© 2017 SPLUNK INC.

splunk> .conf2017

ITSI in the Wild

Why Micron Technology© chose ITSI and lessons learned from real world experience

Mike Scully | IT Area Lead

Joe Trimmings | IT Area Lead

September 2017 | Washington, DC

© 2017 SPLUNK INC.

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.

splunk> .conf2017

© 2017 SPLUNK INC.

Agenda

- Micron Technology
- Path to ITSI
- ITSI @ Micron
- None to Done
- Lessons Learned
- Advanced ITSI Topics
- Q&A

© 2017 SPLUNK INC.

Micron Technology, Inc.

1978
Founded in Boise, Idaho

#1 Broadest memory solutions portfolio in the industry

26,000+
Patents

Locations in **18** Countries

30,000+
Employees worldwide

2015 No. 1 employer in electric design

DRAM | NAND | HMC | SSD | 3D XPOINT | Solid Scale

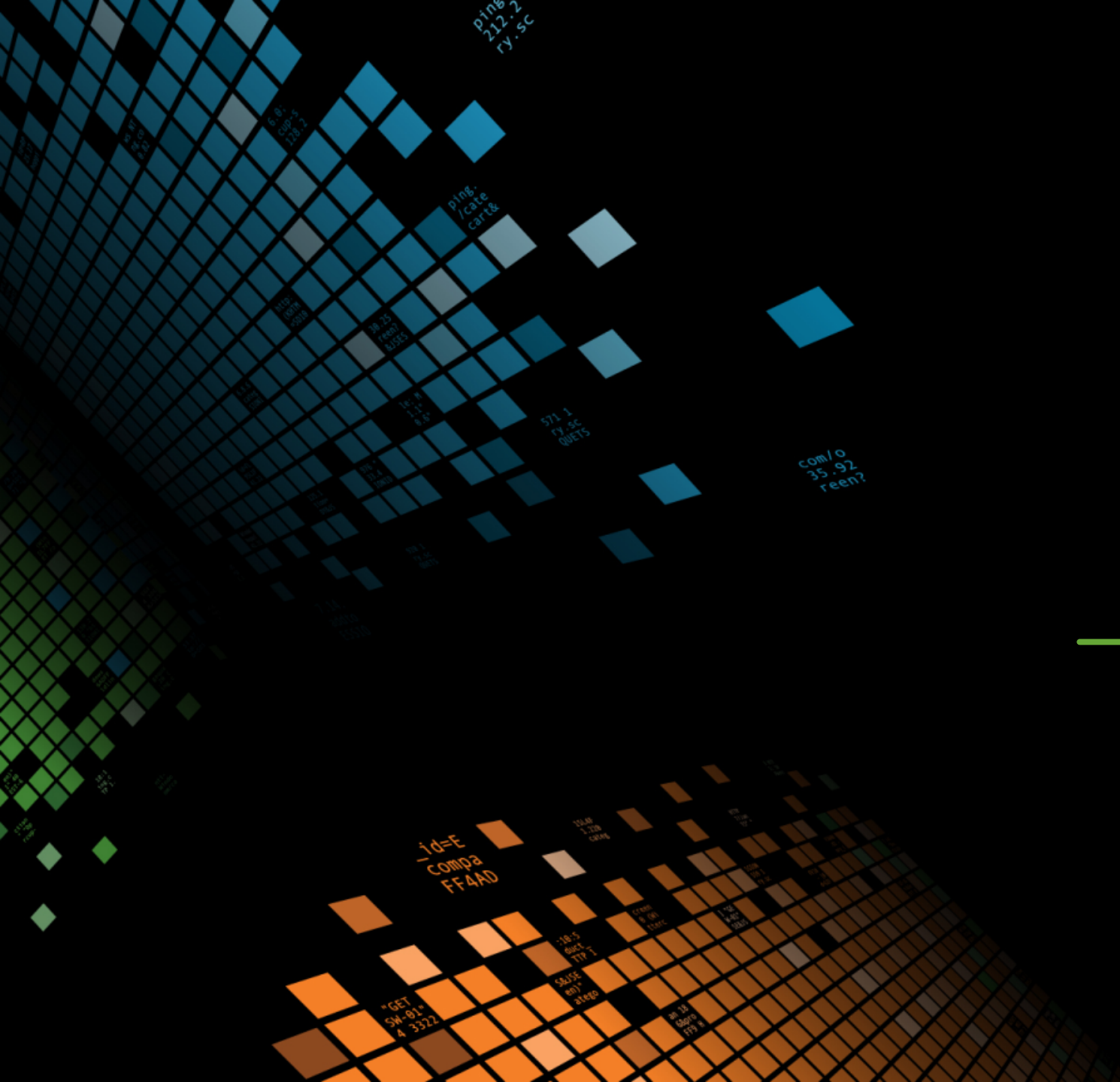
splunk> .conf2017

© 2017 SPLUNK INC.

What Does Manufacturing IT Do For Micron?

- Product Tracking
- Equipment Tracking
- Equipment Integration
- Automated Material Handing System Integration
- Engineering Analysis Software

© 2017 SPLUNK INC.



Path to ITSI

It’s a journey, not a destination

splunk> .conf2017

© 2017 SPLUNK INC.

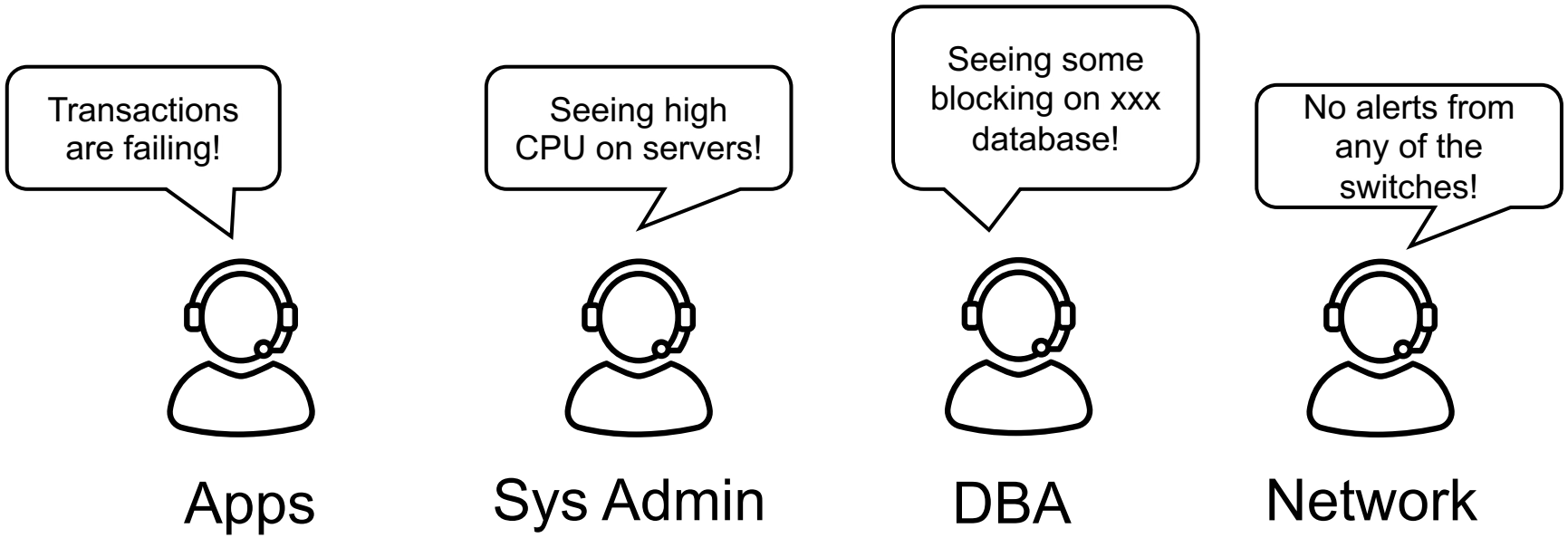
Gopher Effect

How we knew we were having a Major Incident prior to Splunk

© 2017 SPLUNK INC.

Major Incident Bridge

Pre-Splunk



splunk> .conf2017

© 2017 SPLUNK INC.

Silo'd Approach to Alerting and Support

- SME's and experience are a must
- Everyone needs to be involved
- Only a few can help fix a problem
- Breeds distrust during difficult times

© 2017 SPLUNK INC.

Enter Stage Left: Splunk!

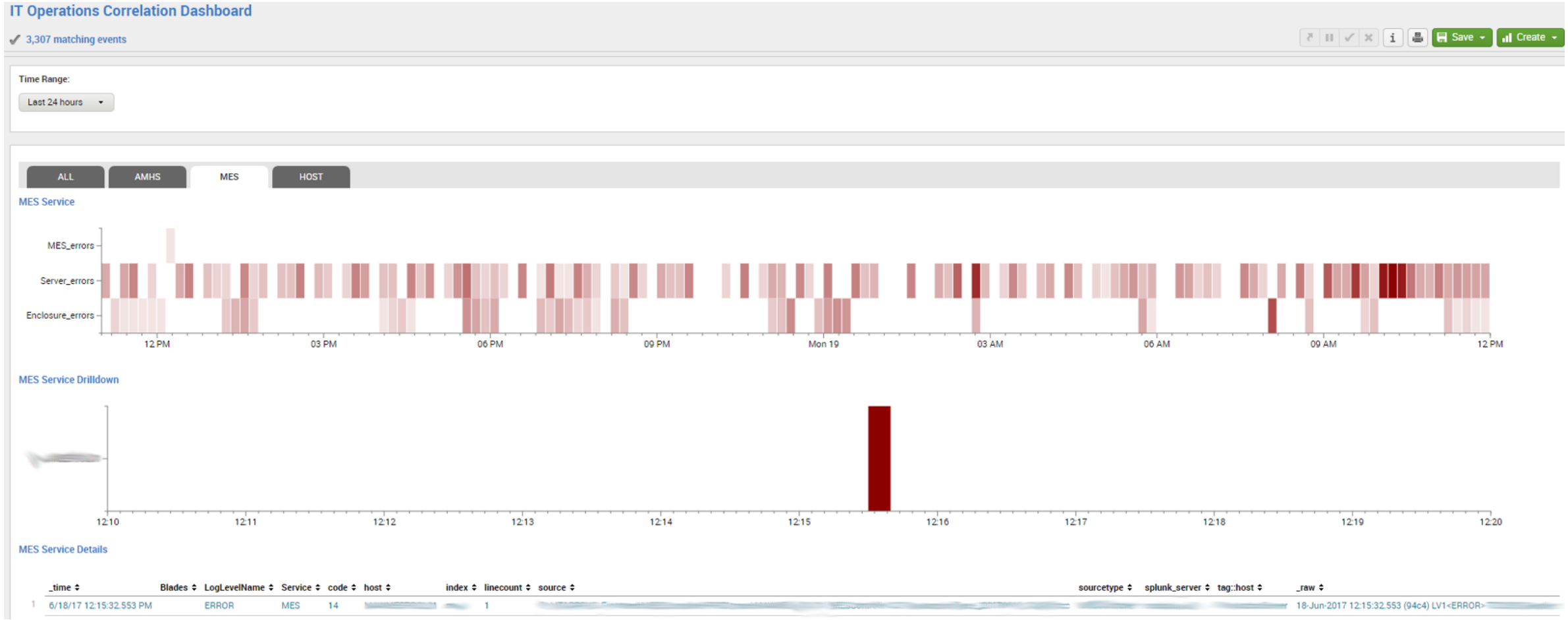
Our Objective in Introducing Splunk to Micron

splunk> .conf2017

© 2017 SPLUNK INC.

Result: IT Operations App

After 6 months of intense work

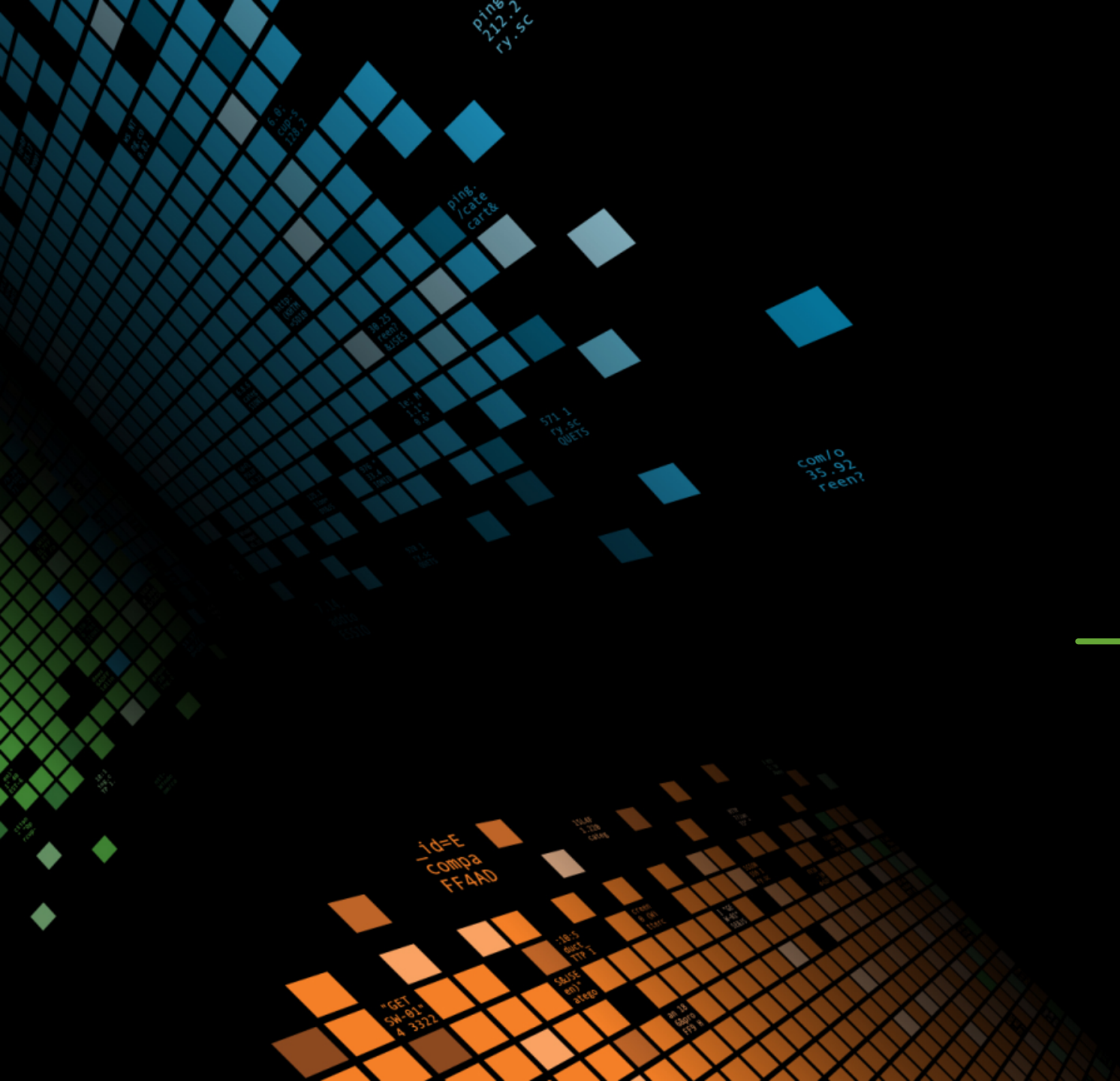


splunk> .conf2017

© 2017 SPLUNK INC.

splunk> .conf2017

© 2017 SPLUNK INC.



ITSI @ Micron

Current State

splunk> .conf2017

© 2017 SPLUNK INC.

Our Current ITSI Stats

89

Services Defined

745

KPI's Defined

78

KPI's w/ anomaly detection

splunk> .conf2017

© 2017 SPLUNK INC.

Results of Implementing ITSI and Splunk

Benchmark Performance

52%↓

Business Impact from Major Incidents

32%↓

Mean Time to Recover from Major Incidents

23%↓

# of Major Incidents

splunk> .conf2017

© 2017 SPLUNK INC.

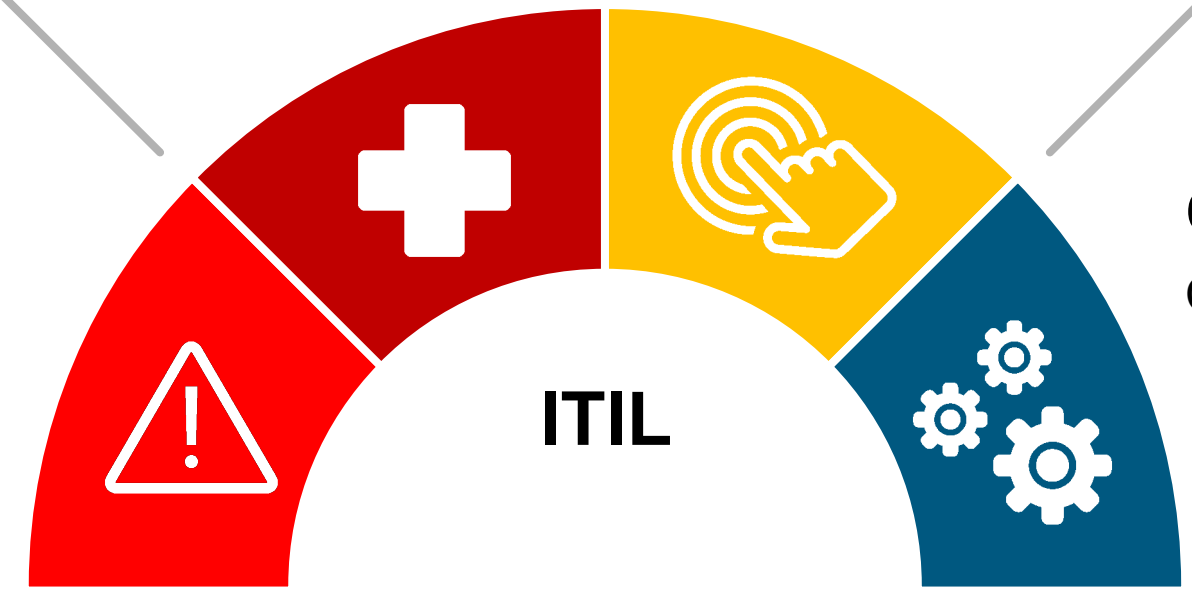
Times When We Use ITSI

Incident Management

Major Incident Investigation
Postmortem Review

Problem Management

Problem Investigation Initiation



Event Management

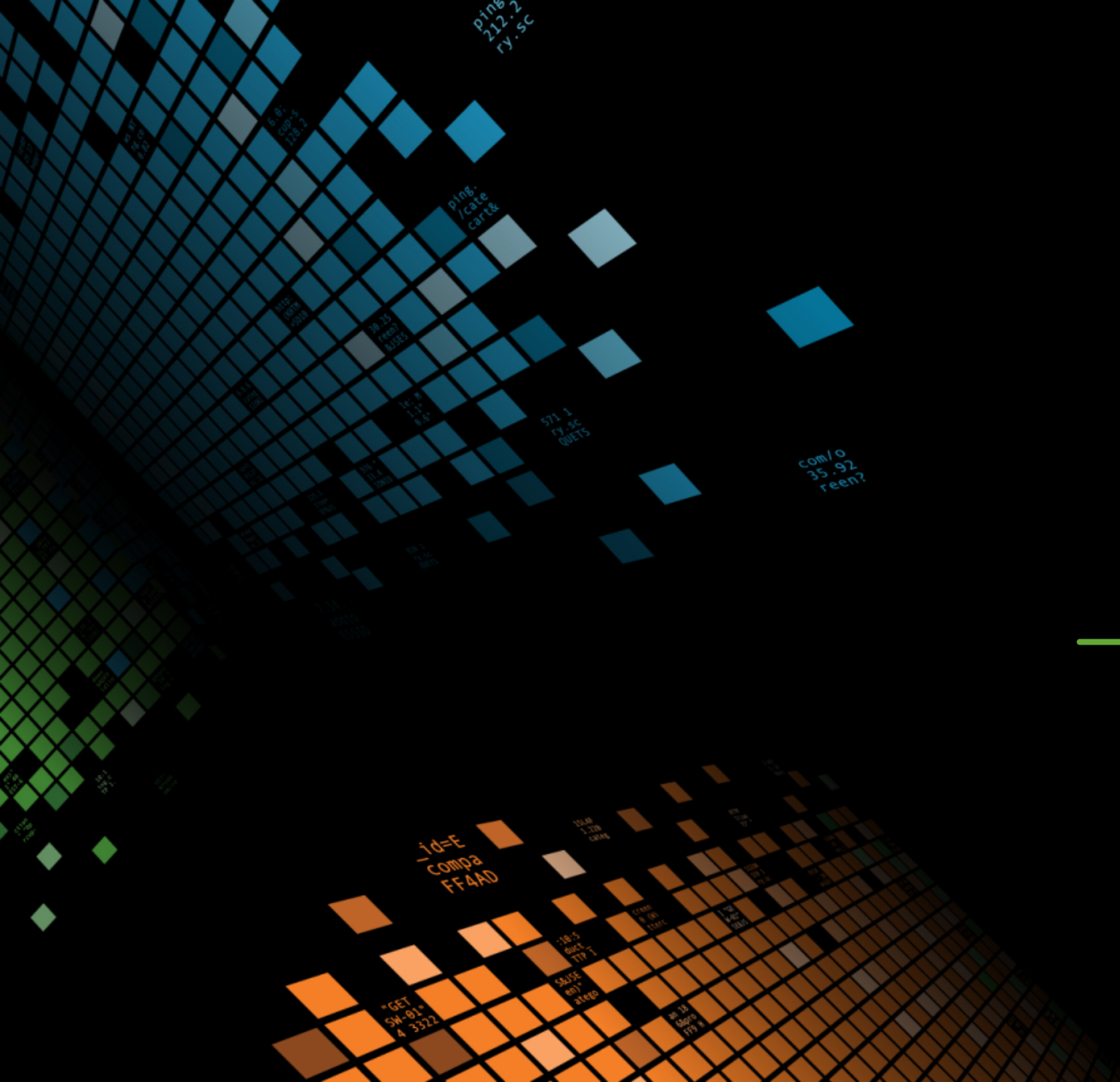
Alerting

Change Management

Change Point Monitoring

splunk> .conf2017

© 2017 SPLUNK INC.



None to Done

Are you ever completely done?

© 2017 SPLUNK INC.

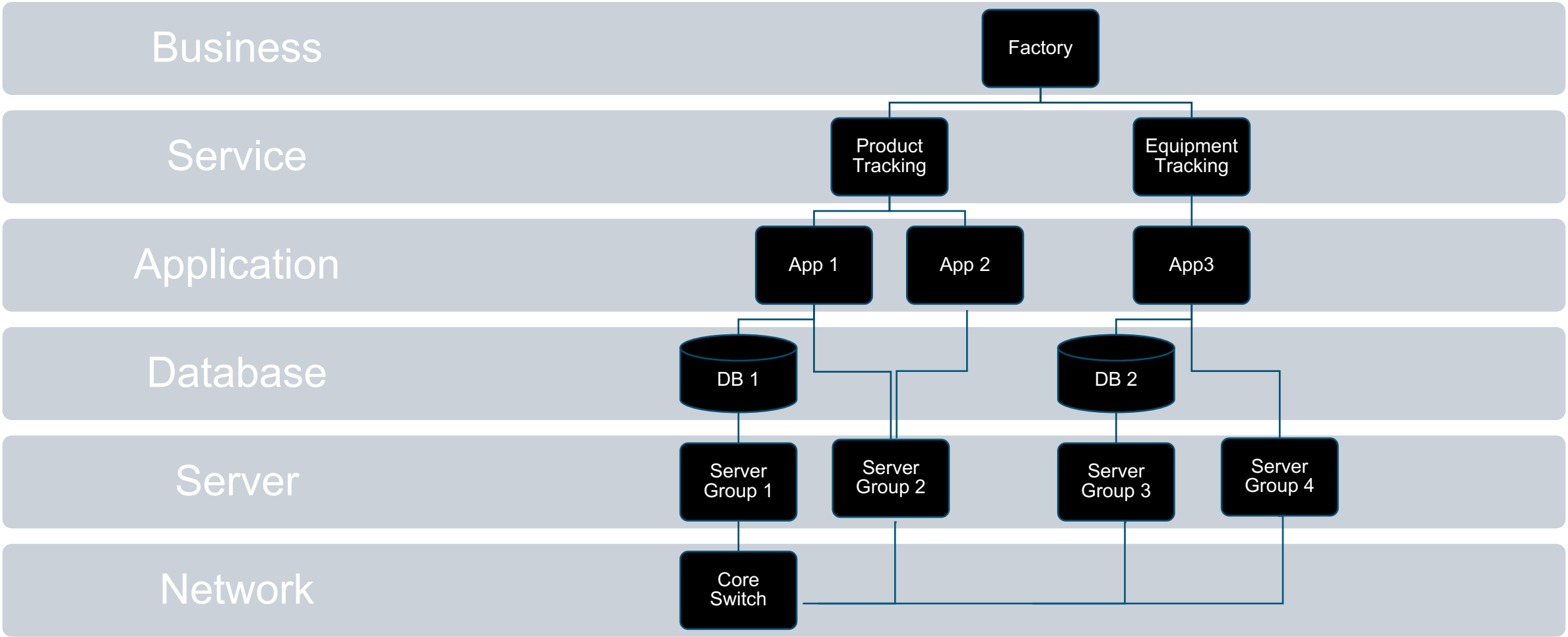
Critical Success Factors

What made us successful

- Executive sponsorship & recognition that this is a journey
- Engaged team of Subject Matter Experts (SME's) across all domains
- Embracing the concept of a ‘Service’ that encompasses multiple tiers of the IT domain
- Training for one or more Splunk ninjas
- Close relationship between Splunk ITSI Engineers and Splunk Admins

© 2017 SPLUNK INC.

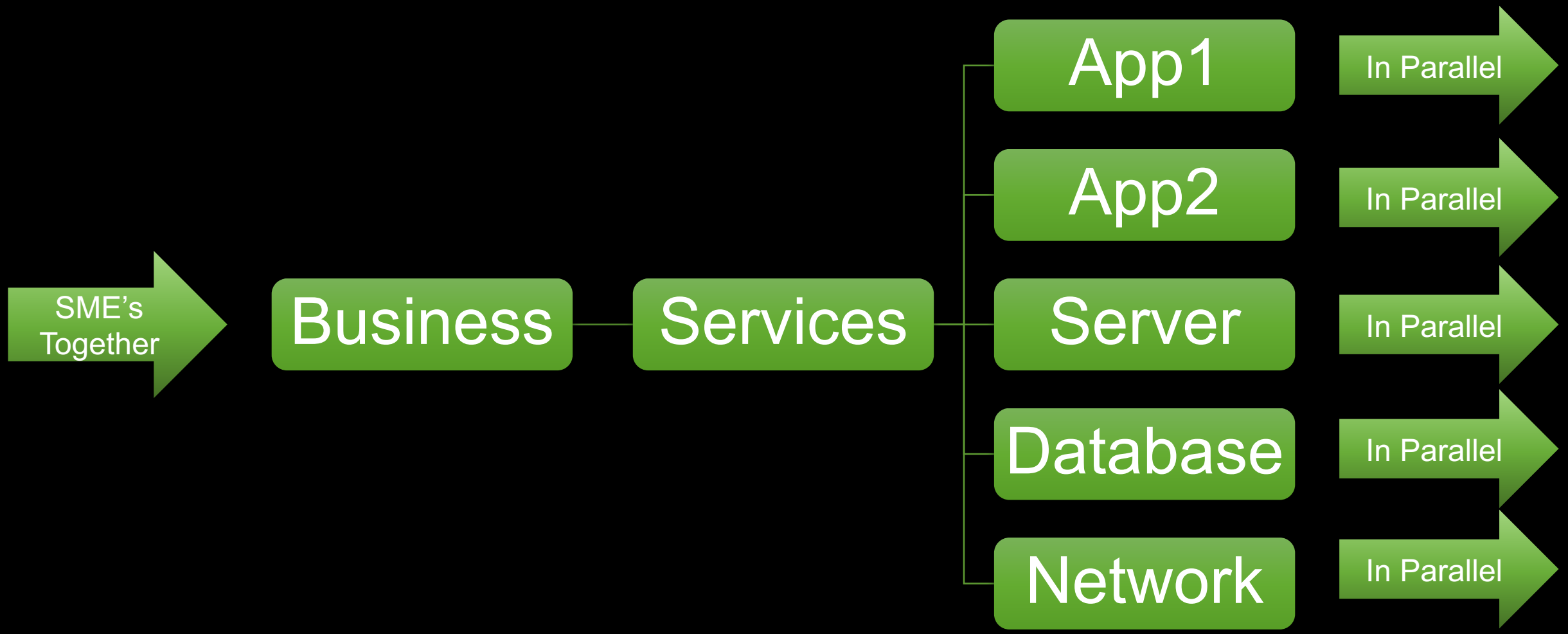
Service Decomposition



splunk> .conf2017

© 2017 SPLUNK INC.

How Do You Get All Your Services Defined?



splunk> .conf2017

© 2017 SPLUNK INC.

The ITSI Service Workflow

How to go about defining an ITSI Service

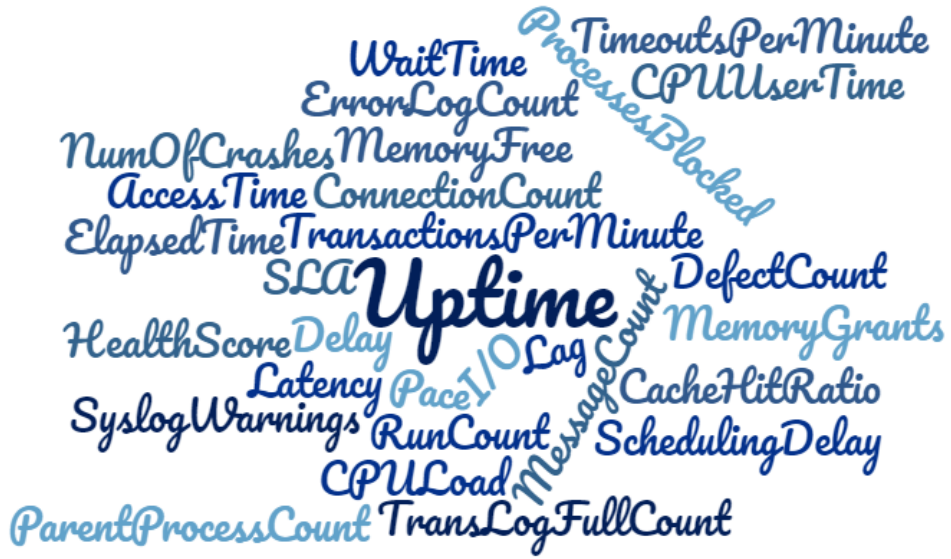
1. Determine the scope of the ITSI Service
2. Define the Entities involved
3. Create the ITSI Service
4. Configure your dependencies
5. Define the KPI's

splunk> .conf2017

© 2017 SPLUNK INC.

KPI vs Metrics

All KPI's are Metrics. but not all Metrics are KPI's



splunk> .conf2017

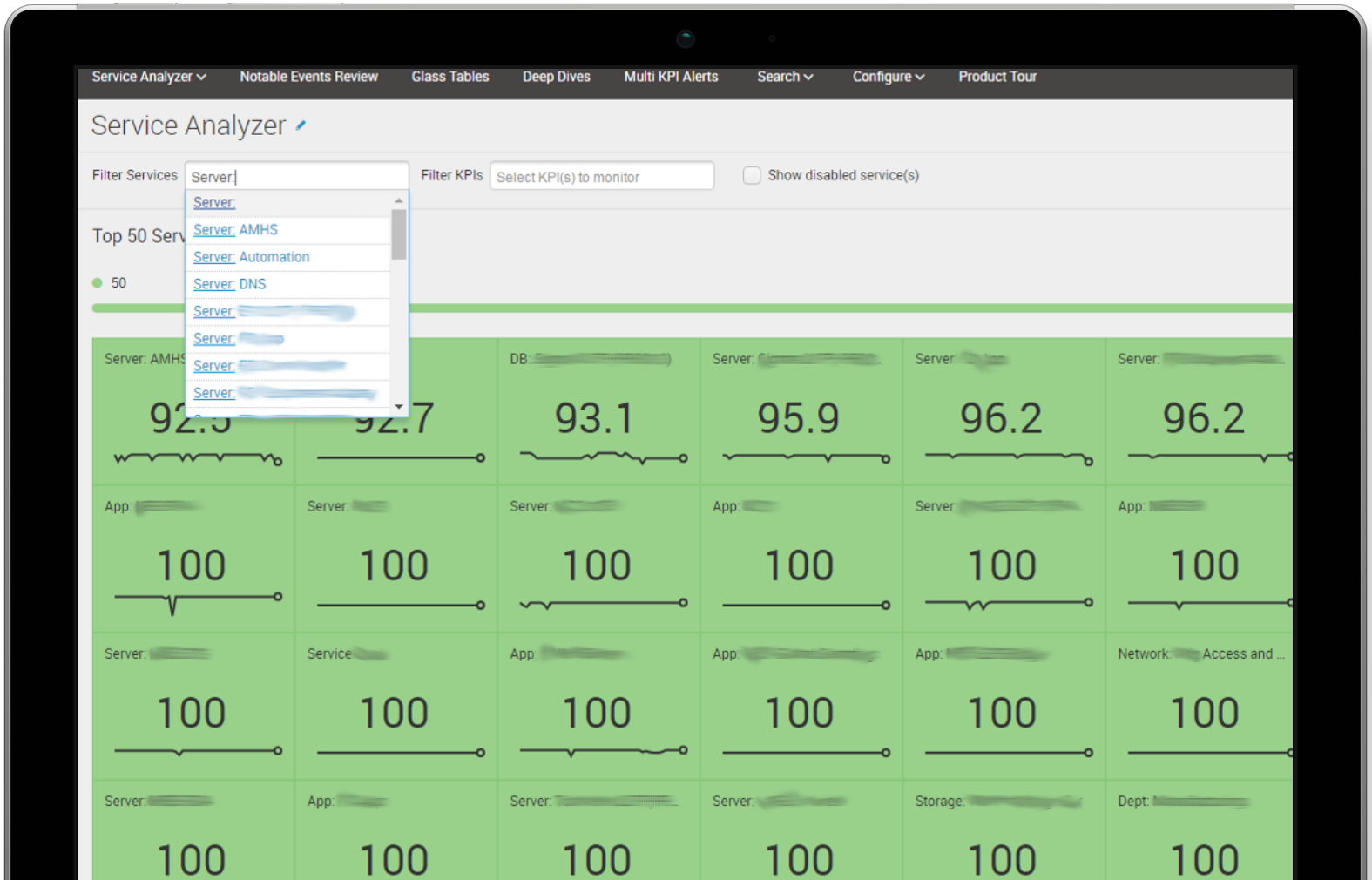
© 2017 SPLUNK INC.

Lessons Learned

© 2017 SPLUNK INC.

ITSI Service Naming

Naming Conventions are very helpful



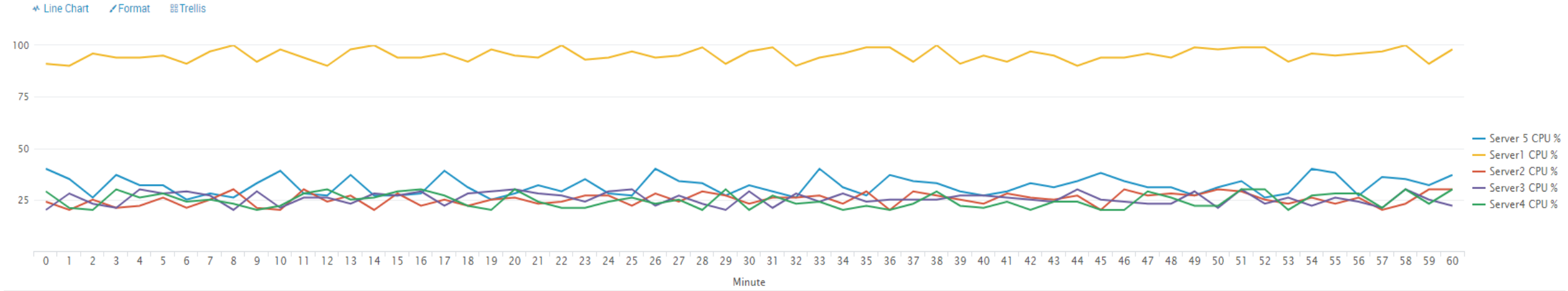
- Service:
  - IT Service Layer ITSI Services
- App:
  - Application Services that support the Business Layer
- DB:
  - Databases that support the applications
- Server:
  - OS KPI's for the servers that run the applications
- Network:
  - Network gear that is critical to the servers

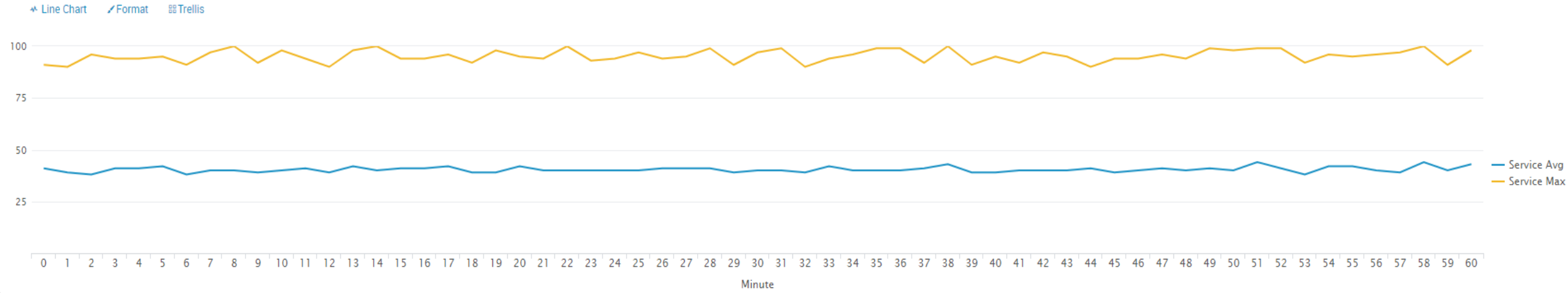
splunk> .conf2017

© 2017 SPLUNK INC.

KPI Aggregation

How you aggregate the KPI matters





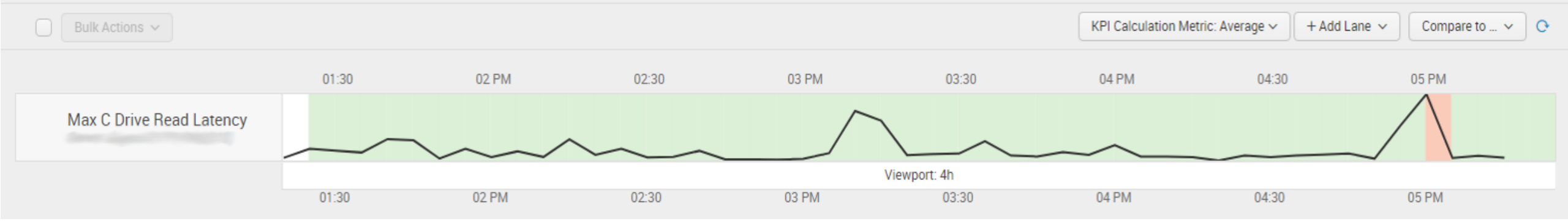
splunk> .conf2017

© 2017 SPLUNK INC.

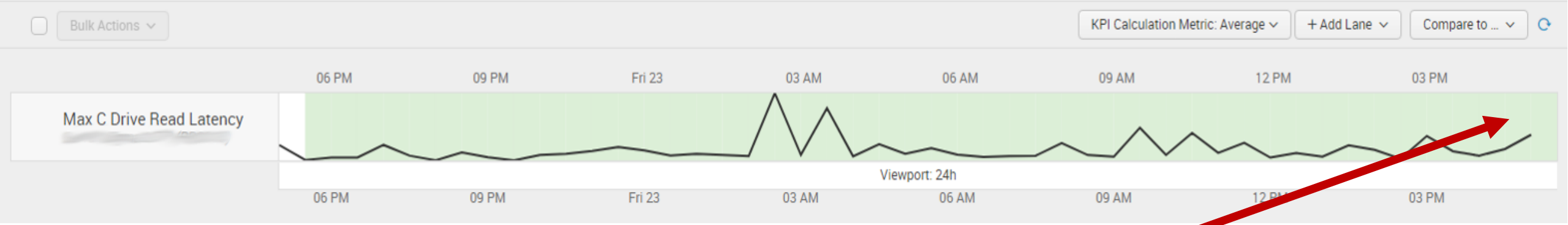
Deep Dive Aggregation

These are the same metric just different time range

Last 4 Hours



Last 24 Hours



Where did my alert go?!?

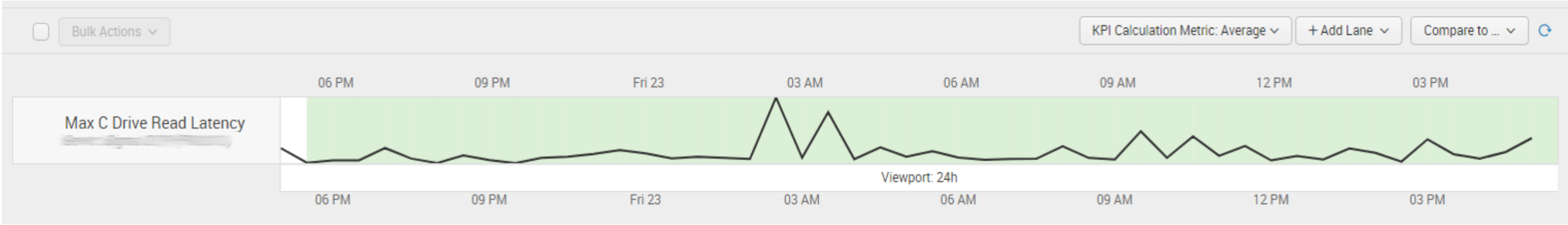
splunk> .conf2017

© 2017 SPLUNK INC.

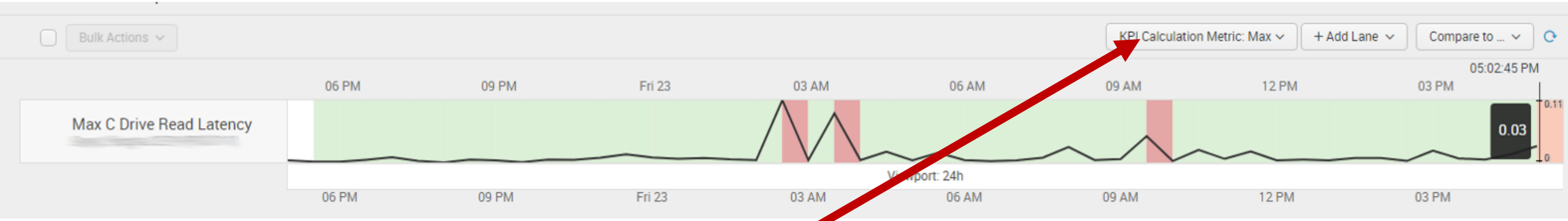
Deep Dive Aggregation

There's my alert!

Last 24 Hours w/ Average Aggregation



Last 24 Hours w/ Max Aggregation



Use Max for KPI's where you have upper thresholds

Use Min for KPI's where you have lower thresholds

splunk> .conf2017

© 2017 SPLUNK INC.

Other Lessons Learned

- Make use of **base searching**
- Make use of **cloning**
- Stop using thresholds to find anomalies. Turn on **anomaly detection.**
- **Fine tune** by adding or removing KPIs or services
- Continually evaluate **data and threshold accuracy**.
- **Consolidate** and use entities to simplify KPI build out.

© 2017 SPLUNK INC.

Advanced ITSI Topics

Satisfy your inner Splunk ninja

splunk> .conf2017

© 2017 SPLUNK INC.

What is ITSI doing in the background?

CPU: Max % User Time

KPI description

Search and Calculate

Source	**Search:** sourcetype=cpu cpu=all **Threshold field:** PercentUserTime	Edit
Entities	**Entity Split by field:** host **Data filtered by service entities in field:** host **Service matches entities on fields:** title	Edit
Calculation	Calculating **Maximum** per entity, **Maximum** of aggregate over the last **5 minute(s)** every **5 minute(s)**	Edit
Unit	**Unit:** %	Edit

Thresholding

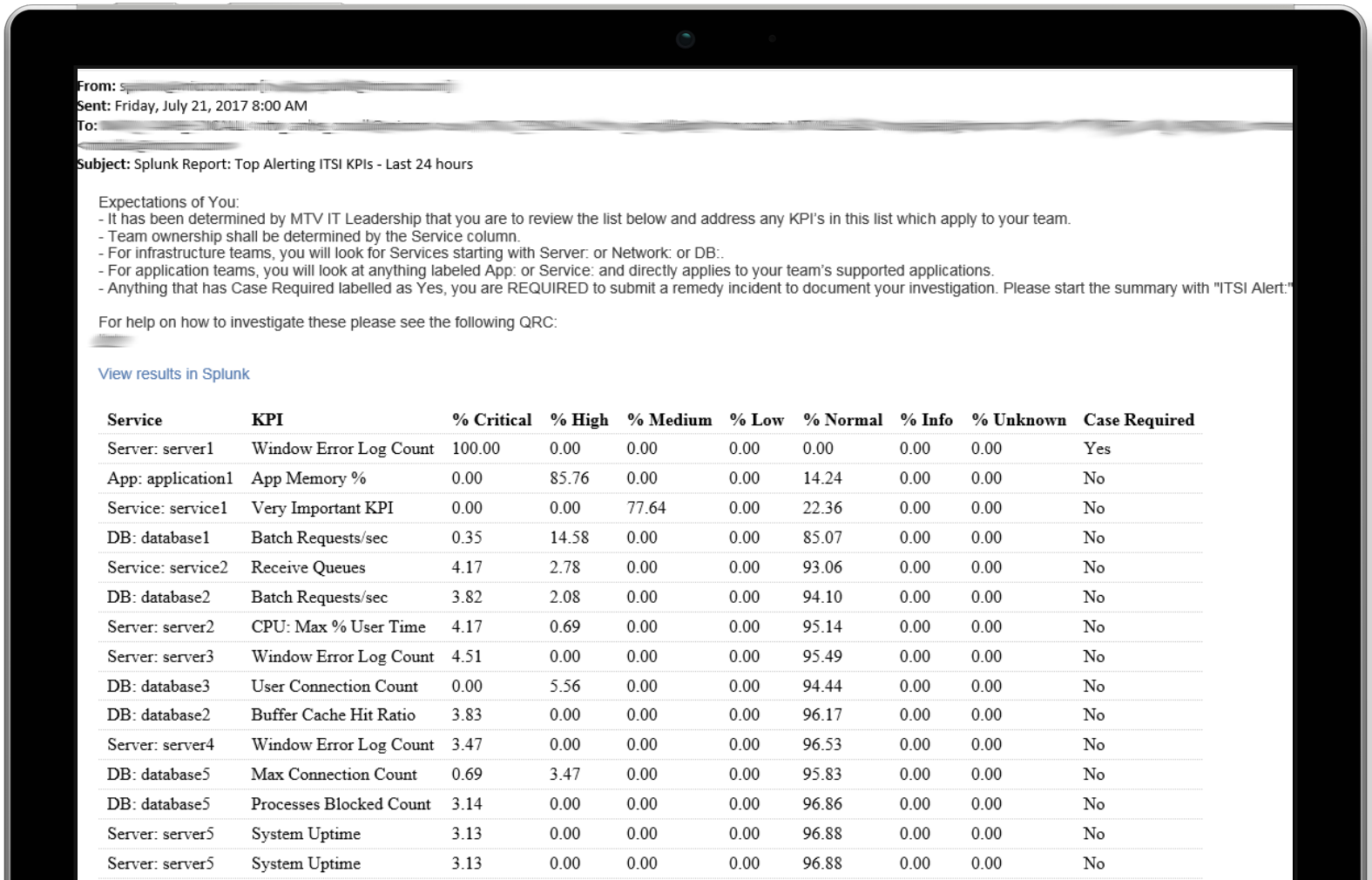
Anomaly Detection

splunk> .conf2017

© 2017 SPLUNK INC.

Daily Reports

What's bubbling under the surface?



From: [redacted]
Sent: Friday, July 21, 2017 8:00 AM
To: [redacted]

Subject: Splunk Report: Top Alerting ITSI KPIs - Last 24 hours

Expectations of You:
- It has been determined by MTV IT Leadership that you are to review the list below and address any KPI's in this list which apply to your team.
- Team ownership shall be determined by the Service column.
- For infrastructure teams, you will look for Services starting with Server: or Network: or DB:.
- For application teams, you will look at anything labeled App: or Service: and directly applies to your team's supported applications.
- Anything that has Case Required labelled as Yes, you are REQUIRED to submit a remedy incident to document your investigation. Please start the summary with "ITSI Alert:"

For help on how to investigate these please see the following QRC:
[redacted]

View results in Splunk

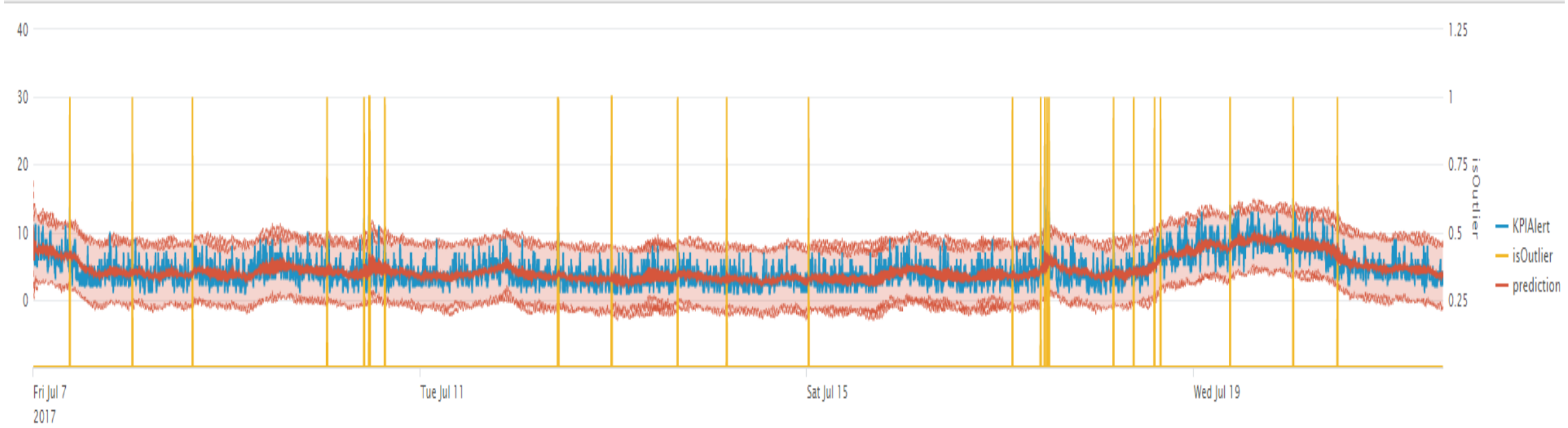
Service	KPI	% Critical	% High	% Medium	% Low	% Normal	% Info	% Unknown	Case Required
Server: server1	Window Error Log Count	100.00	0.00	0.00	0.00	0.00	0.00	0.00	Yes
App: application1	App Memory %	0.00	85.76	0.00	0.00	14.24	0.00	0.00	No
Service: service1	Very Important KPI	0.00	0.00	77.64	0.00	22.36	0.00	0.00	No
DB: database1	Batch Requests/sec	0.35	14.58	0.00	0.00	85.07	0.00	0.00	No
Service: service2	Receive Queues	4.17	2.78	0.00	0.00	93.06	0.00	0.00	No
DB: database2	Batch Requests/sec	3.82	2.08	0.00	0.00	94.10	0.00	0.00	No
Server: server2	CPU: Max % User Time	4.17	0.69	0.00	0.00	95.14	0.00	0.00	No
Server: server3	Window Error Log Count	4.51	0.00	0.00	0.00	95.49	0.00	0.00	No
DB: database3	User Connection Count	0.00	5.56	0.00	0.00	94.44	0.00	0.00	No
DB: database2	Buffer Cache Hit Ratio	3.83	0.00	0.00	0.00	96.17	0.00	0.00	No
Server: server4	Window Error Log Count	3.47	0.00	0.00	0.00	96.53	0.00	0.00	No
DB: database5	Max Connection Count	0.69	3.47	0.00	0.00	95.83	0.00	0.00	No
DB: database5	Processes Blocked Count	3.14	0.00	0.00	0.00	96.86	0.00	0.00	No
Server: server5	System Uptime	3.13	0.00	0.00	0.00	96.88	0.00	0.00	No
Server: server5	System Uptime	3.13	0.00	0.00	0.00	96.88	0.00	0.00	No

- Comes in every morning to the on call and management
- There are clear expectations of the on call to address the issues.
- Also have a daily Unknown report that identifies KPI's which are not working.

splunk> .conf2017

© 2017 SPLUNK INC.

Anomaly Detection on # of ITSI Threshold Breaches



splunk> .conf2017

© 2017 SPLUNK INC.

Deep Dive Drilldown

Extending your investigation beyond Deep Dive!

- Make a copy of deep_dive_drilldown.conf from itsi/default to itsi/local
- Place the following for running the base search drilldown

```
[Run KPI Base Search]
type = search
search = $kpi.base_search$
metric_lane_enabled = false
event_lane_enabled = false
kpi_lane_enabled = true
```

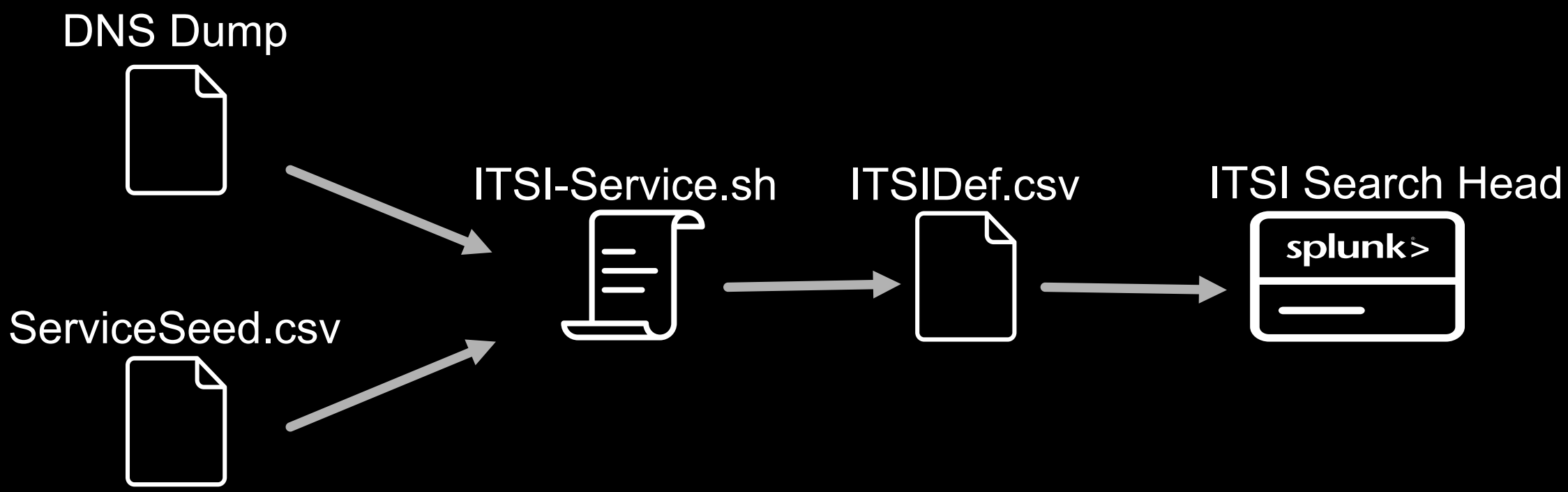
- To callout to a knowledge base web page, place the following

```
[Search RKM]
type=uri
replace_tokens=true
metric_lane_enabled=false
event_lane_enabled=false
kpi_lane_enabled=true
uri=http://somewebserver/some_web_page?searchText=$kpi.kpi_title$
uri_payload_type=simple
```

splunk> .conf2017

© 2017 SPLUNK INC.

Entity Definition

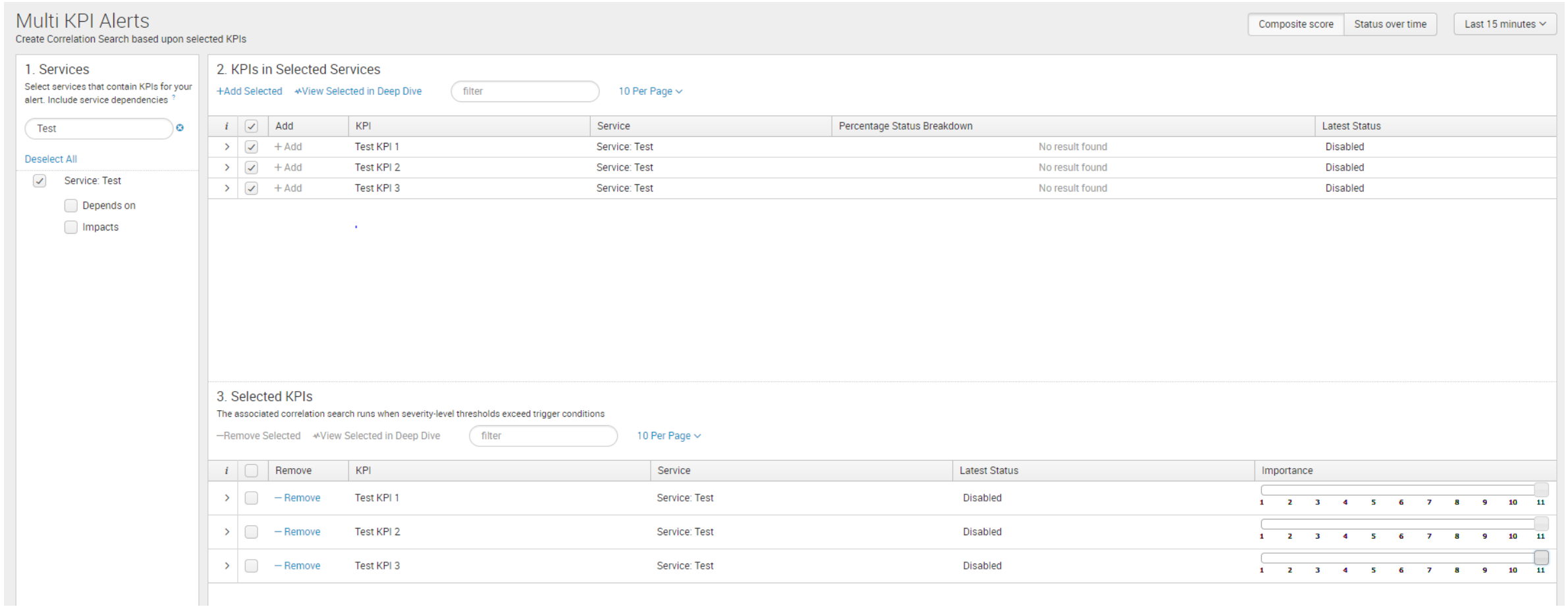


splunk> .conf2017

© 2017 SPLUNK INC.

Alerting

Creating the Multi KPI Alert



splunk> .conf2017

© 2017 SPLUNK INC.

Alerting

Notable Event Aggregation Policy

- Notable Event Aggregation is helpful especially for complex alerting such as:
  - Only sending an email after 3 concurrent alerts of the same type
  - Applying the same alerting rule to multiple Multi KPI Alerts
  - Sending notifications when the Multi KPI has stopped alerting
- Notable Event Aggregation allows you to take different actions
  - Send an email
  - Submit a Remedy ticket
  - Run a script to recover

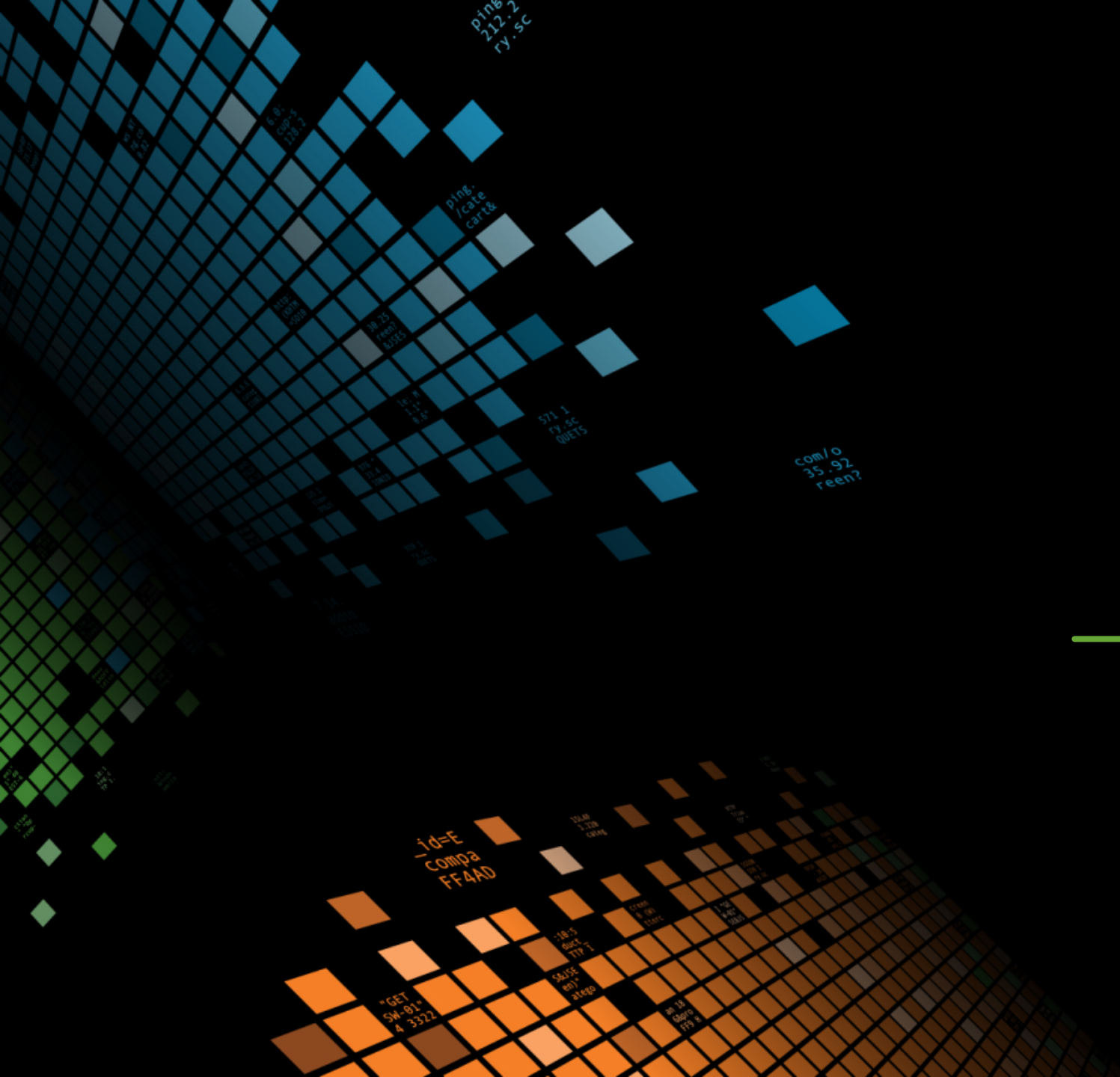
splunk> .conf2017

© 2017 SPLUNK INC.

Key Takeaways

1. Aim for transparency and eliminate the silos.
2. Embrace the Service concept.
3. Every metric is NOT a KPI.
4. Use naming conventions.
5. Aggregation matters!
6. Don’t be afraid to experiment.

© 2017 SPLUNK INC.



Q&A

Mike Scully

Joe Trimmings

splunk> .conf2017

© 2017 SPLUNK INC.

Thank You

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

© 2017 SPLUNK INC.

Want to Learn More About ITSI at .conf2017?

Tuesday September 26th, 2017

- **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
- **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, 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

Wednesday September 27th, 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, 201711:00 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 Room147AB
- **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 28th, 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

splunk> .conf2017