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
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.
Agenda

- Micron Technology
- Path to ITSI
- ITSI @ Micron
- None to Done
- Lessons Learned
- Advanced ITSI Topics
- Q&A
What Does Manufacturing IT Do For Micron?

- Product Tracking
- Equipment Tracking
- Equipment Integration
- Automated Material Handling
- System Integration
- Engineering Analysis Software
Path to ITSI

It’s a journey, not a destination
Gopher Effect
How we knew we were having a Major Incident prior to Splunk
Transactions are failing!

Seeing high CPU on servers!

Seeing some blocking on xxx database!

No alerts from any of the switches!

Apps
Sys Admin
DBA
Network
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
Enter Stage Left: Splunk!
Our Objective in Introducing Splunk to Micron
Result: IT Operations App

After 6 months of intense work
INTRODUCING Splunk IT Service Intelligence™
ITSI @ Micron

Current State
Our Current ITSI Stats

- Services Defined: 89
- KPI’s Defined: 745
- KPI’s w/ anomaly detection: 78
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
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

ITIL
None to Done

Are you ever completely done?
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
How Do You Get All Your Services Defined?

- SME's Together
- Business
- Services
- App1
- App2
- Server
- Database
- Network
- In Parallel
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
KPI vs Metrics

All KPI’s are Metrics, but not all Metrics are KPI’s
Lessons Learned
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
KPI Aggregation
How you aggregate the KPI matters
Deep Dive Aggregation
These are the same metric just different time range

Last 4 Hours

Last 24 Hours

Where did my alert go?!?
Deep Dive Aggregation
There’s my alert!

Last 24 Hours w/ Average Aggregation

Use Max for KPI’s where you have upper thresholds
Use Min for KPI’s where you have lower thresholds
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.
Advanced ITSI Topics

Satisfy your inner Splunk ninja
What is ITSI doing in the background?

### CPU: Max % User Time

#### KPI description

| Source | Search: source=cpu cpu=all  
| Threshold field: PercentUserTime |

| Entities | Entity Split by field: host  
| Data filtered by service entities in field: host  
| Service matches entities on fields: title |

| Calculation | Calculating Maximum per entity, Maximum of aggregate over the last 5 minute(s) every 5 minute(s) |

| Unit | Unit: % |

#### Thresholding

#### Anomaly Detection
Daily Reports
What’s bubbling under the surface?

▶ 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.

<table>
<thead>
<tr>
<th>Service</th>
<th>KPI</th>
<th>% Critical</th>
<th>% High</th>
<th>% Medium</th>
<th>% Low</th>
<th>% Normal</th>
<th>% Info</th>
<th>% Unknown</th>
<th>Case Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: server1</td>
<td>Window Error Log Count</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>Yes</td>
</tr>
<tr>
<td>App: application1</td>
<td>App Memory %</td>
<td>0.00</td>
<td>85.76</td>
<td>0.00</td>
<td>0.00</td>
<td>14.24</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Service: service1</td>
<td>Very Important KPI</td>
<td>0.00</td>
<td>0.00</td>
<td>77.64</td>
<td>0.00</td>
<td>22.36</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>DB: database1</td>
<td>Batch Requests/sec</td>
<td>0.35</td>
<td>14.58</td>
<td>0.00</td>
<td>0.00</td>
<td>83.07</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Service: service2</td>
<td>Receive Queries</td>
<td>4.17</td>
<td>2.78</td>
<td>0.00</td>
<td>0.00</td>
<td>93.06</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>DB: database2</td>
<td>Batch Requests/sec</td>
<td>3.82</td>
<td>2.08</td>
<td>0.00</td>
<td>0.00</td>
<td>94.10</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Server: server2</td>
<td>CPU: Max % User Time</td>
<td>4.17</td>
<td>0.69</td>
<td>0.00</td>
<td>0.00</td>
<td>95.14</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Server: server3</td>
<td>Window Error Log Count</td>
<td>4.51</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>95.49</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>DB: database3</td>
<td>User Connection Count</td>
<td>0.00</td>
<td>5.56</td>
<td>0.00</td>
<td>0.00</td>
<td>94.44</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>DB: database2</td>
<td>Buffer Cache Hit Ratio</td>
<td>3.83</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>96.17</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Server: server4</td>
<td>Window Error Log Count</td>
<td>3.47</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>96.53</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>DB: database5</td>
<td>Max Connection Count</td>
<td>0.69</td>
<td>3.47</td>
<td>0.00</td>
<td>0.00</td>
<td>95.83</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>DB: database5</td>
<td>Processes Blocked Count</td>
<td>3.14</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>96.86</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Server: server5</td>
<td>System Uptime</td>
<td>3.13</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>96.88</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
<tr>
<td>Server: server5</td>
<td>System Uptime</td>
<td>3.13</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>96.88</td>
<td>0.00</td>
<td>0.00</td>
<td>No</td>
</tr>
</tbody>
</table>
Anomaly Detection on # of ITSI Threshold Breaches
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
Entity Definition

DNS Dump

ServiceSeed.csv

ITSI-Service.sh

ITSIDef.csv

ITSI Search Head
Alerting
Creating the Multi KPI Alert
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
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.
Q&A

Mike Scully
Joe Trimmings
Thank You

Don't forget to rate this session in the .conf2017 mobile app
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, 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 Room 147AB
- **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 Room 143ABC
- **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, 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, 2017 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, 2017 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