



splunk®

Orchestrating an Improved Customer Experience

Utilize Splunk ITSI Insights to Drive Automation

Scott Hamrick | PwC, IT Director – Operations Analytics

Patrick Combs | TCS, Data Analytics Leader

October 2018 | Version 2.0

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.

Today's Speakers



PATRICK COMBS

TCS, Data Analytics Leader



SCOTT HAMRICK

PwC, IT Director – Operations Analytics

PricewaterhouseCoopers

Our purpose is to build trust in society and solve important problems

- ▶ Globally - 223,468 people in 743 locations in 157 countries
- ▶ 46k partners and staff in the US
- ▶ Provide industry-focused assurance, advisory and tax services for over 90% of the companies in the Fortune Global 500 list



PRICEWATERHOUSECOOPERS

Problem Statement

Implementing & Measuring Analytic Value

Sub-optimal IT processes

- ▶ Large, complex environment
- ▶ Frequent Change Requests
- ▶ Random outages
- ▶ Slow resolution time for failures
- ▶ Lack of confidence from end users

Overall Impact

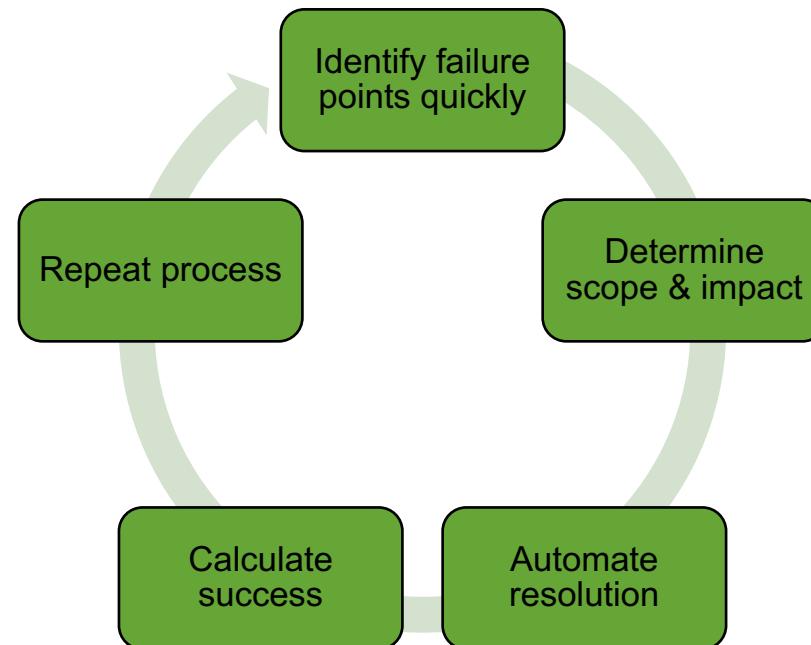
- ▶ Increased support costs
- ▶ Extensive manual effort
- ▶ Extended unplanned downtime
- ▶ Negative customer feedback
- ▶ Rogue IT efforts

Utilize analytics to automate issue resolution

Imagine the Possible: What If?

Implementing & Measuring Analytic Value

Anomaly detection



Measure Improvement & Impact

- Reduce cost
- Automate manual tasks
- Eliminate unplanned downtime
- Reduce MTTR for Incidents
- Quantify / Track User Experience

Data leads to action...action to results...results to value

IT Operations Analytics

“Sunlight is said to be the best of disinfectants”

Justice Louis D. Brandeis



PwC ITOA Mission

Enabling & Measuring Superior Client Experience

Holistic approach to data analytics

- ▶ Become “The” source of information
 - ▶ Aggregate all relevant data
 - ▶ Organize complex data sources
 - ▶ Offer guided navigation
 - ▶ Provide targeted data detail

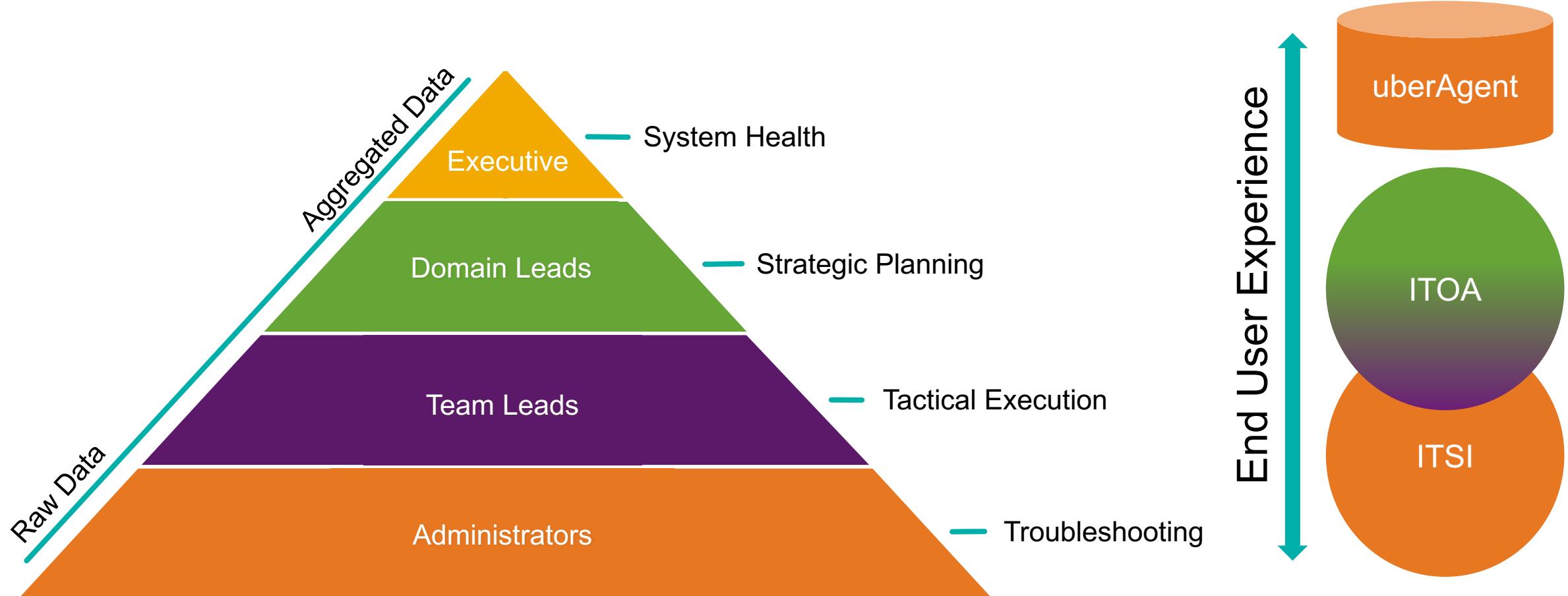
Critical Success Factors

- ▶ Quantify / Track User Experience
 - ▶ Eliminate unplanned downtime
 - ▶ Reduce MTTR for Incidents
 - ▶ Improve IT capacity management
 - ▶ Remove Manual Reporting

Measure and improve end-to-end user experience

Pyramid of Transparency™

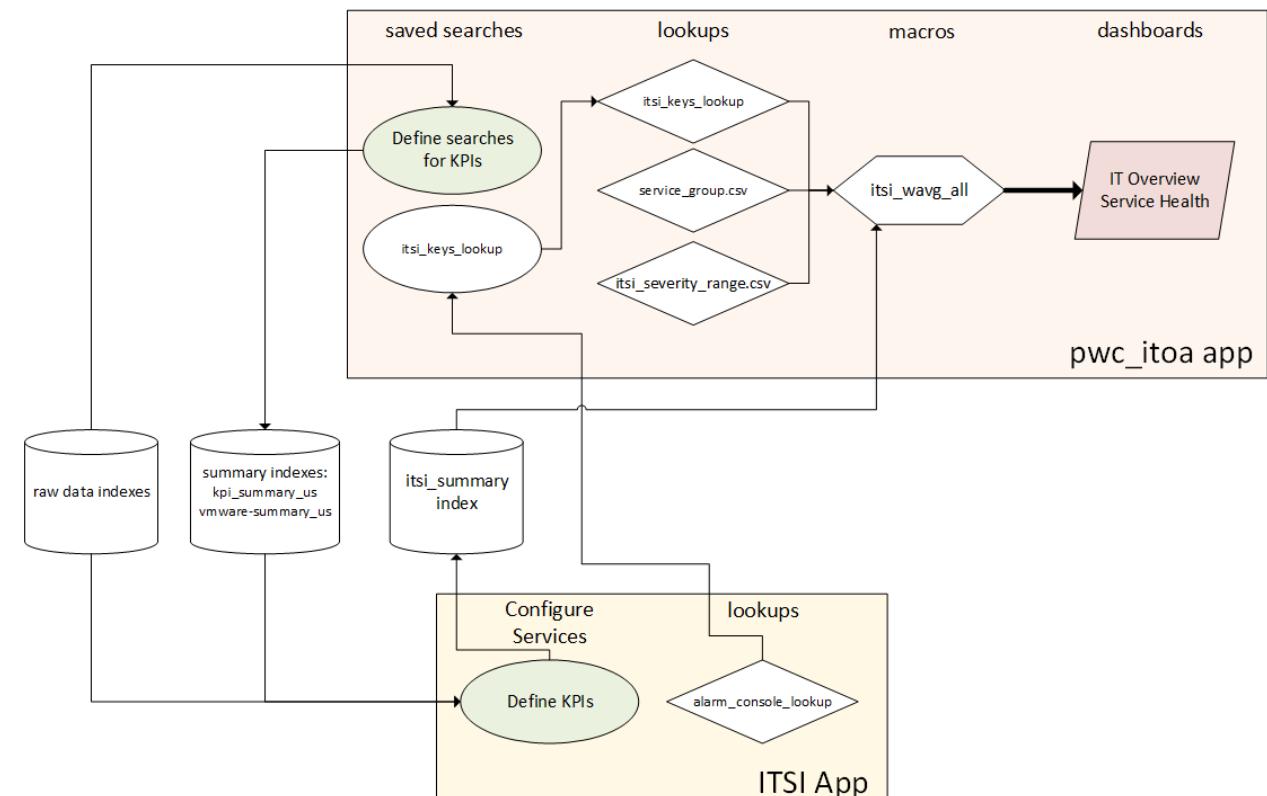
Data targeted to organizational role



ITSI Driving Applied Analytics Through ITOA

Key components required by ITOA app

- ▶ ITSI Service / KPI Definitions
- ▶ ITSI Entity and Base Searches
- ▶ ITOA Lookups
- ▶ ITOA Weighted Average Macro
- ▶ ITOA Framework to present results



IT Operations Analytics Product

Executive-level health score overview

The screenshot shows a tablet displaying the PwC IT Executive-level health score overview dashboard. The dashboard has a top navigation bar with links: Overview, Infrastructure, Service Health, Customer Experience, IT Service Management, Troubleshooting, Raw Data, Help, and a PwC IT logo. Below the navigation is a section titled "Overview" with a sub-section "Health Score Details". The main area is divided into four main sections: Infrastructure, Service Health, Customer Experience and Service Management, and Core Services. Each section contains a summary card with two green checkmarks and a detailed table below it.

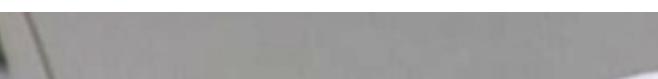
Infrastructure			Service Health			Customer Experience and Service Management																																																					
PERFORMANCE	CAPACITY		BUSINESS APPS	CORE SERVICES		CUSTOMER EXPERIENCE	SERVICE MANAGEMENT																																																				
Performance			Business Applications			Customer Experience																																																					
<table border="1"> <thead> <tr> <th>Performance</th> <th>Status</th> <th>Health Score</th> </tr> </thead> <tbody> <tr> <td>Palo Alto Firewall</td> <td></td> <td>93</td> </tr> <tr> <td>VMware Performance</td> <td></td> <td>95</td> </tr> <tr> <td>Network</td> <td></td> <td></td> </tr> <tr> <td>Wireless</td> <td></td> <td></td> </tr> <tr> <td>Storage</td> <td></td> <td></td> </tr> </tbody> </table>			Performance	Status	Health Score	Palo Alto Firewall		93	VMware Performance		95	Network			Wireless			Storage			<table border="1"> <thead> <tr> <th>Business Application Service</th> <th>Status</th> <th>Health Score</th> </tr> </thead> <tbody> <tr> <td>MyPortfolio</td> <td></td> <td>72</td> </tr> <tr> <td>CIA</td> <td></td> <td>74</td> </tr> <tr> <td>Feedback</td> <td></td> <td>74</td> </tr> <tr> <td>KSG - Profile</td> <td></td> <td>74</td> </tr> <tr> <td>Tax Source</td> <td></td> <td>74</td> </tr> </tbody> </table>			Business Application Service	Status	Health Score	MyPortfolio		72	CIA		74	Feedback		74	KSG - Profile		74	Tax Source		74	<table border="1"> <thead> <tr> <th>Customer Experience</th> <th>Status</th> <th>Health Score</th> </tr> </thead> <tbody> <tr> <td>Interactions</td> <td></td> <td>73</td> </tr> <tr> <td>Incidents</td> <td></td> <td>100</td> </tr> <tr> <td>Major Incidents</td> <td></td> <td>100</td> </tr> <tr> <td>Customer Satisfaction</td> <td></td> <td>100</td> </tr> </tbody> </table>			Customer Experience	Status	Health Score	Interactions		73	Incidents		100	Major Incidents		100	Customer Satisfaction		100
Performance	Status	Health Score																																																									
Palo Alto Firewall		93																																																									
VMware Performance		95																																																									
Network																																																											
Wireless																																																											
Storage																																																											
Business Application Service	Status	Health Score																																																									
MyPortfolio		72																																																									
CIA		74																																																									
Feedback		74																																																									
KSG - Profile		74																																																									
Tax Source		74																																																									
Customer Experience	Status	Health Score																																																									
Interactions		73																																																									
Incidents		100																																																									
Major Incidents		100																																																									
Customer Satisfaction		100																																																									
Capacity			Core Services			Service Management																																																					
<table border="1"> <thead> <tr> <th>Capacity</th> <th>Status</th> <th>Health Score</th> </tr> </thead> <tbody> <tr> <td>VMware Capacity</td> <td></td> <td>95</td> </tr> <tr> <td>Network</td> <td></td> <td></td> </tr> <tr> <td>Wireless</td> <td></td> <td></td> </tr> <tr> <td>Firewall</td> <td></td> <td></td> </tr> <tr> <td>Storage</td> <td></td> <td></td> </tr> </tbody> </table>			Capacity	Status	Health Score	VMware Capacity		95	Network			Wireless			Firewall			Storage			<table border="1"> <thead> <tr> <th>Core Service</th> <th>Status</th> <th>Health Score</th> </tr> </thead> <tbody> <tr> <td>IdAM</td> <td></td> <td>86</td> </tr> <tr> <td>AD-DNS</td> <td></td> <td>89</td> </tr> <tr> <td>Siteminder</td> <td></td> <td>94</td> </tr> <tr> <td>MobileIron</td> <td></td> <td>94</td> </tr> <tr> <td>ED</td> <td></td> <td>99</td> </tr> </tbody> </table>			Core Service	Status	Health Score	IdAM		86	AD-DNS		89	Siteminder		94	MobileIron		94	ED		99	<table border="1"> <thead> <tr> <th>Service Management</th> <th>Status</th> <th>Health Score</th> </tr> </thead> <tbody> <tr> <td>Change</td> <td></td> <td>100</td> </tr> <tr> <td>Release</td> <td></td> <td>100</td> </tr> <tr> <td>Problem</td> <td></td> <td>100</td> </tr> </tbody> </table>			Service Management	Status	Health Score	Change		100	Release		100	Problem		100			
Capacity	Status	Health Score																																																									
VMware Capacity		95																																																									
Network																																																											
Wireless																																																											
Firewall																																																											
Storage																																																											
Core Service	Status	Health Score																																																									
IdAM		86																																																									
AD-DNS		89																																																									
Siteminder		94																																																									
MobileIron		94																																																									
ED		99																																																									
Service Management	Status	Health Score																																																									
Change		100																																																									
Release		100																																																									
Problem		100																																																									

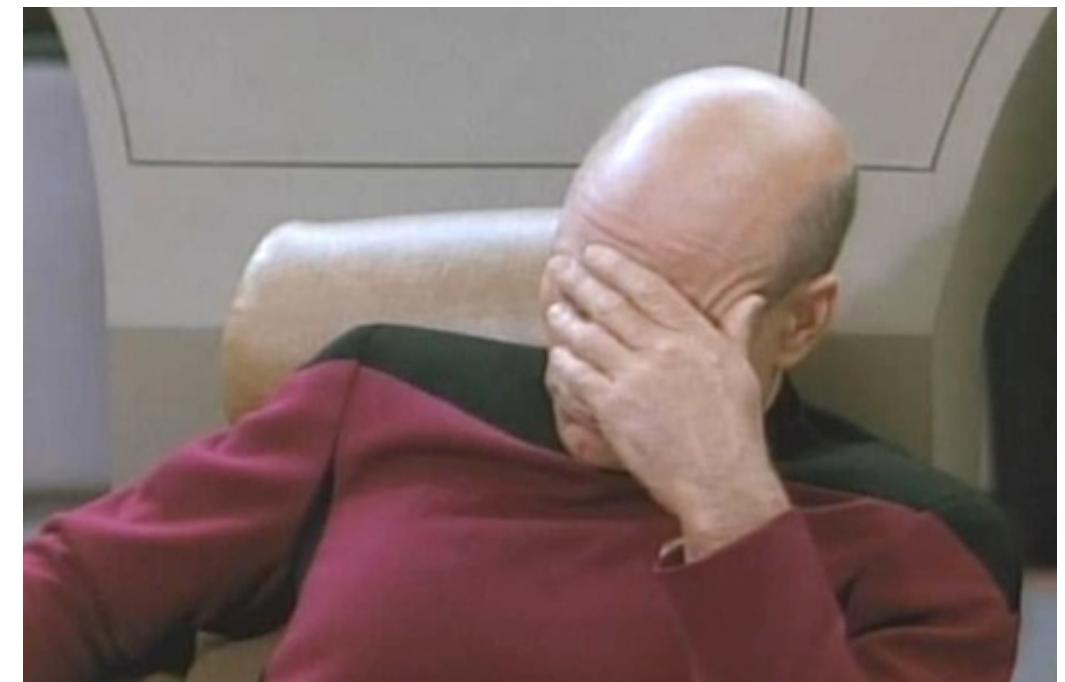
Customized app
providing near real-time
visibility of service health

- ▶ Core Services
- ▶ Applications
- ▶ Infrastructure
- ▶ Service Management

Top 5 Reactions to ITOA

Feedback we most frequently received

1. Splunk is the key to every initiative we have planned for the next 5 years!
 2. OK, what's next??
 3. What does Splunk say about...
 4. That's great, but can it do _____?
 5. Wait...what??



Applied Analytics

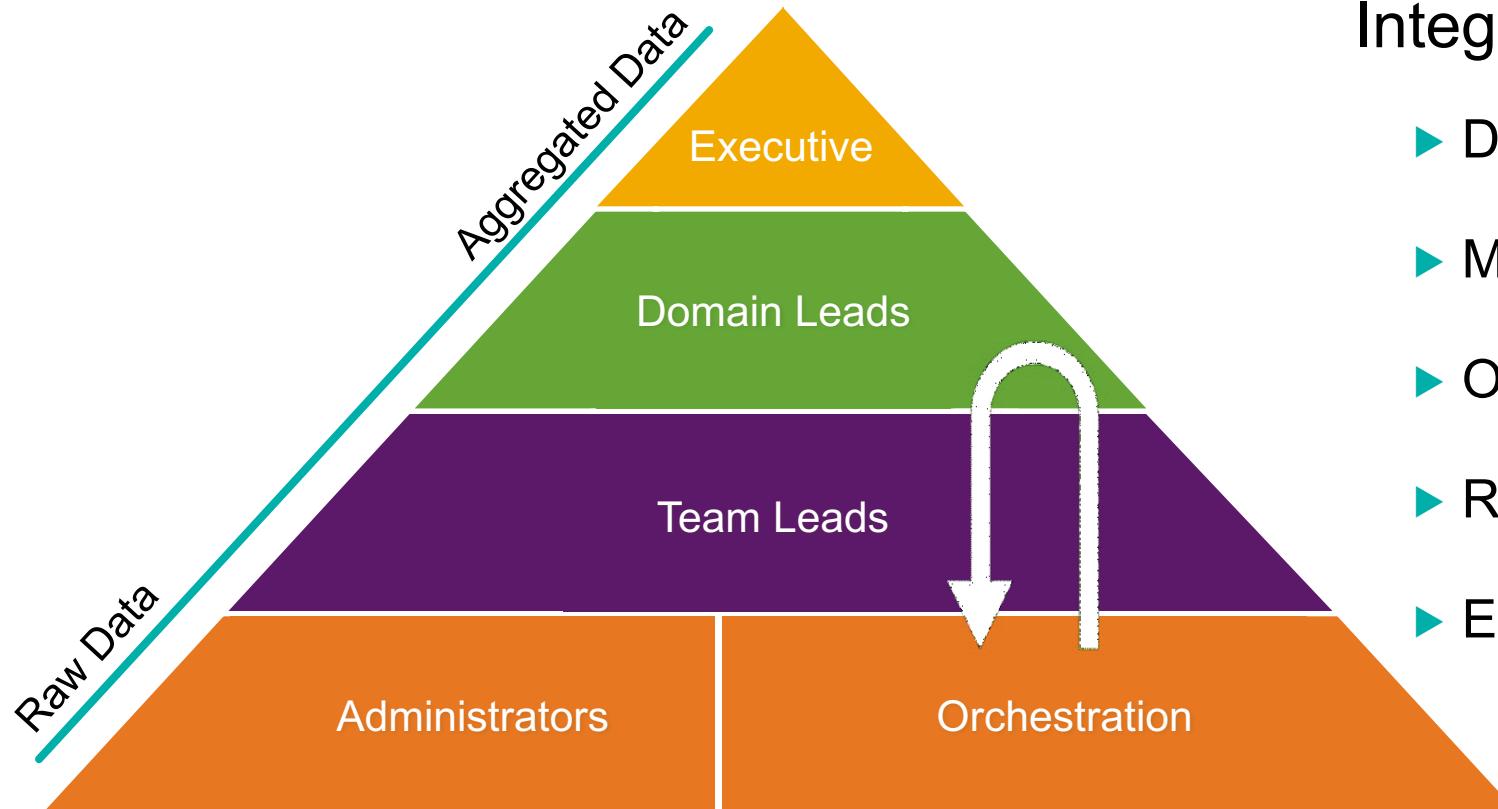
"Analytics without action are less valuable"

Anonymous CTO



New ITOA Mission

Utilizing Analytics to drive automation

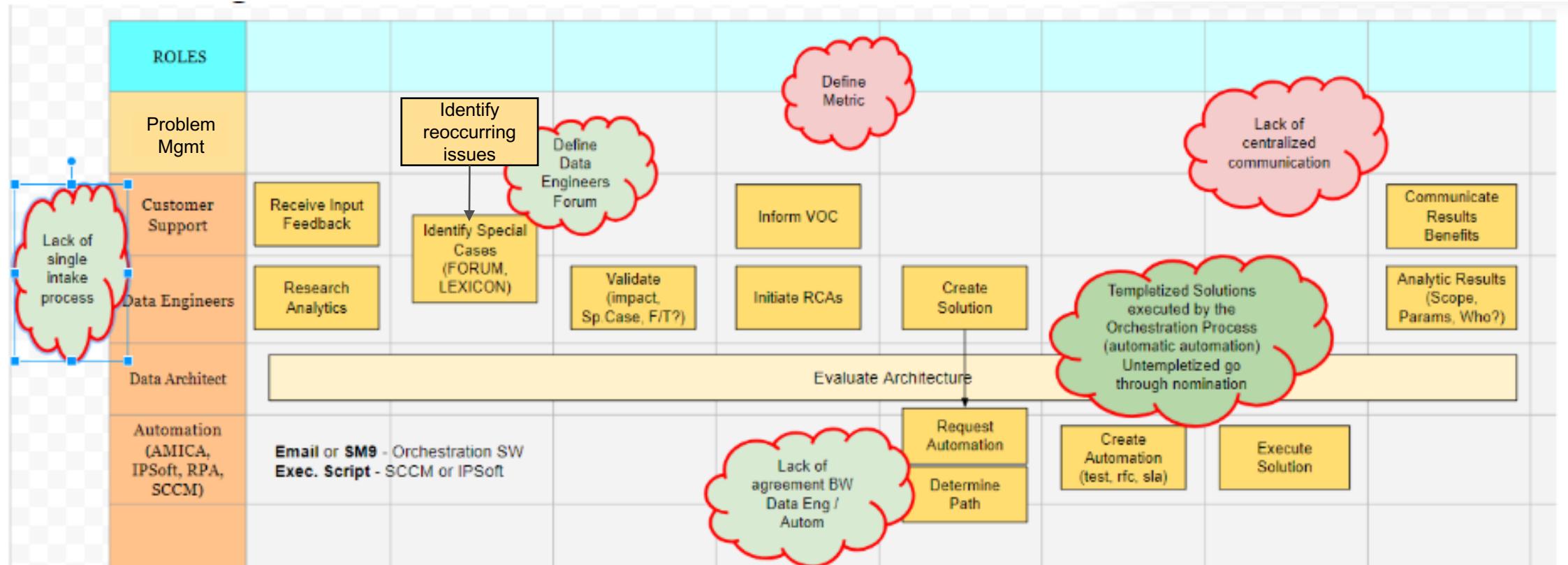


Integrate analytics with Automation

- ▶ Define metrics through ITSI
- ▶ Measure anomalies
- ▶ Orchestrate alerts to initiate action
- ▶ Resolve issues near real-time
- ▶ Eliminate re-occurrence

This is great...but its only the first half of the solution

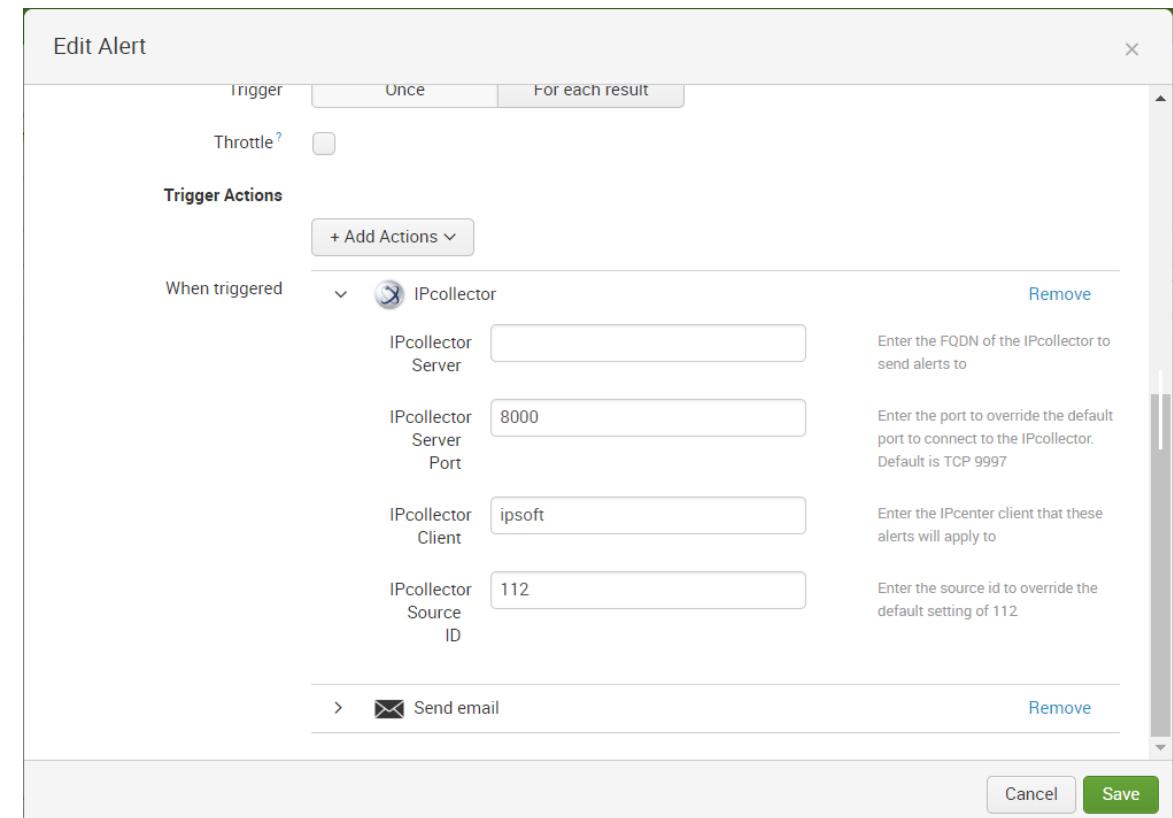
Orchestration Workflow



Splunk to Orchestration Architecture

Key components enabling orchestration

- ▶ Utilize each platform's strengths
- ▶ Tool agnostic
- ▶ Utilize standard Splunk alert feature
- ▶ Implement new Alert Action
- ▶ Deliver only actionable events
- ▶ Format data to meet orchestration needs



Orchestration Paths

Alerts generated through IPCollector integration

Notification

- ▶ Email
 - ▶ SMS
 - ▶ Key field values
 - To
 - From
 - Subject
 - Body
 - Issue Details
 - KB article

Service ticket creation

- ▶ ServiceNow API integration
 - ▶ Incident
 - ▶ Request
 - ▶ Key Field values
 - Requestor name
 - Hostname
 - IP address
 - Issue Details

Script execution

- ▶ Custom development
 - ▶ Value assessed
 - ▶ Script maintained and executed through orchestration platform
 - ▶ Key Field Values
 - Hostname
 - IP Address
 - OS

Automation Examples

"If nothing changes, nothing changes"

Courtney C. Stevens

Application Performance

Failed SQL Job Management

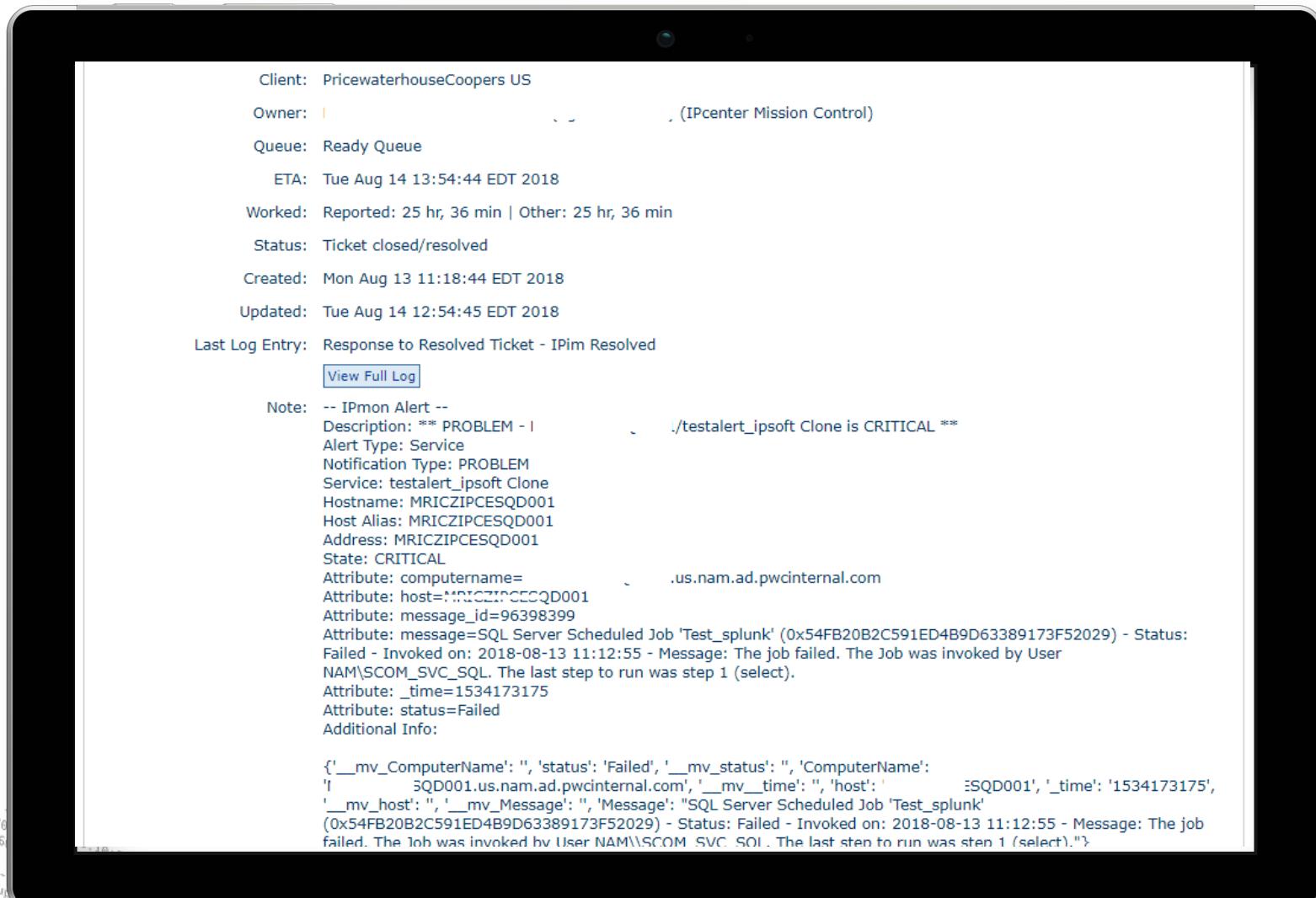
The screenshot shows the 'Alert' configuration page in Splunk. The alert is titled 'IPCenterSQLJobs_Failed'. The search query is set to 'index=wineventappsys_us host= SourceName=SQLSERVERAGENT EventCode=208 "Status: Failed" | eval status="Failed" | table _time host ComputerName status Message'. The alert type is set to 'Scheduled' and runs on a cron schedule of '*/2 * * * *'. The time range is set to 'Last 2 minutes'. The trigger condition is set to 'Number of Results is greater than 0' and triggers 'Once'. There is also a 'Throttle' checkbox.

Identify and Escalate

- ▶ Create standard alert
- ▶ Monitor for failed jobs
- ▶ Format results as table
- ▶ Utilize custom alert action

Application Performance

Failed SQL Job Management

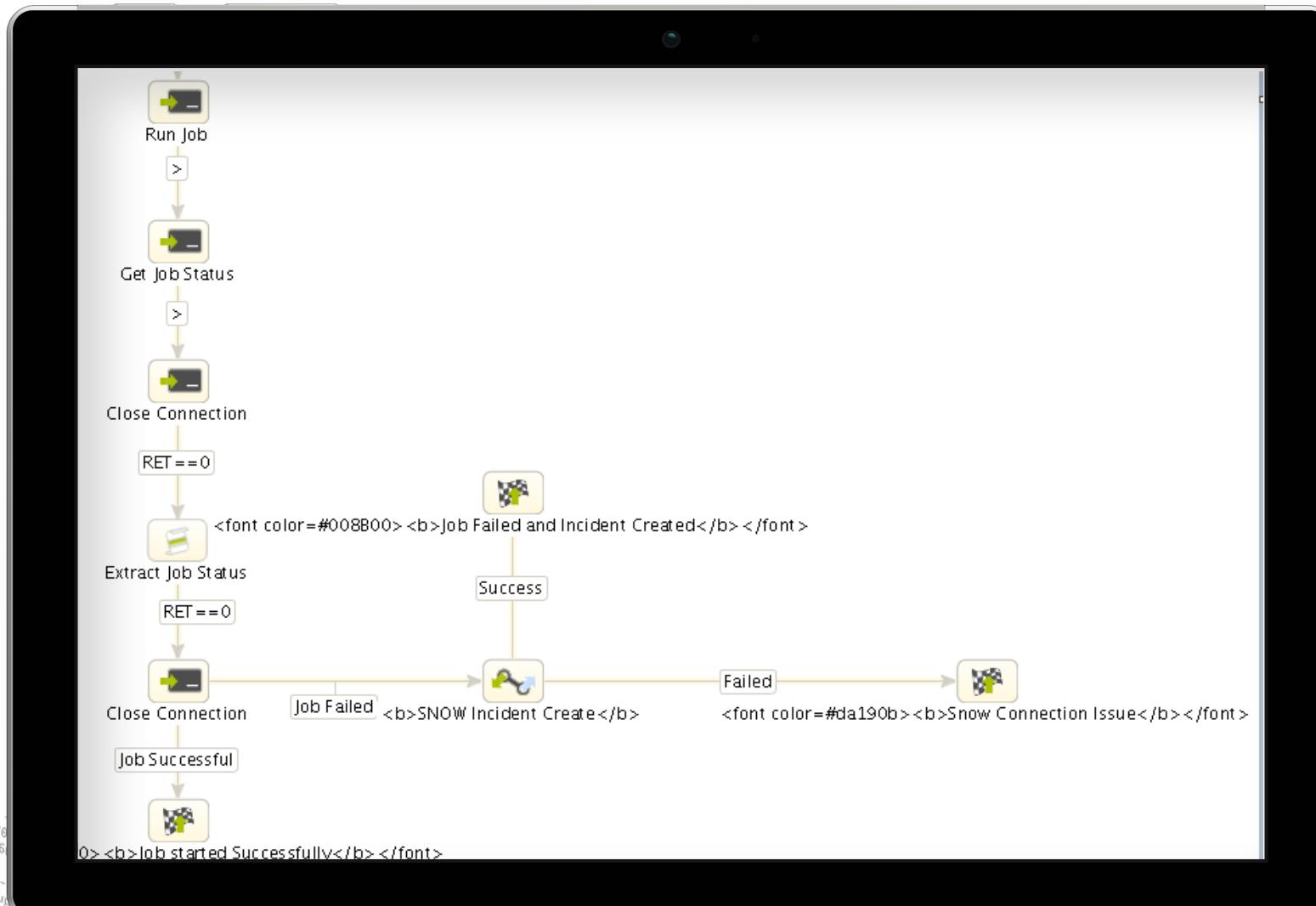


Deliver to Orchestration

- ▶ IPCollector receives alert
 - ▶ Forwards details to
IPCenter
 - ▶ Actionable Event is created
in IPCenter

Application Performance

Failed SQL Job Management



Orchestration Takes Action

- ▶ Regex matching identifies appropriate workflow
 - ▶ Branching script tasks initiate
 - ▶ Success or failure managed by workflow

Infrastructure - Platform

Virtual Machine Resource Allocation

The screenshot shows a Splunk-based dashboard titled "Underutilized Virtual Machines". The dashboard includes the following key elements:

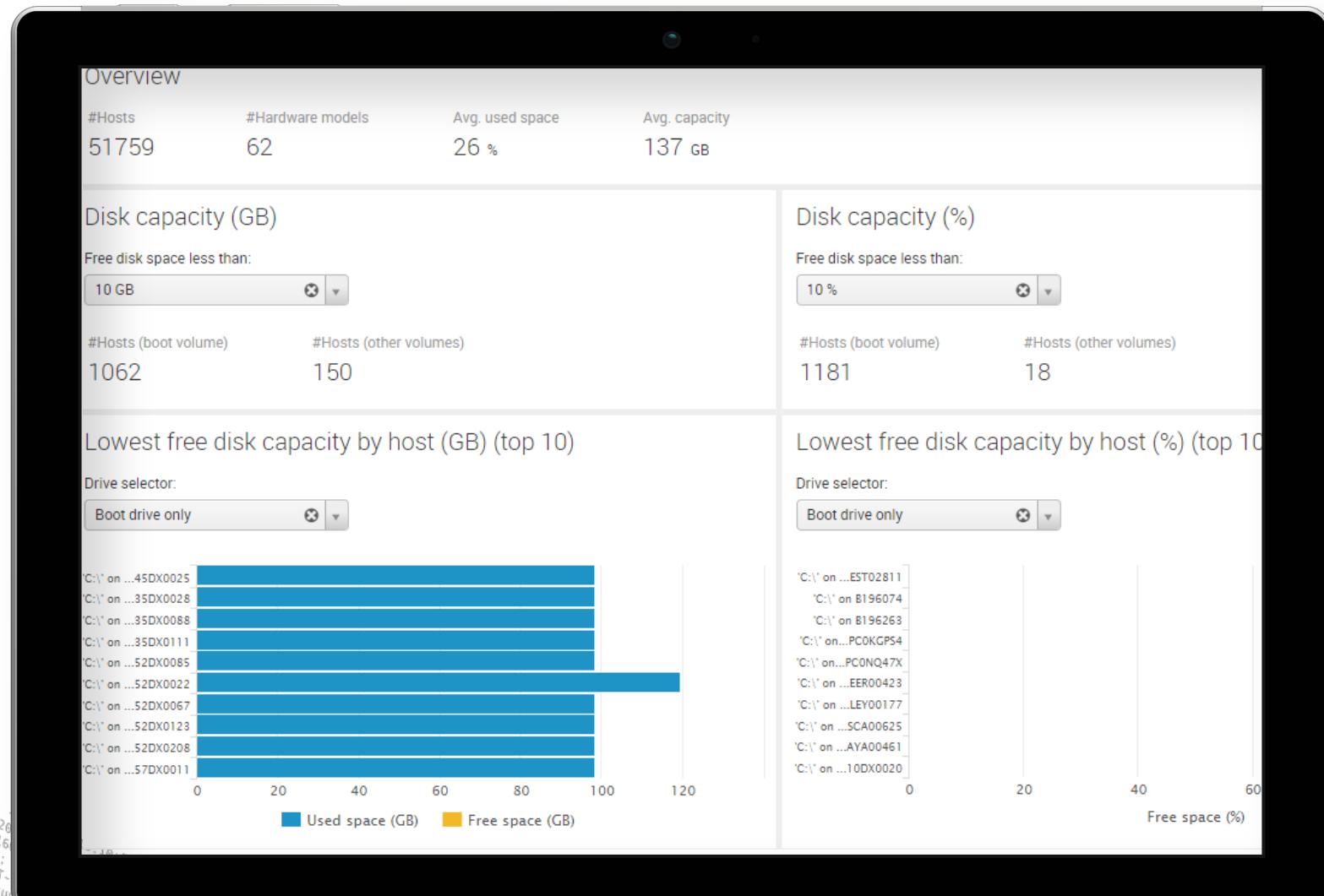
- Statistics:** Three large numbers at the top: "359 Total VMs", "3.6 % Combined CPU Usage", and "2.8 % Combined RAM Usage".
- Filters:** A section for filtering VMs by CPU and RAM usage percentages, with dropdowns for "Last day" and search fields for "VM" and "Service".
- Table:** A table listing 10 underutilized VMs with columns for Average CPU Usage %, Average RAM Usage %, CPU Cores, Total RAM (GB), Cluster, Owner, Service, and Status. The table shows data such as 3.51% CPU usage for GDC_NAM_INT_PRD11 and 2.63% RAM usage for GDC_NAM_INT_PRD05.
- Pagination:** A page navigation bar at the bottom of the table.

Identify Over-Allocated VMs

- ▶ Report utilization over time
- ▶ Identify VMs for resizing
- ▶ Trigger alert to IPCenter to subtract resources based on utilization

Endpoint Analytics

Low Disk Space



Disk Space Issues

- ▶ Identify low disk space on end-user laptops
- ▶ Deploy resolution proactively
- ▶ Continually monitor for reoccurrence

IT Service Management

Automate Report Generation and Distribution

Incident Update Analysis

Incidents that have not been updated in more than 3 days broken down by Assignment Group and last update time. Click on the Assignment name to see the list of the incident details.

Assignment Group Search Hide Filters

Incident Counts by Assignment Group

Assignment_Group	3-5	5-10	10-15	15-20	>20	Total
AMERICAS - IT APP SPT	0	3	10	0	1	14
AMERICAS - IT DCS - FACILITIES MGMT	0	2	4	0	0	6
AMERICAS - IT DCS - MESSAGING INFR SUPPORT	1	9	0	0	2	12
AMERICAS - IT DCS - NETWORK SERVICES	0	13	2	0	1	15
AMERICAS - IT DCS - PLATFORM	1	14	0	0	1	16
AMERICAS - IT DCS - STORAGE MGMT	1	4	1	0	0	6
AMERICAS - IT DCS - UNIX	0	3	0	0	0	3
PwC IT - APP SPT - L2 ASSURANCE	0	6	0	0	0	6
UK/US - IT DCS NETWORK - IPCC VOICE	0	1	0	0	0	1
UK/US - IT DESKTOP ENGINEERING - REQUESTS	1	18	4	0	0	23
US - ADV - APP DEV - AUDIT360	0	1	4	0	0	5
US - ADV - APP SPT - LMCC	0	0	1	0	0	1
US - ADV - CAAT TRACKER SUPPORT	0	1	6	0	0	7
US - ADV - HOSTING SERVICES OPERATIONS	0	1	0	0	0	1
US - ADV - IT DBA SUPPORT	0	0	2	0	0	2

Queue Management

- ▶ Repurposed dedicated reporting team
- ▶ Identify Aging Incidents
- ▶ Deliver Reports to large audience

Delivering Analytic Value



Measuring Results

How are we successful?

► Cost out (--\$\$\$)

- Hardware Capacity
- Resource Allocation
- Manual Administration
- Labor reduction
- Eliminate lost time

\$1.5M in cost
elimination

► Hours saved (++Time)

- Contact Reduction
- Report Automation
- Delivery Notification
- Incident Resolution Time

6,000
employee &
contractor hrs

► Quality (--Defects)

- Automated workflow
- Consistent Execution
- Immediate Response
- Simplification

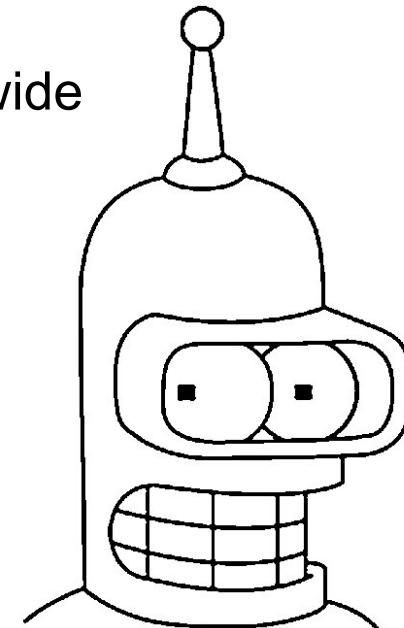
99% reduction
in downtime

Next Steps

Enabling & Measuring Superior Client Experience

Analytics Factory

- ▶ Expand ITSI Service Creation
 - ▶ Extend Actionable Analytics platform-wide
 - ▶ Build Analytic inventory
 - ▶ Integrate with Orchestration Platforms



Critical Success Factors

- ▶ Reduce customer support calls
 - ▶ Eliminate unplanned downtime
 - ▶ Reduce MTTR for Incidents
 - ▶ Reduce manual administration

“All hail our new robot-overlords!”

Key Takeaways

1. Building an analytics foundation
2. Foundation enabled actionable analytics
3. Factory approach drives value

Q&A

Thank You

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



A Little More About Us...

Patrick Combs

TCS, Data Analytics Leader

- ▶ 18+ yrs combined experience at PwC
 - Web Development
 - Database Reporting
 - Platform Services
 - Data Analytics

- ▶ Soccer coach and cyclist

Scott Hamrick

PwC, IT Director – Operations Analytics

- ▶ 20+ yrs combined experience with GE/PwC
 - Networking (CCNP)
 - InfoSec (CISSP)
 - Data Analytics

- ▶ Softball professional, RiffTrax backer