

# Splunk ITSI as a Foundation for.

#### Measuring End-to-End User Experience

Patrick Combs | Data Center Services & Analytics Scott Hamrick | IT Director – Operations Analytics

Date | Washington, DC



splunk> .conf201

#### **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. © 2017 Splunk Inc. All rights reserved.

## **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



© 2017 SPLUNK INC.

#### **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 🛛



© 2017 SPLUNK INC.

## **PwC IT Environment**

**Diverse IT Infrastructure** 

- Data Center Services Responsibilities
  - Support Multiple Lines of Service
  - 100s of applications
  - 24x7 support for production applications
  - Distributed workforce
  - Dedicated support teams by technology
  - Numerous "Mission Critical" application environments





## **Legacy Challenges**

#### Troubleshooting Outages

- Issues reported by users or by Up/Down device monitoring
- Large audience Conference calls
- Siloed investigation of possible cause
- Lack of data availability lead to slow progress.
- Problem Management
  - Lengthy investigations relying on Vendors or manual analysis
  - Root Cause frequently incomplete
  - Repetitive outages from similar causes





## 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??



splunk'> .conf2017

© 2017 SPLUNK INC

# **IT Operations Analytics Mission**

"Sunlight is said to be the best of disinfectants"

Justice Louis D. Brandeis

splunk> .conf2017

splunk> .conf2017

## **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

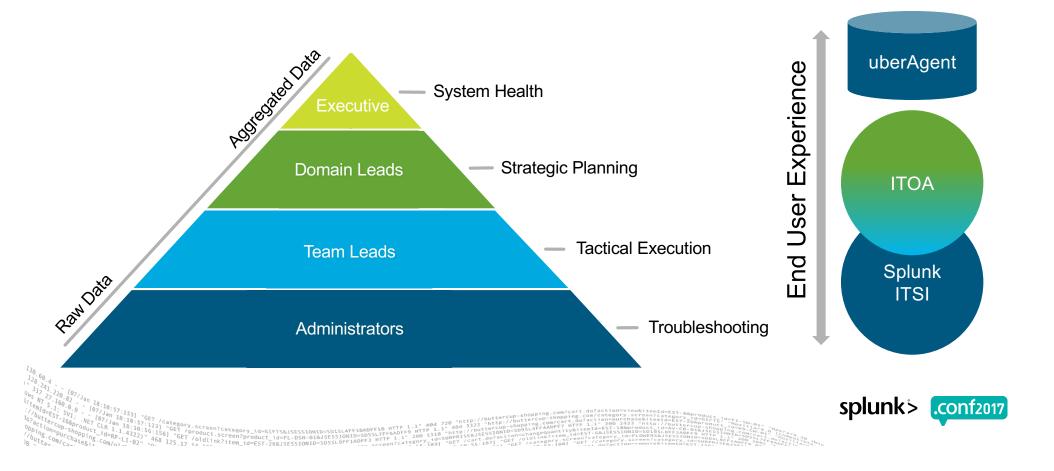
- Critical Success Factors
  - Quantify / Track User Experience
  - Eliminate unplanned downtime
  - Reduce MTTR for Incidents
  - Improve IT capacity management
  - Remove Manual Reporting

#### Measure and improve end-to-end user experience

© 2017 SPLUNK INC

## **IT Operation Analytics**

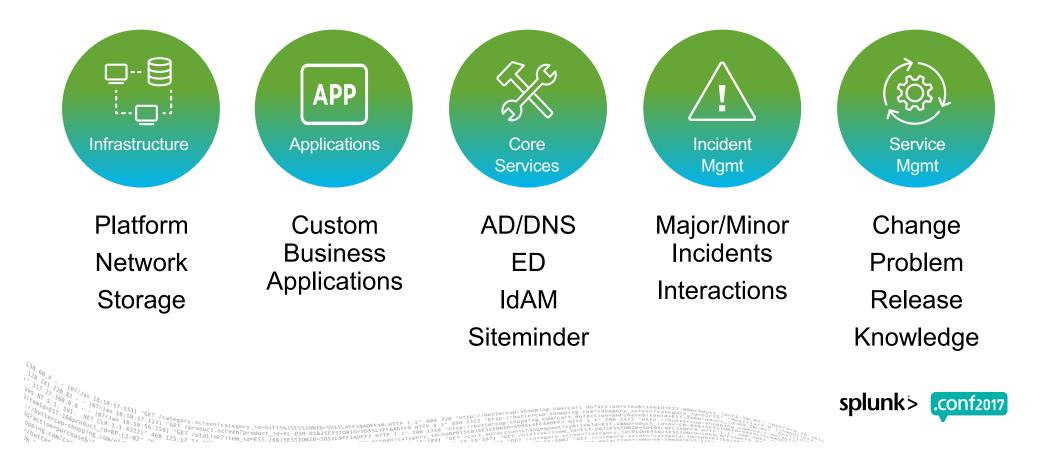
Variable levels of specificity based on organizational role



© 2017 SPLUNK INC

## **IT Operation Analytics**

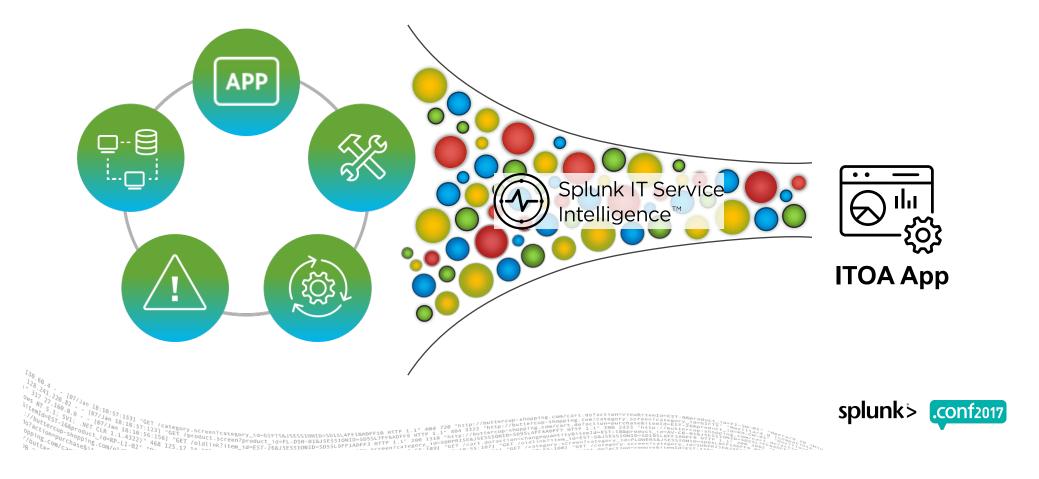
End-to-End visibility for user experience



© 2017 SPLUNK INC.

## **IT Operations Analytics**

Leveraging Splunk ITSI backbone to organize info in custom application



## **ITOA Application**

Executive-level health score overview

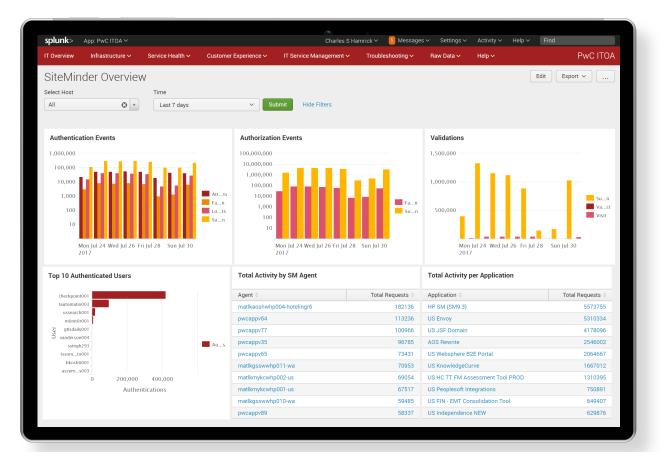
T Overview	Infrastructure 🗸	Service Heal	th∽ Custome	Experience ~	IT Service Manageme	ent 🗸 🔄 1	roubleshooting $\checkmark$	Raw Data 🗸	Help 🗸		PwC ITOA
T Overv	iew									Edit	Export ~
		f IT Operations a	and highlights those	assets or services	where issues are occur	rring in real-t	ime.				
Health Score	e Details (check the bo	ox and scroll do	wn for details on cal	culations)							
	Infrastru	ucture			Service He	ealth		Customer I	Experience ar	nd Service I	Vanagement
											5
PERFORMANCE CAPACITY			BUSIN	ESS APPS	CORE	SERVICES	CUSTOMER	EXPERIENCE	SERVICE N	ANAGEMENT	
	Perform	nance			Business Appli	ications		Customer Experience			
Performance	\$	Status 0	Health Score 0	Business App	lication Service 0	Status 0	Health Score 0	Customer Exper	rience 0	Status 0	Health Score 0
Palo Alto Fire	wall		93	MyPortfolio		72		Interactions		<b>v</b>	73
VMware Perfo	ormance		95	CIA			74 Incidents				100
Network				Feedback			74	Major Incidents			100
Wireless				KSG - Profile			74	Customer Satis	faction		100
Storage				Tax Source			74				
						« prev	2 next »				
	Capac	ity			Core Servic	ces		Service Management			
Capacity 0		Status 0	Health Score 0	Core Service 0		Status 0	Health Score 0	Service Manage	ment 0	Status 0	Health Score 0
VMware Capac	city	Ø	95	IdAM			86	Change			100
Network				AD-DNS			89	Release			100
Wireless				Siteminder			94	Problem			100
Firewall				MobileIron			94				
Storage				ED			99				
		and the Const		the state of the	and are currently in the p						

- 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

splunk>	App: PwC ITOA 🗸			Charles S	Hamrick 🗸 🛛 👍	Messages ~ Settings	✓ Activity ✓	Help V Find
IT Overview	Infrastructure 🗸	Service Health $\sim$	Customer Experience 🗸	IT Service Management $\checkmark$	Troubleshootin	g ∽ Raw Data ∽	Help 🗸	PwC ITOA
This dashboar	s (right pane). Click on t	t health scores (infrastr		vice management) for each servic	e. Each compone	nt health score is calculate	ed as a weighted	Edit Export
					Infi	rastructure KPIs		
	In	frastructur	0		Int	frastructure_KPI 0	Value 0	Time Trend 0
	11	Ji usti uctui	e .		CF	PU Utilization: %	47.17	
					M	emory Free: %	66.30	
			83	3%	St	orage Free Space: %	14.67	
					Арј	plication KPIs		
A	pplication				Ap	plication_KPI 0	Value 🗘	Time Trend 🗅
					Au	thentication Rejections	40.00	
			100%	$\sim$	Fa	iled Handshakes	1.00	Ammin
					Fa	iled Logins	28.00	
				<b>C</b> <sup>1</sup> . 1	н	gh Queue Depth	0.00	
	l'Service	·····		Siteminder	п	Service Management H	Pls	
	Managemer	nt 🚺			Se	rvice_Management_KPI 0	Value 0	Time Trend 0
1	nunugemer	"	93%		Vo	lume Future RFCs	2.00	
			90%		Vo	lume Past RFCs	1.00	
					Vo	lume of Incidents	2.00	
					Vo	lume of Major Incidents	0.00	

- 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



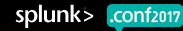
- Native Splunk ITSI functionality
- Correlate KPIs in context with each other
- Viewable by entity
- Service dependencies available as defined
  - Authentication tier
  - Web/Database tier



© 2017 SPLUNK INC

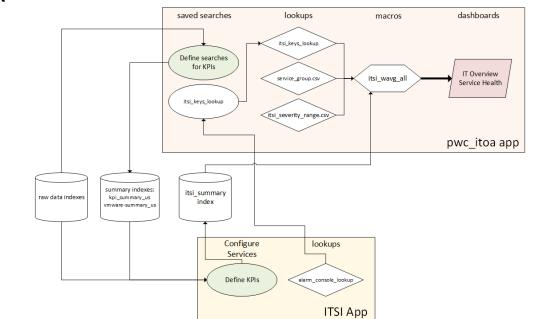
# Integrating Splunk ITSI with ITOA app

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

Siteminder /	o	
Entities KPI Service Dependencies		
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.
× Alias ~ × host	matches ~ X MATLKSMPSIFP*	
× Info ~ (* itsi_role	matches v v operating_system_	host
+ Add Rule (AND)		
+ Add Set of Rules (OR)		
3 Entities		10 per page ∽
Title ^	Aliases	Info
MATLKSMPSIFP001	MATLKSMPSIFP001	6.1.7601, operating_system_host, Microsoft Windows Server 2008 R2 Enterprise, WinHostMon
MATLKSMPSIFP002	MATLKSMPSIFP002	6.1.7601, operating_system_host, Microsoft Windows Server 2008 R2 Enterprise, WinHostMon
MATLKSMPSIFP003	MATLKSMPSIFP003	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-ITS	I-OS:Perfo	rmance.CPl							
KPI base search used by KPIs that track CPU perform									
Sear	rch? (index=* tag tag=cpu) Bun Search ta	g=oshost tag=performa	ance						
KPI Search Sched	6	linutes ~							
Calculation Wind	ow? Last 5 Mi	nutes 🗸							
Monitoring Lag (second									
Monitoring Lag (second		ommended Lag 🛽							
Split by Ent	Split by Entity? Yes No								
Filter to Entities in Serv	ice? Yes N	0							
	Service must h	Service must have entities to filter by entities							
Entity Lookup Fi	eld? host	host							
Entity Alias Filte	ering × host	× host							
			n the entity value) that you w						
		search. (For example, "hos ated with the service.	t", "ip_address", etc.). This fil	ters out all other					
4 Metrics	filter				Add Metric				
Title ^	Threshold Field	Entity Calculation	Service Calculation	Unit	Actions				
cpu_interrupts	cpu_interrupts	avg	avg	ct/s	Edit ~				
	cpu_load_percent	avg	max	%	Edit ~				
system_thread	system_threads_c	avg	avg	count	Edit 🛩				
wait_threads_c	wait_threads_count	avg	avg	thds	Edit 🗸				

- 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

		۲	
splunk> App: IT Service Intelligence			Wade T Cooper v Messages v Settings v Activity v Help v Find
Service Analyzer 🗸 Notable Events Re	view Glass Tables Deep Dives Multi KPI Alerts S	Search 🗸 Configure 🗸 Product Tour	IT Service Intelligen
Siteminder 🗸			
Service description 🥖			
Entities KPI Service Depen	Idencies		
KPIs Clone New ~	Composite Score: 100 Normal Range: Critical 0:20, High 20-40, Medium 40-60, Low 60-80, Normal 80-100		
Service Health	KPI Title	Simulated Severity	Importance
Authentication Rejections	Authentication Rejections	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
	CPU Utilization: %	III Normal V	0 1 2 3 4 5 6 7 0 9 10 11
CPU Utilization: %	CPU Utilization: % MATLKSMPSIFP001	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
CPU Utilization: % MATLKSMPSIFP001	CPU Utilization: % MATLKSMPSIFP002	Normal V	0 1 2 3 4 5 6 7 8 9 10 11
CPU Utilization: % MATLKSMPSIFP002	CPU Utilization: % MATLKSMPSIFP003	Normal ~	0 1 2 3 4 5 6 7 8 9 t0 t1
CPU Utilization: % MATLKSMPSIFP003	Failed Handshakes	III Normal V	0 1 2 3 4 5 6 7 8 9 10 11
Failed Handshakes	Failed Logins	Normal V	0 1 2 3 4 5 6 7 8 9 10 11
	High Queue Depth	III Normal 🗸	0 1 2 3 4 5 6 7 8 9 10 11
Failed Logins	Memory Free: %	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
High Queue Depth	Memory Free: % MATLKSMPSIFP001	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
Memory Free: %	Memory Free: % MATLKSMPSIFP002	II Normal V	0 1 2 3 4 5 6 7 8 9 10 11
Memory Free: % MATLKSMPSIFP001	Memory Free: % MATLKSMPSIFP003	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
Memory Free: % MATLKSMPSIFP002	Storage Free Space: %	II Normal V	0 i 2 J 4 5 6 7 8 9 10 11
Memory Free: % MATLKSMPSIFP003	Storage Free Space: % MATLKSMPSIFP001	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
	Storage Free Space: % MATLKSMPSIFP002	II Normal V	0 1 2 3 4 5 6 7 8 9 10 11
Storage Free Space: %	Storage Free Space: % MATLKSMPSIFP003	III Normal ~	0 1 2 3 4 5 6 7 8 9 10 11
Storage Free Space: % MATLKSMPSIF	Volume Future RFCs	Normal V	0 1 2 3 4 5 6 7 8 9 10 11
Storage Free Space: % MATLKSMPSIF	Volume of Incidents	Normal ~	0 1 2 3 4 5 6 7 8 9 10 11

- 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

Looki	ups New L	ookup										Lookup Editor
Loc	okup Ed	it										
< Bac	k to Lookups L	ist										
serv	vice_group.	CSV							Import	Export	Revert	to previous version 🗸
	5 1											)
O Rigi		e for editing op		Oren in all a shihibi ana a	0	0T	0.10.	ITO				C. L.
	Service	KPI	service_kpi	ServiceHealthName		GroupType	SubGroup	ITOverviewGroup		Description		link
2	AD-DNS	Storage Free	AD-DNS -	AD/DNS	AD-DNS	Infrastructure	Disk	AD-DNS	Mimimum			/app/pwc_itoa/service
		Space: %	Storage Free						from all AD		's during	form.service=AD%2FD
			Space: %						the last 5 m			
3	AD-DNS	Memory	AD-DNS -	AD/DNS	AD-DNS	Infrastructure	Memory	AD-DNS	Mimimum		·	/app/pwc_itoa/service
		Free: %	Memory						available fr			form.service=AD%2FD
			Free: %						servers dur	ing the last	15	
4	40.000	0.011	10.010	10 (01)0	10.0110		0.011	10.010	minutes			
4	AD-DNS	CPU	AD-DNS -	AD/DNS	AD-DNS	Infrastructure	CPU	AD-DNS	Maximum 9			/app/pwc_itoa/service
		Utilization: %	CPU						from all AD		's during	form.service=AD%2FD
5	AD-DNS	N 1 6	Utilization: %			D	1.11.1		the last 5 m		1.1	
5	AD-DNS	Volume of Incidents	AD-DNS - Volume of	AD/DNS	AD-DNS	Process	Incidents	AD-DNS	Volume of i		ened the	/app/pwc_itoa/service form.service=AD%2FD
		Incidents							previous da AFFECTED	·	-**	Torm.service=AD%2FD
6	AD-DNS	Volume of	Incidents AD-DNS -	AD/DNS	AD-DNS	Process	Major	AD-DNS	Volume of r			/app/pwc_itoa/service
Ŭ	AD-DN2	Volume of Major	AD-DINS -	AD/DINO	AD-DNO	FIOCESS	Incidents	AD-DINO	opened the	· ·		form service=AD%2FD
•							The months		The net net 1 (1) is			•
												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

SI_Wavg_all(3) dvanced 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	d, enclose them in dollar signs. For example: \$arg1\$
<pre>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_group.csv service_kpi     dedup service_kpi     dokup itsi_severity_range.csv alert_severity     eval weight_low_val = if(weight=11, range_val, 100)     eval weight_new = weight     eval wavg = (range_val*weight_new)/weight_sum     eval wavg_min_val = if(weight_low_val</pre>	
<pre>  eval health_score=if(totNum==0, "", health_score)   fields - totNum]</pre>	

- 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

Q New Search Save As	~
`itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=Siteminder", by_clause="by ServiceGroup, link, active_link")`	
<pre>append [`itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=AD-DNS", by_clause="by ServiceGroup, link, active_link")`]</pre>	
<pre>append [`itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=IdAM", by_clause="by ServiceGroup, link, active_link")`]</pre>	
<pre>append [`itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=MobileIron", by_clause="by ServiceGroup, link, active_link")`]</pre>	
<pre>append [`itsi_wavg_all(time_filter="earliest=-30m", search_term="ServiceGroup=ED", by_clause="by ServiceGrou link, active_link")`]</pre>	p,
<pre>sort health_score</pre>	
<pre>eval Metric=ServiceGroup, Status = case(health_score&lt;30, "severe", health_score&lt;70,"elevated", health_score &lt;101, "low")</pre>	
<pre>table Metric Status health_score link active_link</pre>	
rename Metric as "Core Service", health_score as "Health Score"	
<pre>eval "Health Score" = round('Health Score', 0)</pre>	
append [	
inputlookup temp_data.csv	
<pre>search ServiceCategory=CoreService</pre>	
rename Service AS "Core Service", Health AS "Health Score"	
<pre>table "Core Service" Status "Health Score" link active_link</pre>	
1	

- Call the wavg\_all macro
  - Pass necessary variables
    - Time
    - Service Group
    - By clause



© 2017 SPLUNK INC

# **Closing The User Experience Gap**

## Desktop monitoring



© 2017 SPLUNK INC.

# **Desktop User Experience** Augment ITOA with 3<sup>rd</sup> party add-on uberAgent data APP uberAgent Splunk IT Service Intelligence<sup>™</sup> **ITOA App** splunk'> .conf2017 DISLAFF10ADFF 01&ISESSIONIE

© 2017 SPLUNK INC.

## **Desktop User Experience**

## uberAgent

- 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





## **Desktop User Experience**

Boot & logon dashboard – uberAgent (custom)

<b>splunk</b> > App: PwC uberAgent ∽	Charles S Hamrick 🗸 Messages 🗸	Settings v Activity v Help v Find
Custom V Proactive Improvement V Client Change Management V	Windows 10 Migration ~	uberAgent
Boot & Logon Time range: Filter category: Last 1 month	Filter value(s): IP address filter:	OS filter category: OS version
OS filter value:		
	.8 s 443,62	<b>36.6</b> s avg. duration
PCs not booted for days histogram		
15,000 E 5,000 		' 21 ' 22 ' 23 ' 24 <sup>'</sup> 25 <sup>'</sup> 26 <sup>'</sup> 27 <sup>'</sup> 28 <sup>'</sup> 29 <sup>'</sup> 30 <sup>'</sup> 6051 <sup>'</sup> 6052
	Not booted for days	

- 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)

splunk>	App: PwC uberAgent 🗠			Charles S Hamrick ∽ Message	s ∽ Settings ∽ Activity ∽ H	Help ∨ Find
Custom 🗸	Proactive Improvement $\sim$	r Client Change Management ∽	Windows 10 Migration 🗸			uberAgent
Storage	e Monitoring					Export v
Time range:		Filter category:	Filter value(s):	IP address filter:	OS filter cate	gory:
Last 1 week	× _	Hardware model 😵 🔻	× All	*	OS version	♥ ▼
OS filter value:	Q v	Submit Hide Filters				
Overview 6	<b>2,91</b>		6 re models	<b>56.7</b>		<b>29.5 GB</b> avg. capacity
Disk capa	acity (GB)		Ε	Disk capacity (%)		
Free disk spa	ace less than:		F	ree disk space less than:		
2 GB	O v			1%	v	
2	2,178	3 28	30	1,52	0	14

- 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)

	o: uberAge	nt 🗸						Charl	es S Ha	_	Messages ∨	Settings	s ∽ Activity ∽	Help ∨	Find	
Splunk∨ Ma	chines 🗸	Session	s∨ Applica	tions 🗸 🛛 I	Processes \	- On/0	Off Transition	s∨	SBC/V	) v	Licensing ∽	Support	t∽		ub 🗗	erAgent
Single Ma															Expor	t 🕶 🛛
This dashboard dis	plays deta	iled informat		ic machine.												
Time range:		~	Filter field:		0 v	Filter opera		er express				Submit	Hide Filters			
					•		•				Add filter					
Machine:			#Sessions:	#11	sers:	#Logo	200	#400	s in forq	round:						
CHAMRIC	K0012	28	5	1	Sers.	#Logo	/15.	14	sinitory	round.						
Avg. CPU:	Avc	I. RAM:	Avg. disk:	A	vg. network		Avg. UI late	ncv:		Total UI w	ait time:	Ava. I	logon duration:	Apr	o errors:	
11.7 %		2.9 %	2.44 %		.013 %		203 µs			54507			27 s	0		
																_
Sessions																
		1	Logon		1				Avg.	A	Avg. IO	Avg.	Avg.	Avg. app UI	Avg. ICA	Demotion
User 0	ID 0	Logon time 0	duration (s) ≎	Last seen 0	Last state 0	Protocol 0	#process	Avg. es 0	CPU (%) ି	Avg. IOPS 0	latency (ms) ≎	RAM (MB) 0	network (KB/s) ≎	latency (µs) ≎	latency (ms) ≎	Remoting clients 0
NAM\chamrick0	01 1	2017-07-11 12:53:00	7	2017-07-17 12:53:00	active	Console		95	6.6	4.2	0.6	6883	17.8	248		
NAM\chamrick0	01 1	2017-07-12 10:15:41	2	2017-07-12	active	Console		80	4.2	3.3	1.1	5738	10.3	61		
Notwork d	ata va		atency ove					CD			ver time					
6,000	ata v0	iui ne a li	atency over	ume			15,000				ver time					40
							13,000									
₩ 4,000		$\land$					10,000 at		5		$\wedge$				~	
volum					_		ncy (r	AM (C	0			_				20 CPU (%)
Data D							5,000 3	~	5			Ŷ	~~~/			10
Sat Ju	<u>,</u>	Sat Jul 8	Sat Jul 15	Sat J	ul 22				Sat Ju		Sat Jul 8		Sat Jul 15	Sat Jul 22		
2017	end volur	ne (MR)	Receive volum	e (MR) 🗕	Ava send	latency (m	0		2017			Avg. RAM (	(GB) — Ava	CPU (%)		
5	enu volun		Receive volum		Avg. senu	iatericy (iii:	5/					Avg. NAM	(36) — Avg	. CFU (/0)		
2017	I 1 end volur		Sat Jul 15 Receive volum				10,000 Latency (ms) 5,000 s)	(B)	5 Sat Ju				Sat Jul 15 (GB) — Avg			

- 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



splunk'> .conf201

## 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





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



## Want to Learn More About Splunk ITSI at .conf2017?

		Ready, Set, Go! Learn From Others - The First 30 Day Experiences of ITSI Customers: Tuesday, September 26th, 201712:05 PM- 12:50 PM Room Salon C
		Splunk ITSI Overview: Tuesday, September 26th, 2017 1:10 PM-1:55 PM Room 147 AB
Tuesday		PWC: End-to-End Customer Experience: Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room 143ABC
Tuesday		RSI: Operational Intelligence: How to go From Engineering to Operationalizing IT Service Intelligence Where the Rubber Meets the Road:
September		Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room147AB
26 <sup>th</sup> , 2017		Cardinal Health: Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring Using Splunk ITSI:
		Tuesday, September 26th, 20173:30 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
		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, 201711:00 AM-11:45 AM Ballroom C
Wednesday		Triggering Alerting (xMatters) and Automated Recovery Actions from ITSI: Wednesday, September 27th, 2017 1:10 PM- 1:55 PM Room Salon C
September		Leidos - Our Journey to ITSI: Wednesday, September 27th, 2017 2:15 PM-3:00 PM Room147AB
27 <sup>th</sup> , 2017		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
		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		Thursday, September 28th, 2017 11:35 AM- 12:20 PM Room Salon C
September		Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:
28 <sup>th</sup> , 2017		Thursday, September 28th 11:35 AM - 12:20 PM in Ballroom B
1 * ?/#g		IT Service Intelligence for When Your Service Spans Your Mainframe and Distributed ITSI:
1 temida: 1: 0.0 (07/Jan 18:10) "GET		Thursday, September 28th, 2017 1:20 PM-2:05 PM Room Salon C
-:actionspurchaseki: Doping:computchaseki: 0 utter: 0	ategor "GET / ] "GET 125.17	y.screen?category_id=GIFTS&JSESSIONID=SDISL4FF18ADFF18 HTTP 1.1 #04 720 "http://butting_com/cart.do/activ 200 2423 "http://butting_Som/crts."http://butting_com/category_id=SUFTS&JSESSIONID=SDISL4FF18ADFF18 HTTP 1.1 #04 1322 tercore-shopLankapter HTT Id=EST-18Borduct_id=FL-DSH-01&SESSIONID=SDISL4FF18ADFF3 HTTP 1.1 #04 1322 tercore-shopLankapter HTT Id=EST-18Borduct_id=FL-DSH-01&SESSIONID=SDISL4FF18ADFF3 HTTP 1.1 #04 1322 tercore-shopLankapter HTT Id=EST-18Borduct_id=FL-DSH-01&SESSIONID=SDISL4FF18ADFF3 HTTP 1.1 #04 1322 tercore-shopLankapter HTTP Id=EST-18Borduct_id=FL-DSH-01&SESSIONID=SDISL4FF18ADFF3 HTTP 1.1 #04 132 tercore-shopLankapter HTTP Id=EST-18Borduct_id=FL-DSH-01&SESSIONID=SDISL4FF18ADFF3 HTTP 1.1 #04 130 "http://doi.org/10.2 #05 #05 #05 #05 #05 #05 #05 #05 #05 #05