

splunk® **.conf2017**

# Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring

Using Splunk IT Service Intelligence

Michael Hurley | Sr. Architect

Patrick Farrell | Sr. Engineer

September 27, 2017 | Washington, DC

September 2017 | Washington, DC

# 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.

# Introduction

---

To Cardinal Health and the speakers



# Michael Hurley

- ▶ Splunk Ninja
- ▶ Splunk Solution Architect and Solution Owner at Cardinal Health
- ▶ Focused on integration, monitoring and automation
- ▶ Favorite Splunk tagline: More brain, less surgery



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1



# The Challenge

Pharmaceutical Modernization

# Pharmaceutical Modernization

- ▶ Multi-year investment in the future of Cardinal Health
- ▶ Aligning people, processes and technology
- ▶ Enabling us to continue to be a leader in healthcare
- ▶ Replacing multiple critical independent systems: Accounting/Financial, Warehouse Management and the ParMed Order Management application
- ▶ Monitoring and traceability is a key requirement

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D185L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
137.27.160.0 - - [07/Jan 18:10:56:189] "GET /category.screen?category\_id=SURPRISE&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1  
137.27.160.0 - - [07/Jan 18:10:56:189] "GET /category.screen?category\_id=SURPRISE&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.1





“Correlating business transactions across multiple independent systems is **challenging.**”

---

Patrick Farrell

# Business Sponsor

## Backing and buy-in

### Desire

- ▶ Ability to provide a current state view of the entire business process

### Considerations

- ▶ Capability
- ▶ Cost

### Buy-in achieved based on

- ▶ Speed-to-market
- ▶ Business process visualization
- ▶ Support for Agile methodology

# How Do We Approach The Problem?

- ▶ Gather the transactions
- ▶ Connect the dots
- ▶ Tell the story



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CW-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)"  
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)"  
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)"
```

# Which Options Did We Consider?

For end-to-end business process monitoring

## ► Custom solution using a database

- High license cost ❌
- Long time-to-market ❌
- Fixed database schema ❌
- Lack of alerting capability ❌

### Bottom line:

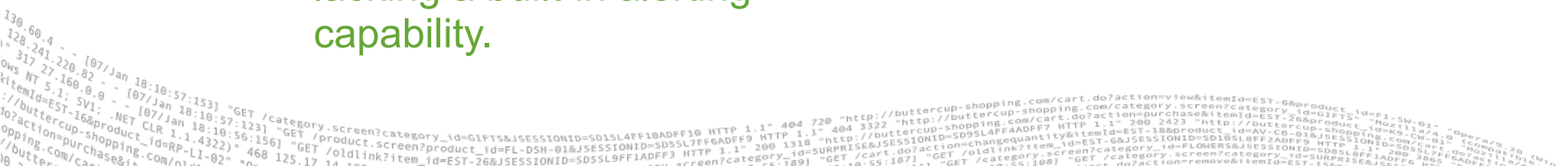
We did not want to build a custom solution based on a fixed database schema or lacking a built-in alerting capability.

## ► Splunk Enterprise

- High development cost ❌
- Long time-to-market ❌
- Schema-on-read ✓
- Alerting ✓

### Bottom line:

We liked the features provided by Splunk Enterprise but needed faster speed to market.



# The Solution



Splunk IT Service  
Intelligence™

# Why Splunk and ITSI?



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&SESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-03" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CW-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
131.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&SESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-5W-03" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=KQ-CW-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
131.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14





# What Was Built

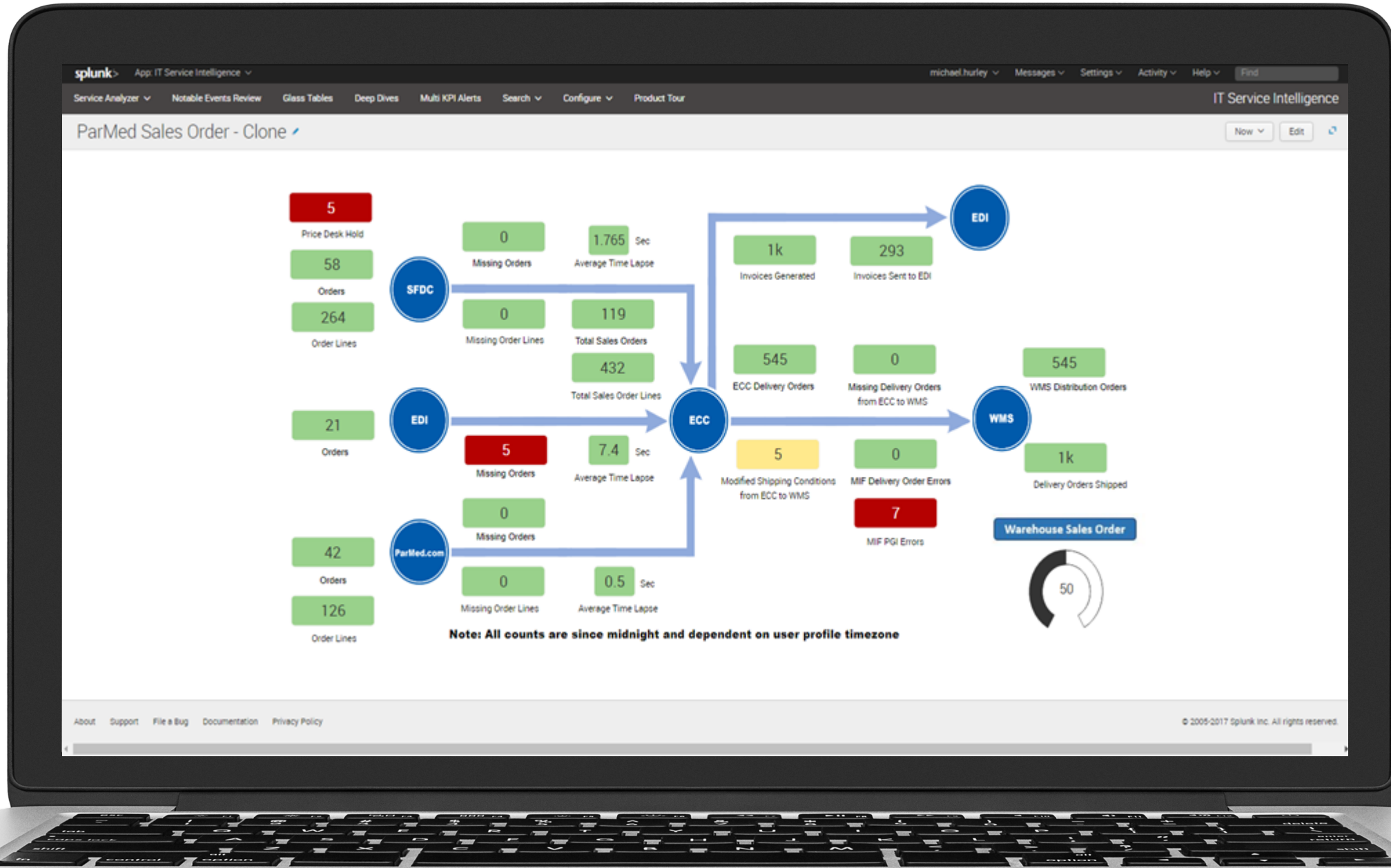
---

Features

# Services & KPIs



# Glass Tables



# Business End User Monitoring

## End-to-end transactional event correlation

- ▶ One view of the entire business process

## Drill down

- ▶ With one click business users have the ability to drill down into a sub business process or see details for a specific business object

## Machine learning

- ▶ Able to clearly see when things are not normal

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.189 "GET /category.screen?category_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0" 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.1.189 "GET /category.screen?category_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0"
```

# How Was It Built

---

Implementation

# Building the Team

Within a short time span

## Splunk skills

- ▶ Splunk ITSI
- ▶ Splunk SPL and Knowledge Objects
- ▶ Splunk Administration

## Other skills

- ▶ Project Management
- ▶ Solution Architecture
- ▶ Business Analysis
- ▶ End Point Application SMEs

“Hiring Splunk Certified Ninjas will have a significant impact on success of your ITSI Project”

“**Agile** software development methodologies work well with Splunk ITSI.”

---

Michael Hurley

# Establishing Governance

## When and how to use ITSI

It was essential to establish use cases for Splunk ITSI

- ▶ Too many competing technologies

Defending when to use ITSI was a constant battle since expectations had already been set

“Providing Architectural Guidelines to the BA’s in the very beginning would have helped significantly”

## Key considerations

- ▶ ITSI is used as a visual means to show transactional correlation across a business process
- ▶ Business users should be given the ability to see correlations in sub processes and see the data that is traveling through each process
- ▶ For this project application monitoring is outside the scope
- ▶ Also not in scope is using ITSI for any long term analysis



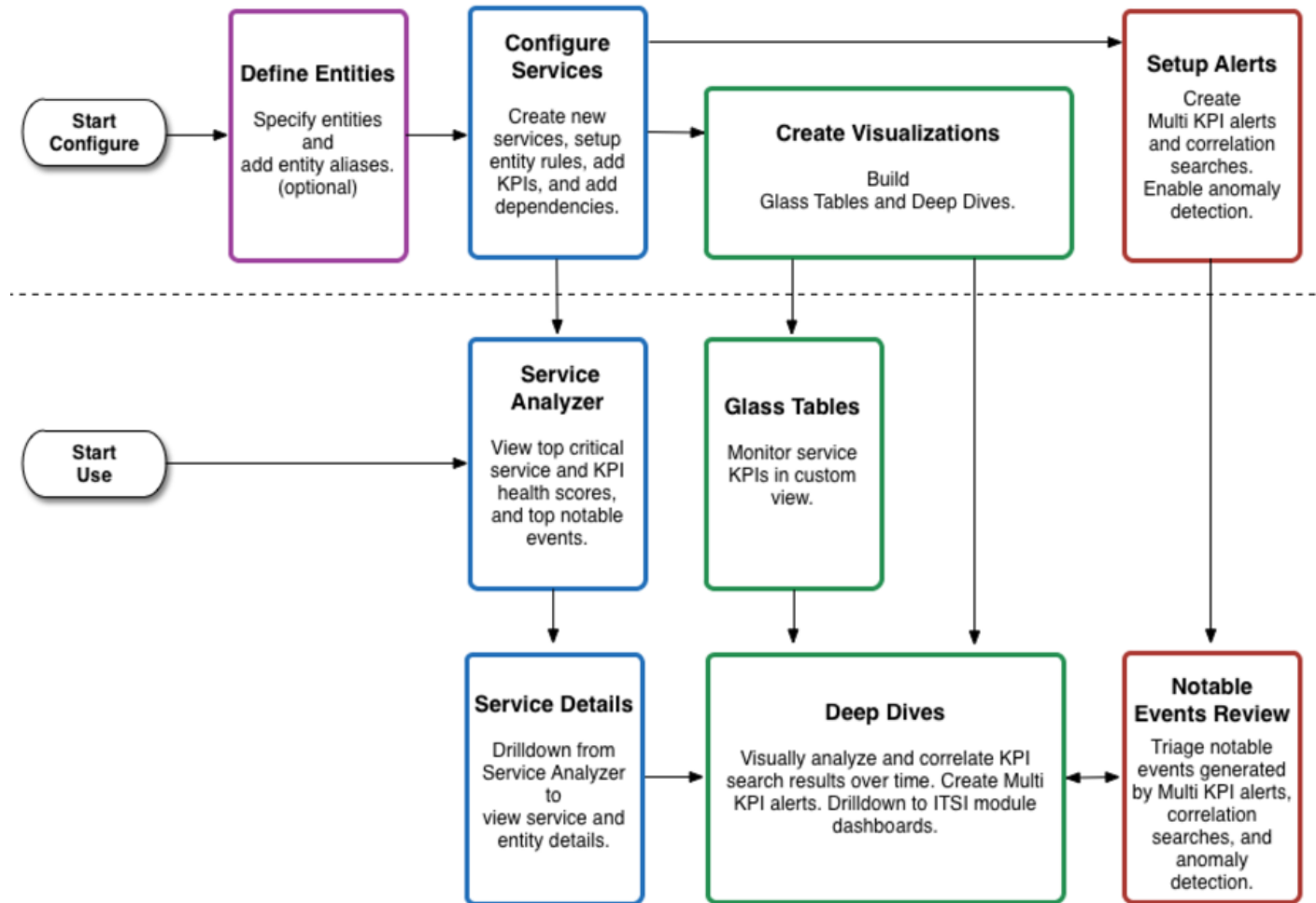




# Telling The Story

With Splunk ITSI

- ▶ Define entities (Optional)
- ▶ Configure services
- ▶ Add KPIs
- ▶ Create visualizations
- ▶ Setup alerts



# Service and KPI Implementation

**Services** are logical groupings of IT objects that align with your business goals, such as a group of applications or a business service, containing one or more Key Performance Indicators (KPIs).

**Key Performance Indicators (KPIs)** are recurring saved searches that return the value of an IT performance metric, such as response time, that can be used to monitor service health.

“Writing the SPL queries to build KPIs consumed about 90% of our development time”



# Glass Table Exercise

One day event where Splunk engineers describe the process of building an ITSI solution and walk you through the build out of a glass table

*Extremely helpful and highly recommended before starting work on any ITSI solution*

Splunk will provide more detailed information about the Glass Table Exercise (GTE) later on during this session...



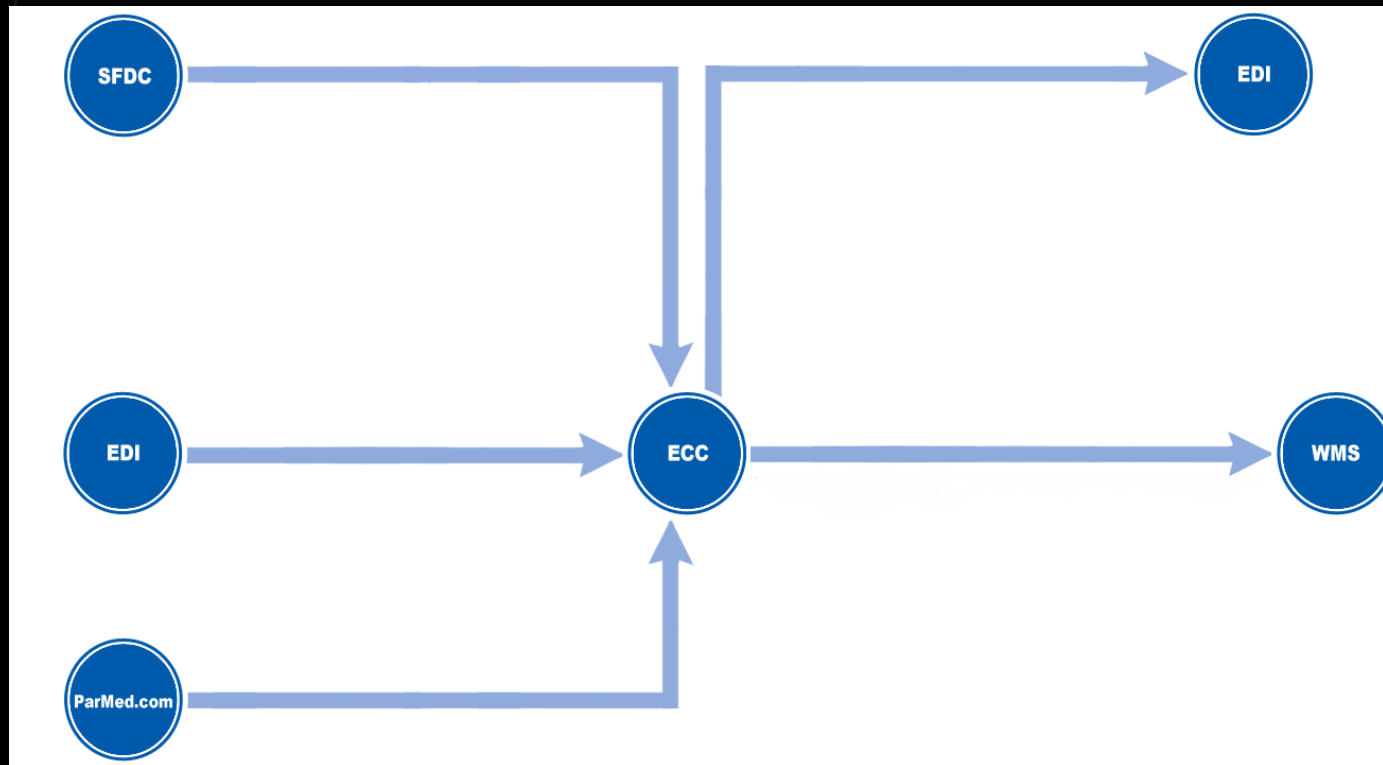
# Glass Table

## Design layout

### Process:

1. Identify the systems that make up a business process and how data flows between them
2. Create a diagram
3. Convert to PNG
4. Import

It is that simple











# splunk>enterprise

<input type="text" value="Username"/>	<input type="password" value="Password"/>	<input type="button" value="Sign in"/>
---------------------------------------	---	--

You have been logged out. Log in to return to the system.

# ITSI Success Stories

- ▶ Early identification of business logic defects in monitored applications through KPI analysis reduced costs compared to identification of the same defect in production.
- ▶ Early discovery of business transaction and process failures prevented service disruption resulting in a better customer experience.
- ▶ Educating senior leadership about our solution sparked new ideas that ultimately led to the discovery of new Splunk use cases.
- ▶ Strong user adoption including 100+ business users and 30+ IT analysts.
- ▶ Interest in Splunk is at an all-time high.

# Key Takeaways

for your next  
ITSI project

- ▶ Define use cases and provide architectural guidelines before gathering requirements
- ▶ Participate in the Glass Table Exercise provided by Splunk before beginning an ITSI project
- ▶ Hire Splunk Certified Ninjas whenever possible to reduce risk when faced with short deadlines
- ▶ Use agile methodology when building out solutions based on Splunk Enterprise or Splunk ITSI

# Thank You

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

splunk> .conf2017

# Want to Learn More About ITSI at .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 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  
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