

splunk> .conf2017

# Splunk ITSI as a Foundation for ITOA

Measuring End-to-End User Experience

Patrick Combs | Data Center Services & Analytics

Scott Hamrick | IT Director – Operations Analytics

Date | Washington, DC

© 2017 SPLUNK INC.



# Biography

Patrick Combs

TCS, Data Center Service & Analytics  
Leader

► 16 yrs combined experience at PwC

- Web Development
- Database Reporting
- Platform Services
- Data Analytics
- Soccer coach and avid cyclist

Scott Hamrick

PwC, IT Director – Operations

Analytics

► 20 yrs combined experience with  
GE/PwC

- Networking (CCNP)
- InfoSec (CISSP)
- Data Analytics
- Softball professional, MST3K backer

- ▶ 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 





## My Top 5 Least Favorite...

## My least favorite comments to hear on a troubleshooting call are...

1. Can we get the Vendor on the call??
2. I am not familiar with this technology but...
3. My application is working but it is slow...
4. Can someone “check” the Network??
5. Has anyone made any changes??



# IT Operations Analytics Mission

---

“Sunlight is said to be the best of disinfectants”

Justice Louis D. Brandeis

## Enabling & Measuring Superior Client Experience

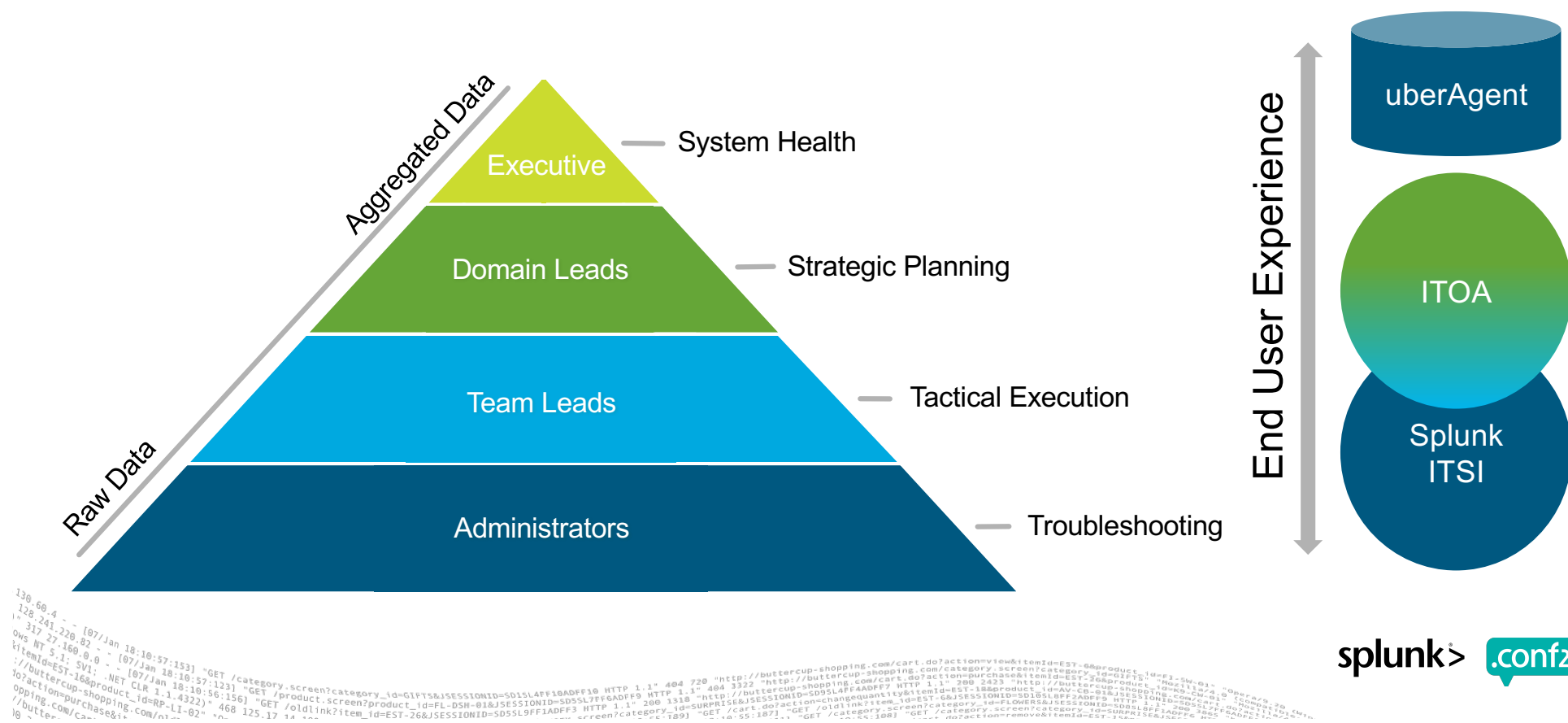
## ► Critical Success Factors

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

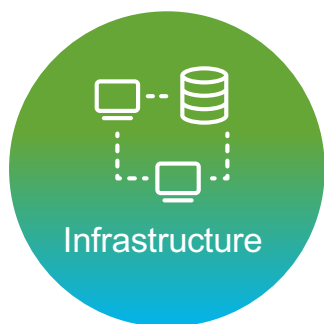
# IT Operation Analytics

Variable levels of specificity based on organizational role



# IT Operation Analytics

## End-to-End visibility for user experience



## Infrastructure

Platform  
Network  
Storage



## Applications

# Custom Business Applications



## Core Services

AD/DNS  
ED  
IdAM  
Siteminder



## Incident Mgmt

# Major/Minor Incidents Interactions

Service  
Mgmt

Change  
Problem  
Release  
Knowledge

# IT Operations Analytics

Leveraging Splunk ITSI backbone to organize info in custom application

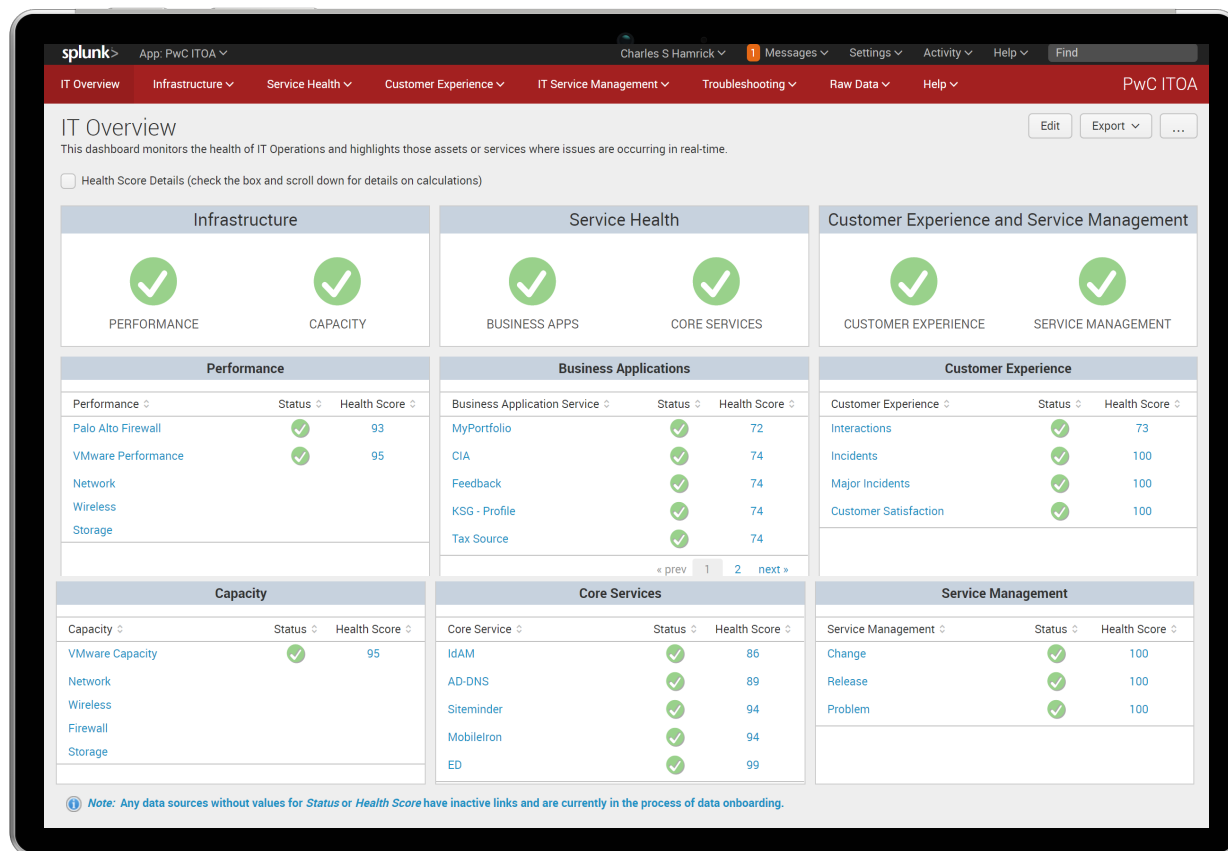


ITOA App

splunk> .conf2017

# ITOA Application

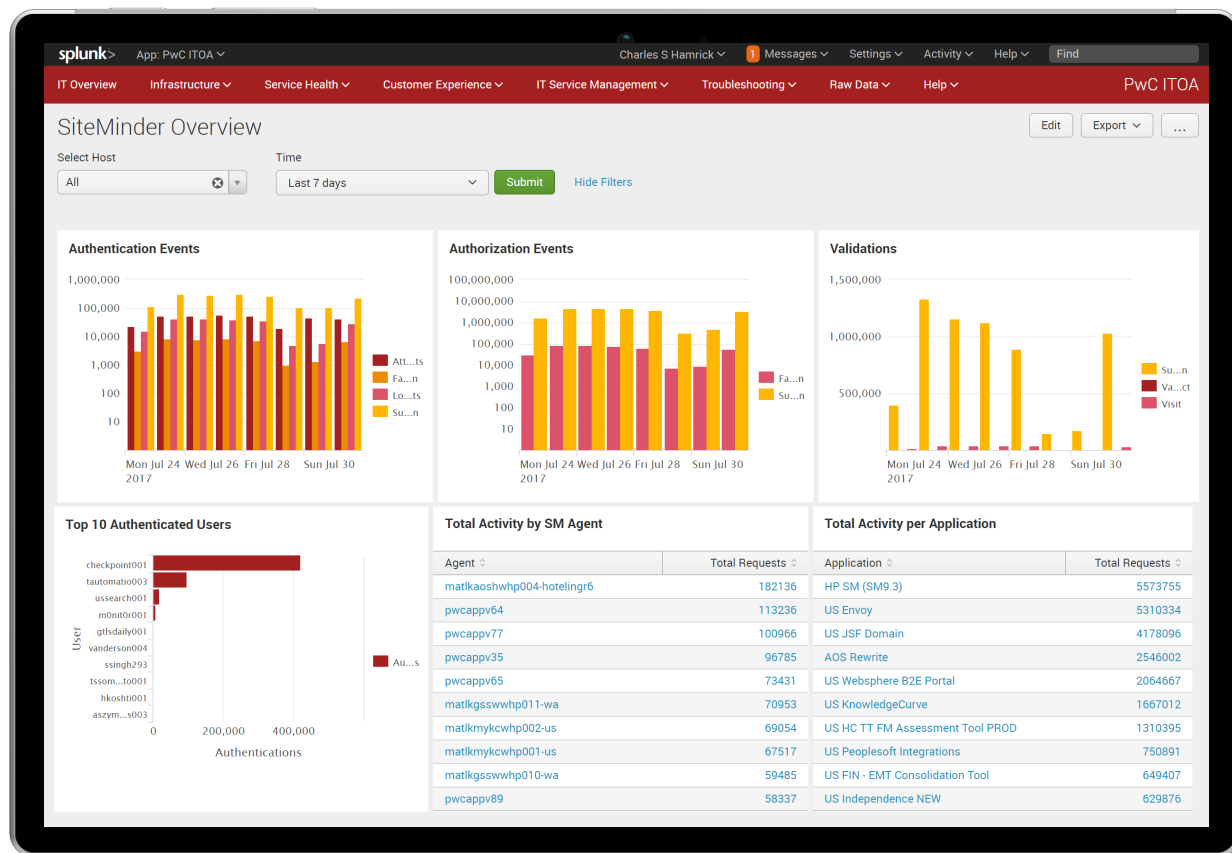
## Executive-level health score overview



- Overview of IT Health based on real-time status
- Aggregates KPIs across dimensions
- Allows custom navigation
  - Drop-down menus
  - Drill-down links

# ITOA Application

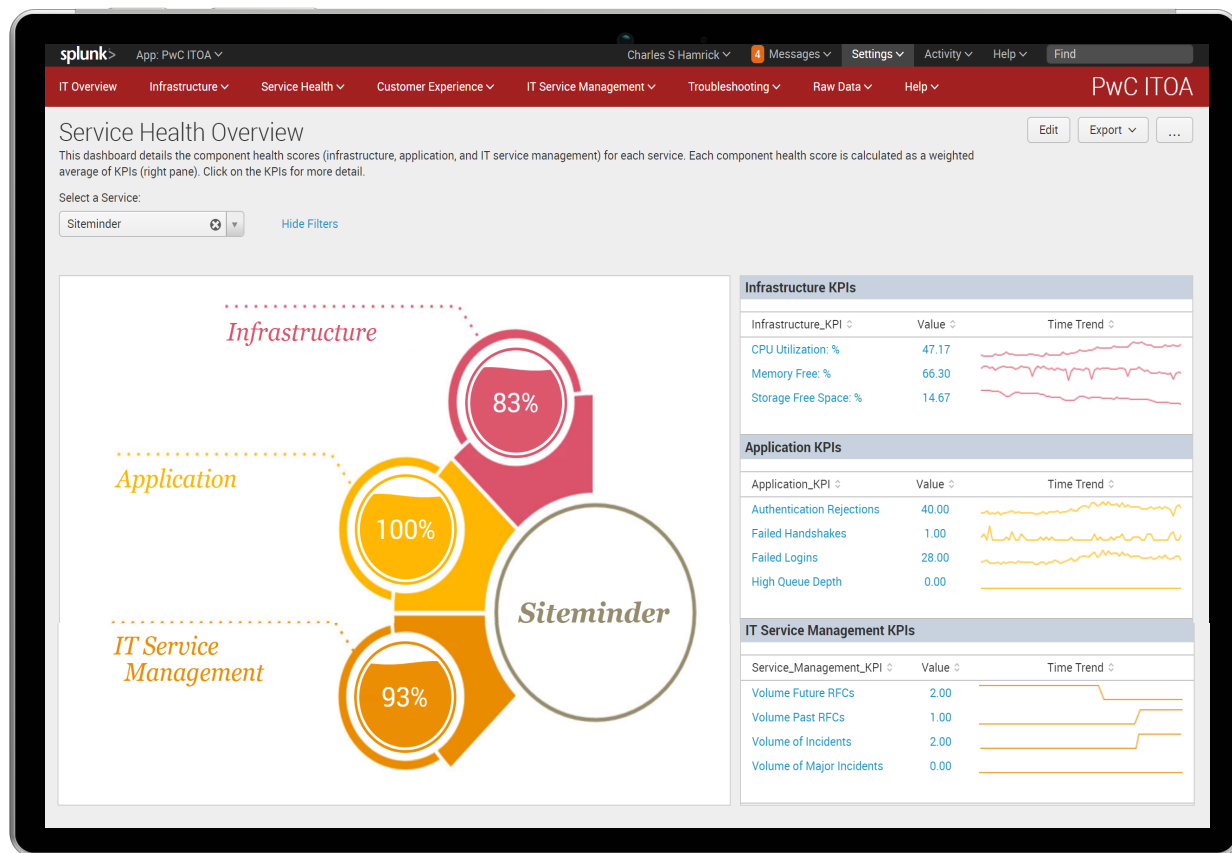
## Custom service health dashboard of critical KPIs



- Metrics determined by service SMEs
- Dashboard nested in dropdown menu
- Consistent look and feel based on branding standards
- Filtered by host
- Minimalized time picker

# ITOA Application – Health Score

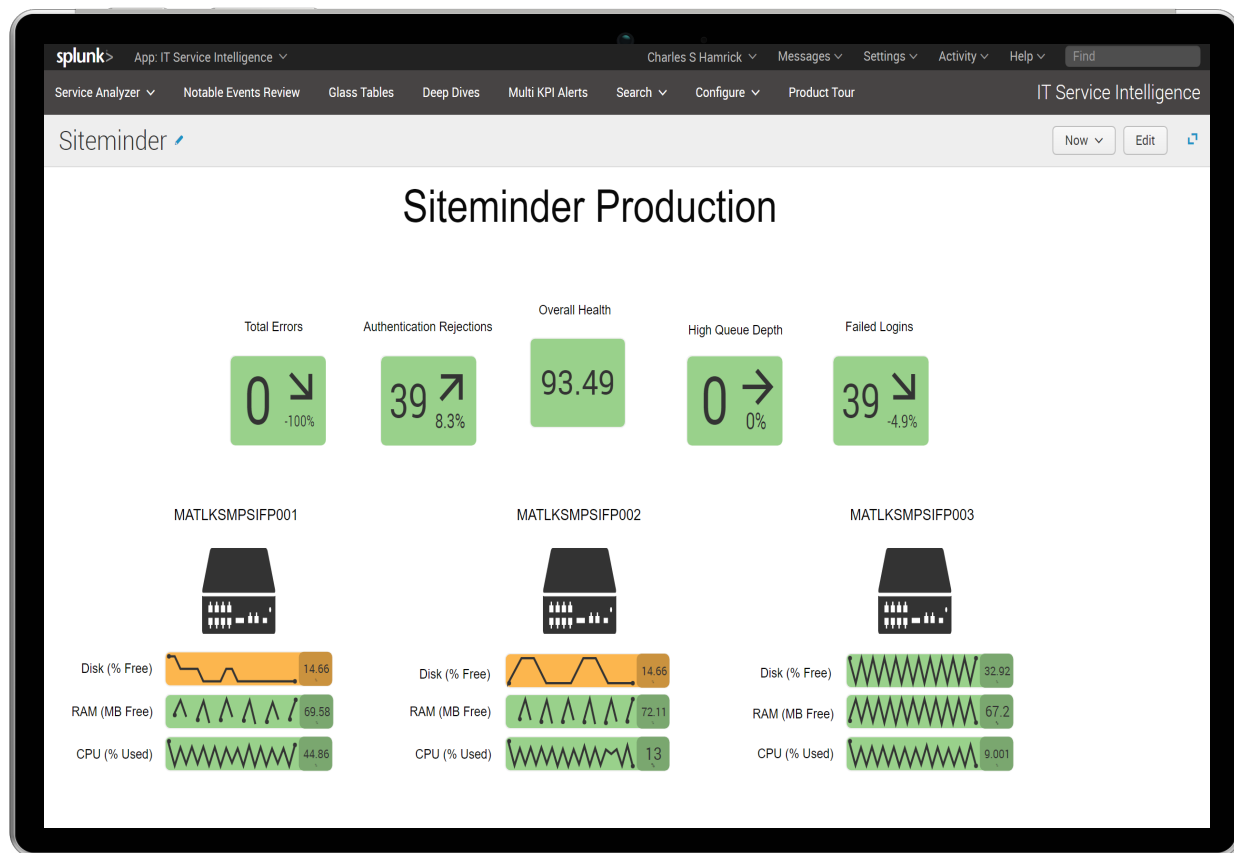
Service health overview for Domain Leaders



- ▶ KPIs listed by segment
  - Infrastructure
  - Application
  - Service Management
- ▶ Trendline metrics included for context
- ▶ Asset/Service navigation
- ▶ Punchout links to native ITSI functionality

# ITOA Application – Splunk ITSI

## Splunk ITSI Glass Table view for Team Leaders

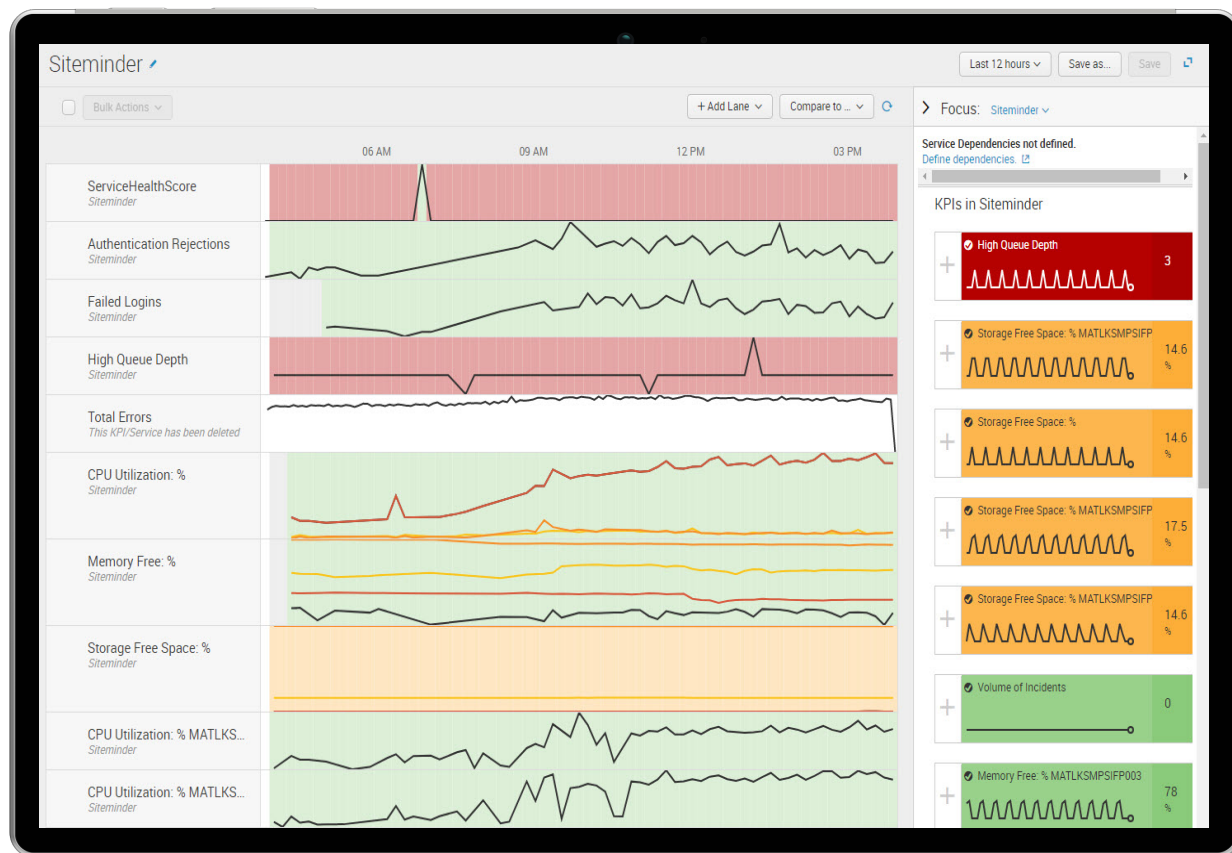


### ► Launch Splunk ITSI in new tab

- KPIs listed by service
  - Real-time value
  - Trend metrics included
- Infrastructure KPIs listed per server
- Drilldown links to deep dive
- ITOA application active in previous tab

# ITOA Application – Splunk ITSI

Deep-dive troubleshooting view for Administrators



- ▶ Native Splunk ITSI functionality
- ▶ Correlate KPIs in context with each other
- ▶ Viewable by entity
- ▶ Service dependencies available as defined
  - Authentication tier
  - Web/Database tier

# Integrating Splunk ITSI with ITOA app

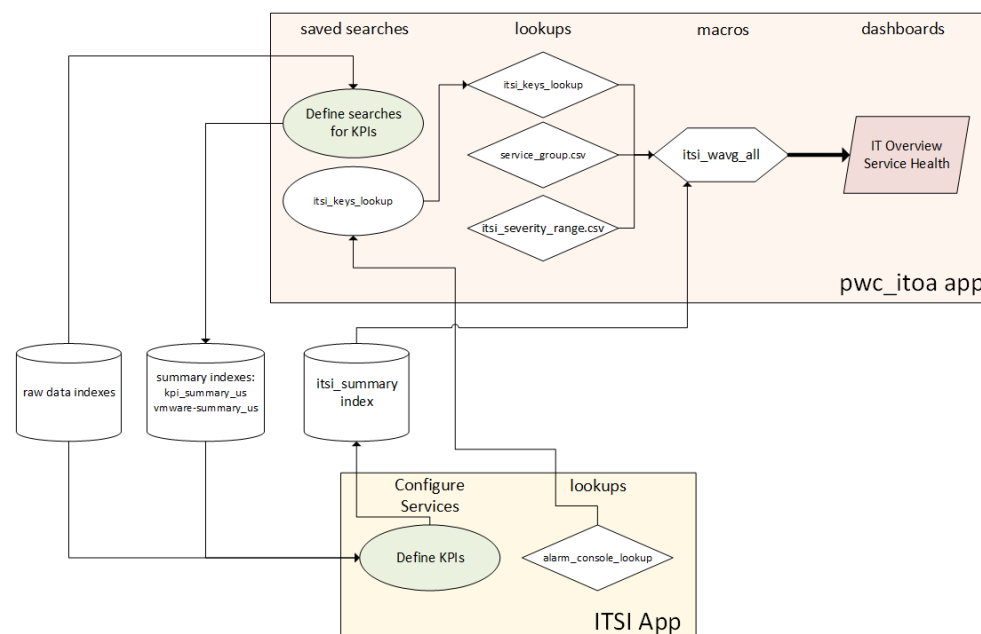
---

Technical walkthrough

# Splunk ITSI and ITOA Overview

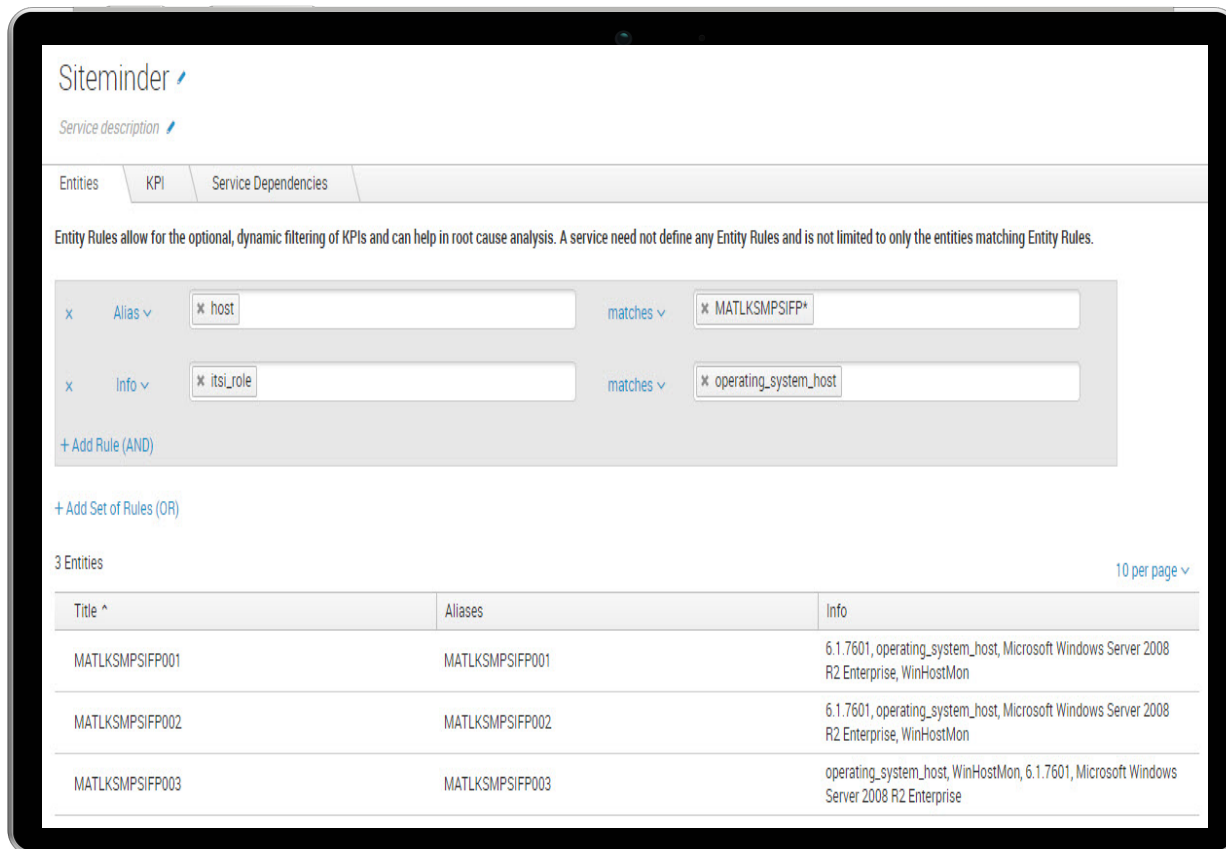
## ► Key components required by ITOA app

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



# ITOA Application – Splunk ITSI

## Entity Definitions



The screenshot displays the 'Siteminder' interface in Splunk ITSI. It features tabs for 'Entities', 'KPI', and 'Service Dependencies'. A descriptive text states: 'Entity Rules allow for the optional, dynamic filtering of KPIs and can help in root cause analysis. A service need not define any Entity Rules and is not limited to only the entities matching Entity Rules.'

Below this, there are two rule definitions:

- Rule 1: Alias (x) matches MATLKSMPISFP\* (x)
- Rule 2: Info (x) matches operating\_system\_host (x)

Buttons for '+ Add Rule (AND)' and '+ Add Set of Rules (OR)' are visible.

A table titled '3 Entities' (with a '10 per page' dropdown) lists the following data:

Title ^	Aliases	Info
MATLKSMPISFP001	MATLKSMPISFP001	6.1.7601, operating_system_host, Microsoft Windows Server 2008 R2 Enterprise, WinHostMon
MATLKSMPISFP002	MATLKSMPISFP002	6.1.7601, operating_system_host, Microsoft Windows Server 2008 R2 Enterprise, WinHostMon
MATLKSMPISFP003	MATLKSMPISFP003	operating_system_host, WinHostMon, 6.1.7601, Microsoft Windows Server 2008 R2 Enterprise

- ▶ Assign entities to the service
  - Either literally list the entities or define rules
  - Confirm all entities present
  - Plan for future changes

# ITOA Application – Splunk ITSI

## KPI Base searches

PWC-DA-ITSI-OS:Performance.CPU

KPI base search used by KPIs that track CPU perform...

Search ?

[Run Search](#)

KPI Search Schedule ?

Calculation Window ?

Monitoring Lag (seconds) ?

[Determine Recommended Lag](#)

Split by Entity ?

Filter to Entities in Service ?

Service must have entities to filter by entities

Entity Lookup Field ?

Entity Alias Filtering

Enter the specific aliases (associated with the entity value) that you want to use in the generated KPI search. (For example, "host", "ip\_address", etc.). This filters out all other entities associated with the service.

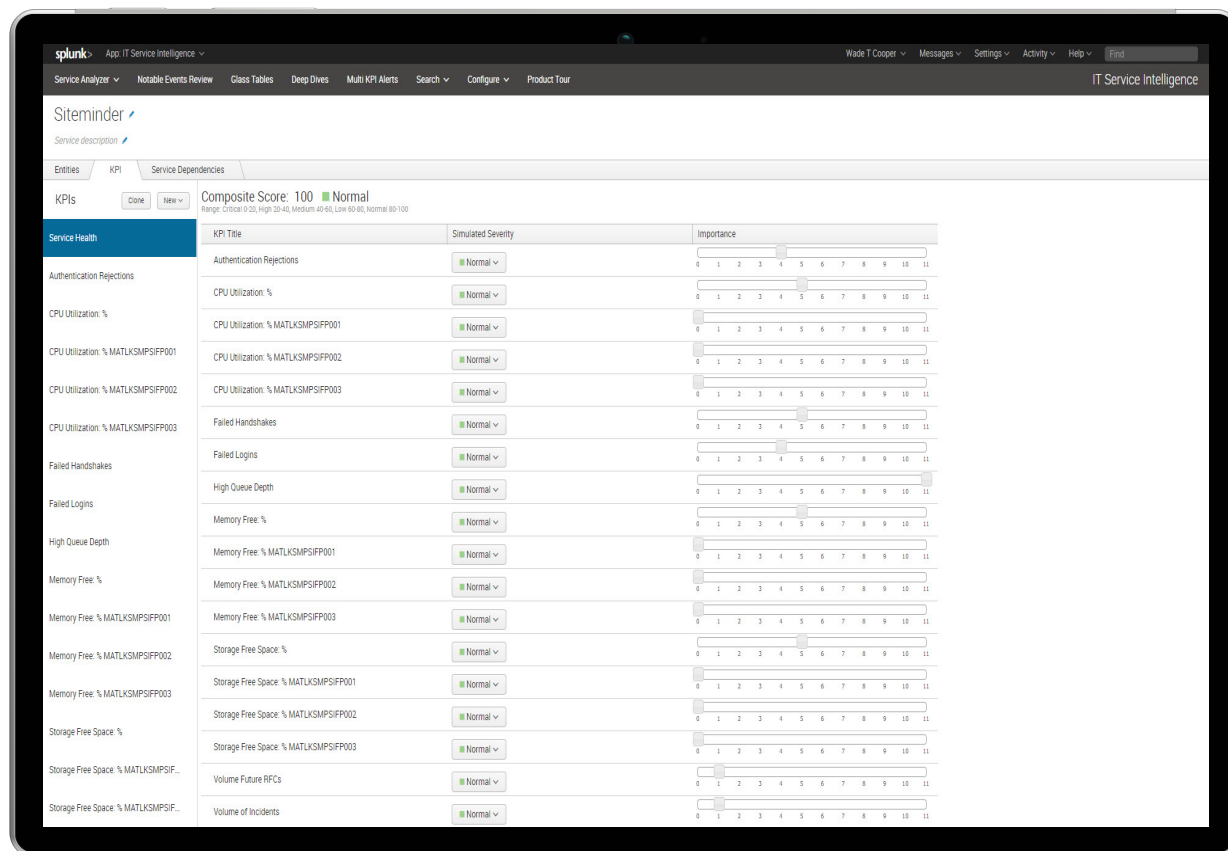
4 Metrics

Title ^	Threshold Field	Entity Calculation	Service Calculation	Unit	Actions
cpu_interrupts	cpu_interrupts	avg	avg	ct/s	<a href="#">Edit</a> ▾
cpu_load_perce...	cpu_load_percent	avg	max	%	<a href="#">Edit</a> ▾
system_thread...	system_threads_c...	avg	avg	count	<a href="#">Edit</a> ▾
wait_threads_c...	wait_threads_count	avg	avg	thds	<a href="#">Edit</a> ▾

- ▶ Utilize KPI base search for standard OS metrics
- ▶ Custom KPIs generate app specific health scores.
- ▶ Both combine for overall health
- ▶ Results written to the summary index

# ITOA Application – Splunk ITSI

## Service Health weighting



- ▶ Utilize Splunk ITSI Service Health to assign weights
- ▶ Overall Service Health based on KPI and assigned weighting
- ▶ Weighting process is iterative

# ITOA Application – Splunk ITSI

## Lookups

Lookups   New Lookup   Lookup Editor

Lookup Edit

[Back to Lookups List](#)

service\_group.csv   Import   Export   Revert to previous version ▾

Right-click the table for editing options

1	Service	KPI	service_kpi	ServiceHealthName	ServiceGroup	GroupType	SubGroup	ITOverviewGroup	Description	link
2	AD-DNS	Storage Free Space: %	AD-DNS - Storage Free Space: %	AD/DNS	AD-DNS	Infrastructure	Disk	AD-DNS	Minimum % of free disk space from all AD-DNS servers during the last 5 minutes	/app/pwc_itoa/serviceform.service=AD%2FD
3	AD-DNS	Memory Free: %	AD-DNS - Memory Free: %	AD/DNS	AD-DNS	Infrastructure	Memory	AD-DNS	Minimum % of memory available from all AD-DNS servers during the last 15 minutes	/app/pwc_itoa/serviceform.service=AD%2FD
4	AD-DNS	CPU Utilization: %	AD-DNS - CPU Utilization: %	AD/DNS	AD-DNS	Infrastructure	CPU	AD-DNS	Maximum % of CPU utilization from all AD-DNS servers during the last 5 minutes	/app/pwc_itoa/serviceform.service=AD%2FD
5	AD-DNS	Volume of Incidents	AD-DNS - Volume of Incidents	AD/DNS	AD-DNS	Process	Incidents	AD-DNS	Volume of incidents opened the previous day with AFFECTED_ITEM="*dns"	/app/pwc_itoa/serviceform.service=AD%2FD
6	AD-DNS	Volume of Major Incidents	AD-DNS - Volume of Major Incidents	AD/DNS	AD-DNS	Process	Major Incidents	AD-DNS	Volume of major incidents opened the previous day with	/app/pwc_itoa/serviceform.service=AD%2FD

Save Lookup

- ▶ Applies the ITOA app framework around Splunk ITSI Data
- ▶ Provides the glue between Splunk ITSI and ITOA App
- ▶ Group KPIs into different levels
- ▶ Detailed descriptions providers for users

# ITOA Application – Splunk ITSI

Transforming Splunk ITSI into ITOA with macro

itsi\_wavg\_all(3)

[Advanced search](#) » [Search macros](#) » itsi\_wavg\_all(3)

## Definition \*

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: Sarg1\$

```
search `get_itsi_summary_index` $time_filter$ entity_title="service_aggregate"
  [| inputlookup itsi_keys_lookup
   | rename key as itsi_kpi_id
   | lookup service_group.csv service_kpi
   | search $search_term$
   | table itsi_kpi_id]
| fields alert_severity alert_value itsi_kpi_id
| lookup itsi_keys_lookup key as itsi_kpi_id
| lookup service_group.csv service_kpi
| dedup service_kpi
| lookup itsi_severity_range.csv alert_severity
| eval weight=if(isnull(range_val), "", weight)
| eval weight_low_val = if(weight=11, range_val, 100)
| eval weight_new = weight
| eventstats sum(weight_new) as weight_sum
| eval wavg = (range_val*weight_new)/weight_sum
| eventstats sum(wavg) as wavg_sum
| eval wavg_min_val = if(weight_low_val<wavg_sum, weight_low_val, wavg_sum)
| stats min(wavg_min_val) as health_score $by_clause$
| appendpipe
  [| stats count AS totNum
   | eval health_score=if(totNum==0, "", health_score)
   | fields - totNum]
```

☐ Use eval-based definition?

- ▶ Utilize Splunk ITSI weighted average calculation to produce health scores
- ▶ Pass time, search term, and service grouping details to calculate health at any level
- ▶ Maintain separation from development environment

splunk> .conf2017

# ITOA Application – Splunk ITSI

## Calling the Weighted Average

New Search

Save As ▾

```
`itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=Siteminder", by_clause="by ServiceGroup, link,
active_link")`
| append ['itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=AD-DNS", by_clause="by
ServiceGroup, link, active_link")`]
| append ['itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=IdAM", by_clause="by
ServiceGroup, link, active_link")`]
| append ['itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=MobileIron", by_clause="by
ServiceGroup, link, active_link")`]
| append ['itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=ED", by_clause="by ServiceGroup,
link, active_link")`]
| sort health_score
| eval Metric=ServiceGroup, Status = case(health_score<30, "severe", health_score<70,"elevated", health_score
<101, "low")
| table Metric Status health_score link active_link
| rename Metric as "Core Service", health_score as "Health Score"
| eval "Health Score" = round('Health Score', 0)
| append [
| inputlookup temp_data.csv
| search ServiceCategory=CoreService
| rename Service AS "Core Service", Health AS "Health Score"
| table "Core Service" Status "Health Score" link active_link
]
```

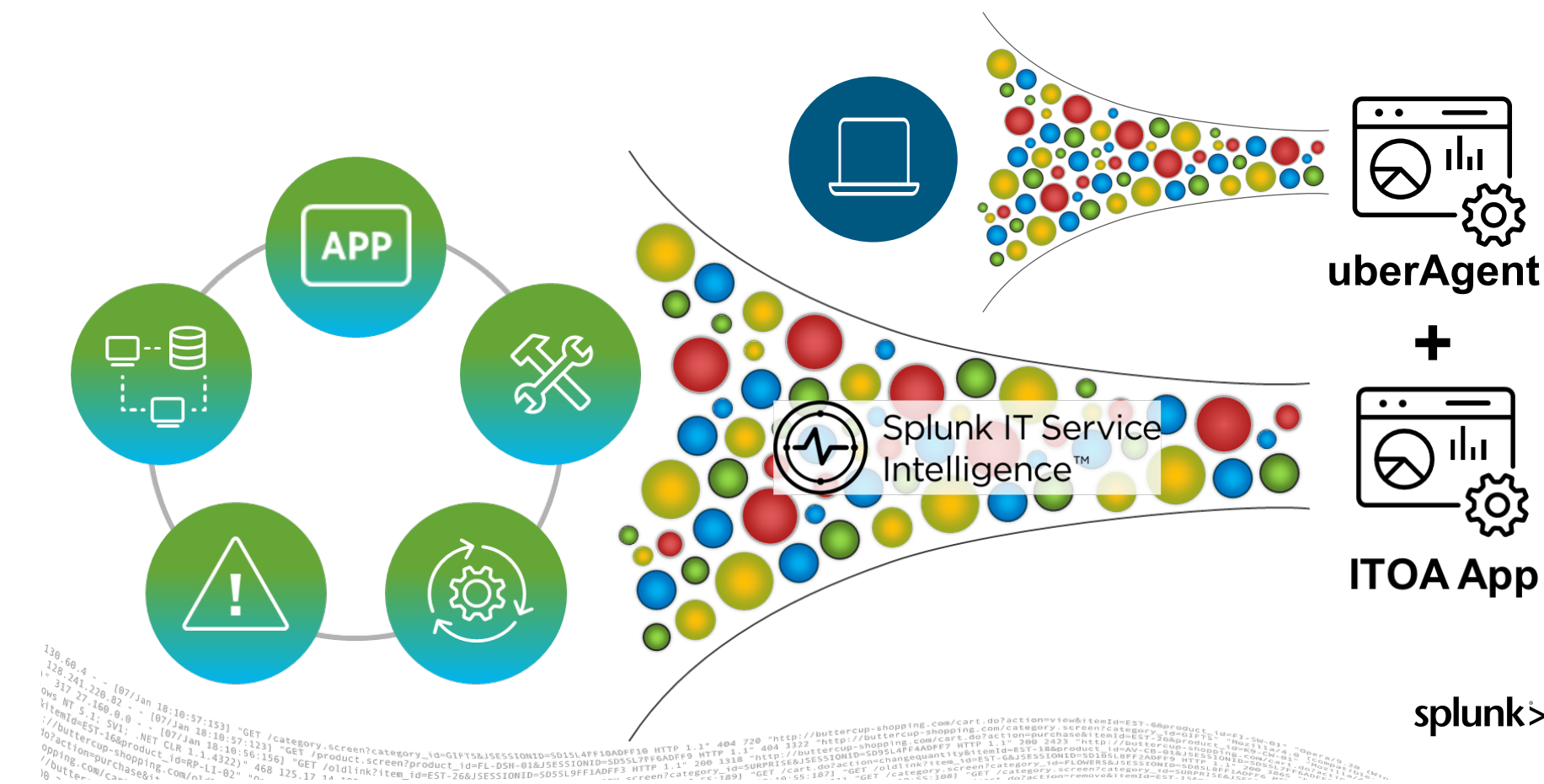
### ► Call the wavg\_all macro

- Pass necessary variables
  - Time
  - Service Group
  - By clause

# Closing The User Experience Gap

---

## Desktop monitoring



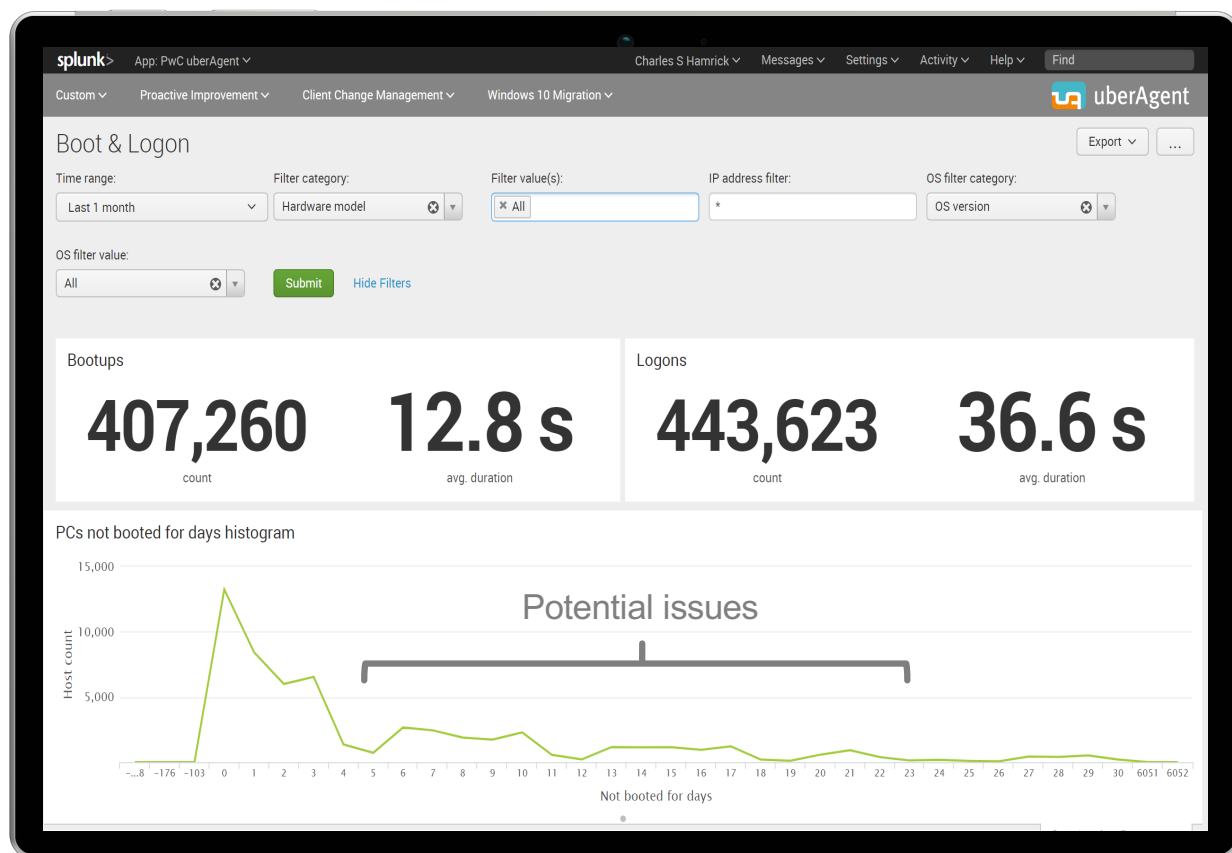


- ▶ Utilizes Splunk Index/SH servers
- ▶ Integrated with Universal Forwarder
- ▶ Deployed to 68k+ laptops in multiple countries
- ▶ Established real-time monitoring and analysis of PC health
- ▶ Data correlated with Splunk ITSI to close the end user experience gap

[illegible]

# Desktop User Experience

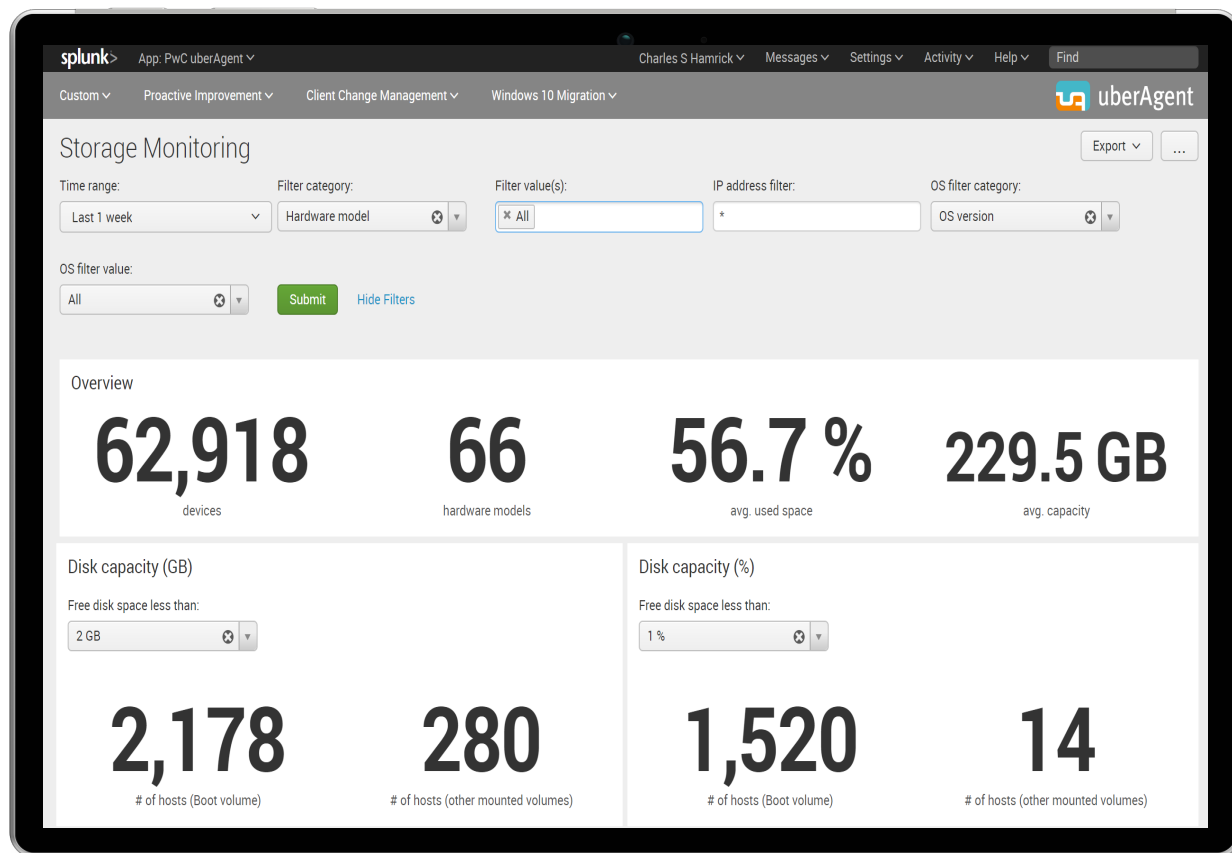
## Boot & logon dashboard – uberAgent (custom)



- ▶ Tracking boot metrics
  - Startup/Shutdown
  - Standby/Resume
- ▶ Filter by
  - Host
  - IP address
  - Hardware model
- ▶ Histogram of days since last boot for troubleshooting

# Desktop User Experience

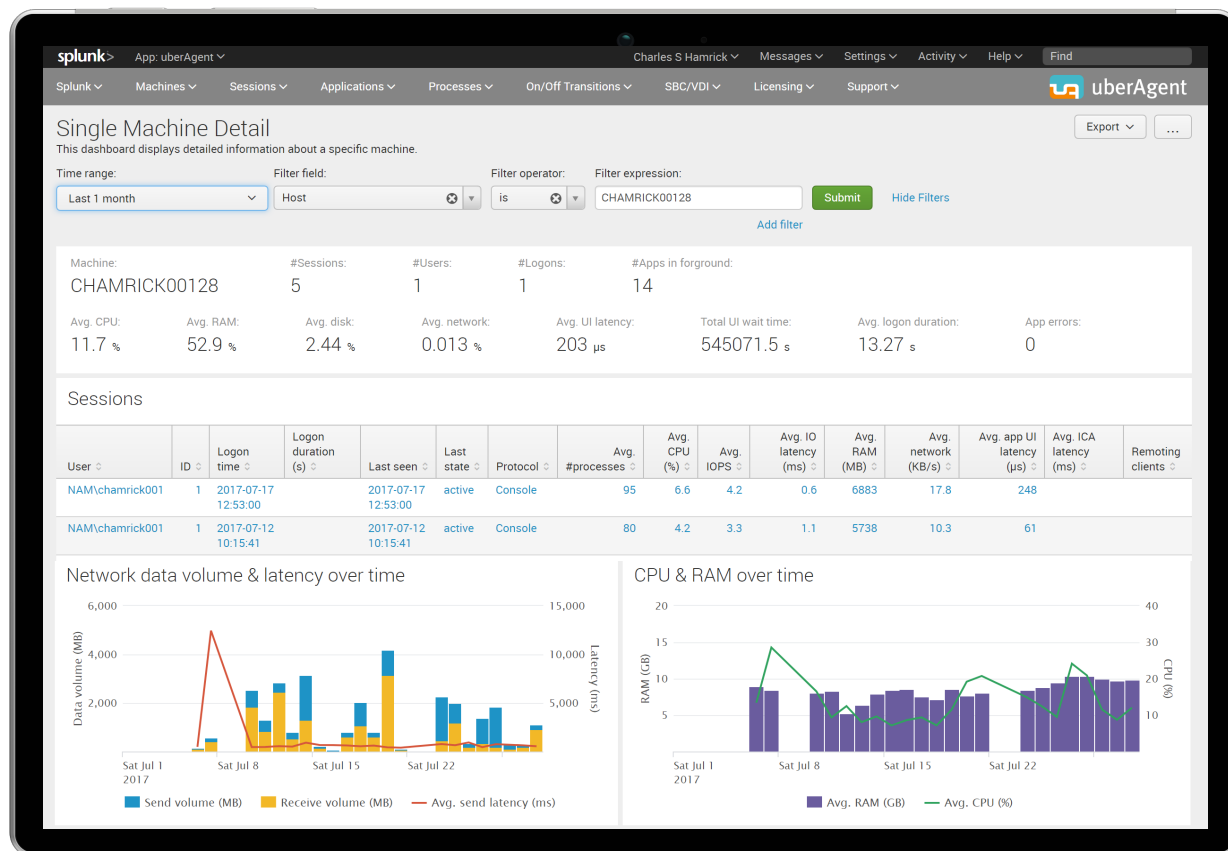
## Storage Monitoring – uberAgent (custom)



- ▶ Tracking disk capacity
  - Total GB remaining
  - % of capacity
- ▶ Disk usage grouped by
  - Hardware Model
  - Host
- ▶ Mounted volumes sorted per user by Free Space (% or GB)

# Desktop User Experience

## Single Machine Detail – uberAgent (default)



- ▶ Drill down to single machine detail
  - Avg CPU/RAM
  - Avg disk available
  - Network volume and latency
  - Session detail
  - Startup/shutdown duration
  - Application & process detail

# Key Takeaways

---

## Summary

# Key Learnings

If we had it to do all over...

## ► Establishing analytics as a service

- Commitment from leadership
- Addressing technical concerns
  - CPU utilization
  - Network firewall access
  - Network bandwidth

- Building analytic ambassadors

## ► Defining innovation opportunities

- Multiple demos required per team
- 10-50-80% method

## ► Managing environment complexity

- Cloud-based vs on-prem
- Heavy Forwarders & syslog
- Managing Universal Forwarders
- Developing add-ons

## ► Overcoming data onboarding issues

- VMWare
- Cisco Wireless (SNMP vs Syslog)
- Storage
- Websphere

```
130.60.4 - - [07/Jun 10:10:57:153] "GET /category.screen?category_id=61f5&SESSIONID=5015L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=EST-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.1) Gecko/20090720 Firefox/3.5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 --
128.241.220.82 - - [07/Jun 10:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5055L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=EST-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.1) Gecko/20090720 Firefox/3.5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 --
128.241.220.82 - - [07/Jun 10:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-13&product_id=AV-CB-01&SESSIONID=5015L4FF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=EST-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.1) Gecko/20090720 Firefox/3.5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 --
128.241.220.82 - - [07/Jun 10:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-13&product_id=AV-CB-01&SESSIONID=5015L4FF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=EST-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.1) Gecko/20090720 Firefox/3.5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 --
128.241.220.82 - - [07/Jun 10:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-13&product_id=AV-CB-01&SESSIONID=5015L4FF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=EST-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.1) Gecko/20090720 Firefox/3.5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 --
```

# Q&A

---



© 2017 SPLUNK INC.

# Thank You

Don't forget to **rate this session** in the  
.conf2017 mobile app

splunk> .conf2017

**Tuesday  
September  
26<sup>th</sup>, 2017**

- ▶ **Ready, Set, Go! Learn From Others - The First 30 Day Experiences of ITSI Customers:** Tuesday, September 26th, 2017 12:05 PM- 12:50 PM Room Salon C
- ▶ **Splunk ITSI Overview:** Tuesday, September 26th, 2017 1:10 PM-1:55 PM Room 147 AB
- ▶ **PWC: End-to-End Customer Experience:** Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room 143ABC
- ▶ **RSI: Operational Intelligence: How to go From Engineering to Operationalizing IT Service Intelligence Where the Rubber Meets the Road:**  
Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room147AB
- ▶ **Cardinal Health: Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring Using Splunk ITSI:**  
Tuesday, September 26th, 2017 3:30 PM-4:15 PM Room143ABC
- ▶ **ITSI in the Wild - Why Micron Chose ITSI and Lessons Learned From Real World Experiences:** Tuesday, September 26th, 2017 4:35 PM- 5:20 PM Room Salon C

**Wednesday  
September  
27<sup>th</sup>, 2017**

- ▶ **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:**  
Wednesday, September 27th, 2017 11:00 AM-11:45 AM Ballroom C
- ▶ **Triggering Alerting (xMatters) and Automated Recovery Actions from ITSI:** Wednesday, September 27th, 2017 1:10 PM- 1:55 PM Room Salon C
- ▶ **Leidos - Our Journey to ITSI:** Wednesday, September 27th, 2017 2:15 PM-3:00 PM Room 147AB
- ▶ **How Rabobank's Monitoring Team Got a Seat at the Business Table by Securing Sustainability on Competitive Business Services Built on Splunk's ITSI:**  
Wednesday, September 27th, 2:15-3:00pm Room 147AB
- ▶ **Here Comes the Renaissance: Digital Transformation of the IT Management Approach:** Wednesday, September 27th, 2017 3:30 PM-4:15 PM Room Salon C

**Thursday  
September  
28<sup>th</sup>, 2017**

- ▶ **The ITSI 'Top 20' KPI's:** Thursday, September 28th, 2017 10:30 AM-11:15 AM Room Salon C
- ▶ **Automation of Event Correlation and Clustering with Machine Learning Algorithms – An ITSI Tool:**  
Thursday, September 28th, 2017 11:35 AM- 12:20 PM Room Salon C
- ▶ **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:**  
Thursday, September 28th 11:35 AM - 12:20 PM in Ballroom B
- ▶ **IT Service Intelligence for When Your Service Spans Your Mainframe and Distributed ITSI:**  
Thursday, September 28th, 2017 1:20 PM-2:05 PM Room Salon C