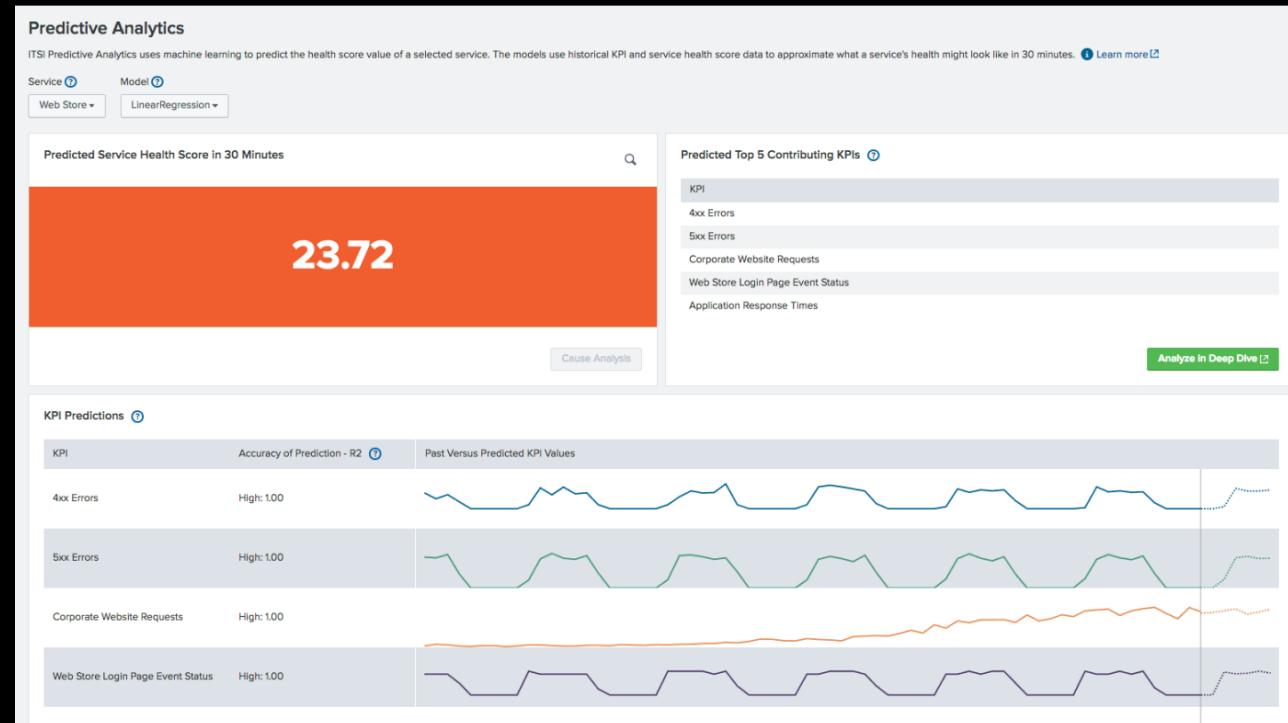
The screenshot shows a Splunk search results page with the following details:

- Search Bar:** 2 groups, Last 24 hours, Policy: , Add Filter, search
- Event List:**
 - Application 1 (Thu Apr 12 2018 17:15:01 GMT-0700 (PDT) - Fri Apr ...)
 - Application 1 (Wed Apr 11 2018 14:50:02 GMT-0700 (PDT) - Thu Ap...)
- Acknowledge:** Application 1 (Thu Apr 12 2018 17:15:01 GMT-0700 (PDT) - Fri Apr 13 2018 09:00:01 GMT-0700 (PDT))
- Filter Options:** Medium, New, Unassigned, Ack
- Description:** Application Interaction status was normal (Health Score=100.0) at 2018-04-12 17:14:00.000 PM
- Group Aggregation Details:** 282 Notable Events are grouped based on the aggregation policy. (● 282)
- All Tickets:** Service Now - INC0011376
- Contributing KPIs:** Open all in Deep Dive
 - Application 1
 - ServiceHealthScore
- Possible Affected Services:** Open all in Deep Dive
 - Application 1

Roadmap to More Value

NO MTTR? SAY WHAT

- ▶ Out of the Box capability to provide imminent outage detection and alerting
- ▶ Provide Analysts/App Teams with pre-emptive notification before degradation in Availability
- ▶ More Time to diagnose and get the right folks to correct an issue



Three Takeaways

Don't leave empty handed!

1. Start by Seeing More

We began by visualizing our entire pricing process, bringing all of the data and services needed into a single view, so we could understand more.

2. Make Sure What You See Is Useful

We made our visualized pricing data easier to understand, so teams could investigate quicker and take the actions they needed quicker.

3. Leverage ML and AI To Be Proactive

We are able to see ahead of some outages before they occur by using the predictive capabilities, alerting, and integrations with other tools

Q&A

Section subtitle goes here

Thank You

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

