ITO1121B – Big Ships Turn Slowly

Getting to the 'True' when moving away from BMC TrueSight. A realistic approach to transformation in the real world of IT.

Mike McGrail
Sr. Infrastructure Specialist | Canada Life
During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk®, Data-to-Everything, D2E and Turn Data Into Doing 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. © 2020 Splunk Inc. All rights reserved.
Mike McGrail

Sr. Infrastructure Specialist  |  Canada Life

Toronto 8 yrs. monitoring @ global 500s
Fav. > T: “Log, I am your father”
1) Background

2) Why Splunk ITSI?

3) Tech Deets

4) Where Are We Now?

5) Where Are We Headed?
Background

Manager of managers

• Deduplication
  – One event for matching alerts
  – Reactive, not predictive

• Correlation
  – “Good” closes event for “Bad”
  – Stateful @ specific moment

• Maintenance Window
  – Close events during planned down time
  – Groups get emails from their systems
Background
TrueSight events

Line by line
Background

IT Silos...|n|o| v|i|s|i|b|i|l|i|t|y|

Service Desk
User-reported

NOC
System-reported

IT Ops
Server Network Storage Virtualization

App. Support
Self-monitoring

Leadership
What’s Happening?

≡ Outage  🔴 Everyone Join War Room!
Why Splunk ITSI?

AIOps

Small Pre-Existing Environment
- Some users & data
- New use case ► infrastructure monitoring

POC Numerous AIOps Vendors
- Point solutions
- “TrueSight 2.0” ► same thing, new tool

ITSI
- Service analyzer ► green/yellow/red
- Glass tables
- Drill-down to Splunk viz.
Tech Deets

Environment

• Data globally visible when sensible
• Intermediate HF masking as necessary
• Summary indexes
  – Consolidated retention
  – Expose non-sensitive data subset
## How Much Data?

<table>
<thead>
<tr>
<th>Interval = 60 Seconds</th>
<th>Windows TA Metrics</th>
<th>Linux collectd Metrics</th>
<th>AIX *nix TA Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS performance</td>
<td>52 mb</td>
<td>87 mb</td>
<td>42 mb</td>
</tr>
<tr>
<td>Services</td>
<td>7.5 mb</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Controller</td>
<td>1.2 gb</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **DBX for Remedy CMDB Data**
  - Asset details
  - Installed software
- **SolarWinds**
  - TA for nodes -> entities
  - HEC for alerts -> episodes

---

© 2020 SPLUNK INC.
Technical Debt Ahead

Lift and Shift TrueSight -> Splunk (fast)
No investment from other teams (non-invasive)
Lift & shift – search based

**Tech Deets**

<table>
<thead>
<tr>
<th>Lookups</th>
<th>Enrich data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core Splunk Search</strong></td>
<td>Output to custom summary index</td>
</tr>
<tr>
<td><strong>Correlation Search</strong></td>
<td>Query custom summary index, create episode</td>
</tr>
<tr>
<td><strong>NEAP</strong></td>
<td>Send alert to team</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ts_kpi</th>
<th>ts_entity</th>
<th>ts_instance</th>
<th>ts_support_team</th>
<th>ts_alert</th>
<th>ts_ticket</th>
<th>KBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>prod</td>
<td>splunk_health</td>
<td>Splunk Ninjas</td>
<td>1</td>
<td>0</td>
<td>KB12345</td>
<td></td>
</tr>
<tr>
<td>prod</td>
<td>logstats_free_percent</td>
<td>Redmond</td>
<td>1</td>
<td>0</td>
<td>KB45678</td>
<td></td>
</tr>
<tr>
<td>prod</td>
<td>filesystem_used_percent</td>
<td>Bell Labs</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prod</td>
<td>security_violation</td>
<td>Whoever Handles Active Directory</td>
<td>1</td>
<td>0</td>
<td>Nobody Knows</td>
<td></td>
</tr>
<tr>
<td>non_prod</td>
<td>swap_used_percent</td>
<td>Tux Penguins</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>non_prod</td>
<td>system_uptime</td>
<td>Bell Labs</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
sourceindex=ts
index=os sourcetype=cpu sourcetype=cpu cpu_instance=all
| fields cpu_load_percent host
| eval ts_instance="total_cpu",ts_kpi="cpu_utilization"
| stats avg(cpu_load_percent) as cpu_utilization
| latest(_time) as _time by ts_instance host ts_kpi
| where cpu_utilization>=95
| `ts_enrich_alert_details(host,ts_instance,ts_kpi)`
| eval sec_grp = "default_itsi_security_group",
| ts_alert_value=cpu_utilization,
| ts_alert_unit="percent",
| ts_alert_level=4
| `match_entities(host, sec_grp)`
```
Tech Deets

ITSI episodes

Lifted & shifted
Where Are We Now?

- All episodes & alerting through ITSI
- Decom. Patrol & TrueSight
Where Are We Headed?

Turn the ship

+ Services & KPIs
  Visibility end silos

- Core Searches
  complexity contextless alerts

+ AIOps
  adaptive thresholds smart mode data-driven decisions
Image Credits

  https://pilotfire.com/first-post-in-turning-a-big-ship-there%E2%80%99s-hope-
  for-us/.
- U2. “I Still Haven’t Found What I’m Looking For.” The Joshua Tree. Island
- Blue Swede. “Hooked on a Feeling.” Hooked on a Feeling. EMI Records,
  1974.
- Eminem. “Cleanin’ Out My Closet.” The Eminem Show. Interscope Records,
  2002.
Thank You

Please provide feedback via the SESSION SURVEY