Splunk App Lifecycle Management
Take control of your apps in the Cloud!

Cecelia Redding  |  Senior Software Engineer
Blaine Wastell  |  Area Product Owner

September 26, 2017  |  Washington, DC
The Road to Splunk ITSI

Donald Mahler | Director - Performance Engineering and Systems Monitoring
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.
Who We Are

- Leidos is a FORTUNE 500® global science and technology solutions leader working to solve the world’s toughest challenges in the defense, intelligence, homeland security, civil, and health markets.
- Government and commercial customers
- 32,000 employees in over 30 countries worldwide
- Founded as SAIC in 1969, changed its name to Leidos in 2013. Headquartered in Reston, Virginia.

Leidos Executive Leadership Team
Who am I?

Manager of Performance Management/monitoring at Leidos, a science and technology solutions leader, based in Reston, Va.

- internal Leidos IT include business service management (BSM), server/cloud monitoring, application performance, and common security/network/application logging.

Career in systems/network management across many platforms and OS’s; presented at numerous conferences and seminars on technology and solutions

- Splunk .conf(s), GovSummit(s) and SplunkLive sessions
- Aprisma Spectrum user conference (keynote), Solarwinds GovSummit
- Netiq’s Netconnect, Novell’s BrainShare, Managed Object’s user conference, Planet Tivoli
Overview of our Splunk environment and story

Problem Statement: Alert manager of managers (MOM)

Overview of ITSI and how we use it

Strengths, areas for improvement, and other topics
Management and Monitoring Services

Operational Intelligence

- Situational Awareness
- Performance and Capacity Reporting
- Common Logging and Analysis
- Service Delivery Reporting

Business Service Management

- Network Management
- Server Management
- Infrastructure Management
- Application Management and Synthetics

Common Logging
Our Splunk journey

► Pre 2010
  • Syslog servers - Grep and spit

► 2010 – Splunk 10GB
  • Routers, switches

► 2012 – Splunk 400GB
  • Routers, switches, Firewalls, Servers

► 2013-2014 - bump to 700GB , then split
  • More servers, more networking gear , more applications

► 2015 - the 1TB club (no tshirt)
  • NIST

► 2017 - the 2TB club (still no tshirt)
  • Merger – and more NIST
Splunk Overall Design

Inputs and sources
- Windows/Linux servers (via Universal Forwarders)
- Network Devices/ Appliances (syslog)

Forwarding
- F5 Load balancers
- Splunk Heavy Forwarders

Indexing
- Splunk Indexers (xx)
- 2TB/day

SearchHeads
- Infrastructure SHC (4)
- Security SHC (4)
- ITSI SH
- Scripted Inputs SH
The Problem

- Needed to retire manager of manager Tivoli TEC (unsupported, Windows 2003) by July, or pay a big financial penalty $$
  - Plan: replace this MOM function with ITSI notable events
- Time crunch – we had a window of time before company IT merge in mid summer 2017.
- Schedule:
  1. ITSI Phase 1 - Replace TEC by May 2017 - alert manager of managers (MOM)
  2. Company IT merge Aug 2017
  3. ITSI Phase 2 - Glass tables replace BSM (service GUI, SLA calculations) in 4Q17
Monitoring products (previous)

- All MLM’s send to TEC via telltec
- BSM has TEC adapter
- TEC provides MOM (alert list, dedup, dispatch, automation)
- BSM provides situational awareness, SLA availability measurements

Business Service Management
(Netiq Operations Center transitioning to Splunk ITSI)

MOM: TEC - Tivoli Enterprise console (win2003!!)

EMGTweb

Splunk

NPM
Cisco LiveAction
HP NA
Vcops/ vCenter
onCommand
Backups (TSM)

OEM
Splunk Windows
ipMonitor
Altiris
WPM
F5
Appmanager AD/EXCH/Lync
Backups (netbackup/Druva)
ChangeAuditor
TripWire
Other sources

Network Management
Server Management
Synthetics

©2013 LEIDOS. ALL RIGHTS RESERVED.
Replace TEC w ITSI (phase 1)

- All MLM’s send to Splunk via emgt “MLM” sourcetype
- ITSI provides MOM (alert list, dedup, dispatch, automation)
- BSM provides situational awareness, SLA availability measurement

Business Service Management
(Netiq Operations Center transitioning to Splunk ITSI)

MOM: ITSI Notable events

Network Management

Server Management

Synthetics

NPM
Cisco LiveAction
HP NA
Cisco LiveAction
Vcops/vCenter
onCommand
SCCM
Backups (TSM)

OEM
Nagios
Splunk UA
Altiris
Appmanager AD/EXCH/Lync
Backups (netbackup/Druva)
HPSim

ipMonitor
WPM
F5
ChangeAuditor
TripWire
Other sources

©2013 LEIDOS. ALL RIGHTS RESERVED.
Requirements of an Event Manager

- Receive events, with rich attributes
  - Location, CMDB system, Environment
- Deduplicate
- Close down with up
  - Note: Routers down for days need to still be shown…
- Self directed event handling
  - Autoescalate
  - Close in xx minutes
  - Openticket
- Automation
  - Notifications:
    - Automated ticketing, emails, SMS
  - Suppressions
    - manual, RFC, TOD
- Absolutely solid – no lost events or correlations
- Refreshable – persistent state
- Logging – event traceability
  - show the lifecycle of an event.
  - defend what the alert handling is doing, including user actions and automated scripts
New solution is ITSI – Splunk’s operational awareness flagship
- Built atop Splunk framework
- Workflow, rules, KPI

Key components
- Notable Events
  - Actionable events display
- Service Analyzer
- Glass tables
  - Like BSM
- Deep dives
  - Metrics in swim lanes
ITSI – a short primer (terms and concepts)

Alert flow

- Alerts posted via correlation searches or HTTP Event Collector (HEC)
- Data flows index itsi_tracked_alerts
- Goes thru rules engine
- Then posted into itsi_grouped_alerts
- Kvstores used for
  - State, Comments, tickets, groupings

Concepts

- Base attributes and user-define attributes
- Event groups used to handle correlation and deduplications
- A clear “breaks” the group
- ITSI objects available to Splunk SPL and Dashboards (this is good)
  - `itsi_event_management_group_index` | lookup itsi_notable_event_group_lookup_key AS itsi_group_id OUTPUT severity AS lookup_severity, status AS lookup_status, owner AS lookup_owner
Alert Logic and flow design – decision

Distributed/flow to ITSI

- Decisions and thresholds distributed down to mid-level managers
- When threshold exceeded, flow alert to ITSI
- Compute load distributed

Centralize in ITSI

- All logic done at the top of the stack
- Splunk has the raw data anyways
- Apply better thresholds, even learned ones, using the same techniques
- More consistent alerts flow into Notable Events
- Alert searches on same server as alert manager

Example: NPM polls router and sends high UTIL alert when uplink >95%. Send alert via HEC to ITSI

Example: Splunk collects NPM perf data via Dbconnect. Correlation search watches for router uplink util >95%. Generates notable event to ITSI.
Event flow (before)

- Mid level managers send events to TEC server.
- Hub augments events, and posts to Tivoli.
- Tivoli drives tecweb displays and notifications.

Network, server, application mid level managers, sending in alerts.
1. All monitors send events as before.
2. EMGThub gathers and augments the events. Adds CMDB attributes
3. ITSI triggers on events coming in via Http event collector (HEC)
4. ITSI notable event aggregation policies assign the events to groups
5. Python apps using the SDK pass information on to the legacy BSM system

Network, server, application mid level managers, sending in alerts as before
ITSI and EMGT in 7 easy steps
What we need the rules to do

### Basics

- **Dispatch**
  - Critical/Minor event comes in – run script and add to comments
- **Event changes state**
  - Event acked/closed – log this, with all event details
- **Good closes bad**
  - Normal event comes in, closes any critical/high events – run script and add to comments
- **Duplicates**
  - Matching event comes in, count it as a duplicate. Do not run scripts – this applies to duplicates of critical, high and even normal

### Escalations and Timed

- **Escalation**
  - Critical event comes in, close any matching normal or high, and post the critical (and see #1)
- **Timed events - autoflags field**
  - **Closeinx**
    - autoflags contains closein5 – close the event if the event is still not closed after 5 minutes
  - **Autoescx**
    - autoflags contains autoesc5 – escalate the event from high to critical if the event is still not closed after 5 minutes
Rules Engine - incoming - actions

- If the group is broken, then change status to Resolved on all events in this group, and perform the selected action on all events in this group.
  - The group is broken
  - and if

- If a specific event occurs, then perform the selected action on all events in this group, and change severity to Critical on all events in this group, and perform the selected action on events specified by the execution.
  - the following event occurs
  - status matches New
  - severity matches Critical
  - Add Rule (AND)
<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>Age</th>
<th>Device</th>
<th>Ticket</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/23/17</td>
<td>00:19</td>
<td></td>
<td>LEDOSNET</td>
<td></td>
</tr>
<tr>
<td>08/23/17</td>
<td>00:19</td>
<td></td>
<td>LEDOSNET</td>
<td></td>
</tr>
<tr>
<td>08/23/17</td>
<td>00:19</td>
<td></td>
<td>LEDOSNET</td>
<td></td>
</tr>
<tr>
<td>08/23/17</td>
<td>00:19</td>
<td></td>
<td>LEDOSNET</td>
<td></td>
</tr>
<tr>
<td>08/23/17</td>
<td>00:18</td>
<td></td>
<td>LEDOSNET</td>
<td></td>
</tr>
</tbody>
</table>

**The old TECweb interface**

- **Concis Time**
- **Severity and status**
- **Age**
- **Device**
- **Ticket**
- **All tools**
- **Repeat count**
- **Suppression in pink**
Embrace the use of "title".

Open and critical

Search only 24 hours for speed reasons. Replay old events.

Filter by any field

ITSM integration

Pending=Suppressed

ITSI Notable Events interface
ITSI Views Of Alerts

- Separate views for separate operational teams
  - OSC
  - NOC

- Types of alerts
  - All
  - Reachability
  - Batch job failures
  - Backup failures
Lessons And Settings Along The Way

- Event posting speed
  - We preferred HTTP Event Collector (HEC) to ITSI correlation searches
  - Tracked alerts to grouped alerts
    - [itsi_event_grouping]
    - dispatch.indexedRealtime = 1
    - dispatch.indexedRealtimeOffset = 60

- Set ITSI to not kill RT searches
  - [itsi_event_grouping] restart_on_searchpeer_add = 0

- KVstore retention settings

- Know your alerts. Be able to validate them
- One needs to log and prove everything.
- Know what the operators are doing
  - Re-animating alerts for example
- Alertutil.py was a game changer
Gather critical events
- earliest=-7d latest=now `itsigroupedopenalerts` | search * | sort itsi_first_event_time desc | table ztime event_id itsi_group_id itsi_first_event_time title device severity num status num autoflags monitoredwhen event age cmdbsys location environment incident itsi_group_count description

Process thru critical events
- Close duplicates (setstatus), Close in (setstatus), autoescprime (setstatus)
- Suppression (RFC) and unSuppression – setstatus
- Selected downgrades (setseverity)
- Apply tickets to alerts
- Replay events older than 24 hrs

Process thru Minor events w autoesc flag
- Escalate based on autosccxx min (setseverity)
As alerts are posted and resolved into ITSI, this is in interest to other IT processes

Python command triggered in rules engine when events are critical, minor or closed (broken group)

Messages arrive into EMGT, and we:
- Post to Business Service Management (BSM)
- Open tickets in ServiceNow
- Send out emails and pages to interested parties

ITSI - The Notification Engine
ITSI Health

- Health of KVStore
- Counts of alert rates and automation rates

<table>
<thead>
<tr>
<th>KVStore-State</th>
<th>KVStore-Groups</th>
<th>KVStore-Comments</th>
<th>KVStore-Tag</th>
<th>KVStore-Ticketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,984</td>
<td>248,096</td>
<td>93,735</td>
<td>172</td>
<td>0</td>
</tr>
</tbody>
</table>
ITSI - Event Disposition

- Bring together logs for alert (down/clear), notifications, tickets. (show lifecycle)
- Detailed logs on operator actions
ITSI - Debugging Clues

- HEC event posting failures (curl)
- Orphaned tracked alerts
- Rules engine issues
  - index=_internal sourcetype=itsi* source=*rule*
- Alert resurrection
  - ITSI user sets “resolved” event to “inProgress”
- Broken groups not resolved
- Monitor Response time of the notable event console
A Few Wish List Items

- **Operational reporting**
  - Provide better metrics and out of the box reports for operations staff perform (event rates, handling speed, workload management)

- **Splunk 6 dashboard-like control over the notable events console**
  - Color coding of columns and cells

- **Auto-refresh with a configurable refresh time**

- **How to close group with >100 subevents**
  - Lose the concept of groups/individual events
Thanks

- The support of Martin W and Ross L.
- We worked with us to make this product shine in our environment, and they share the credit in our success

ITSI Notable Events cutover was successful on May 26
Replace BSM (phase 2 – Sept 2017)

- All MLM’s send to Splunk via emgt mlm sourcetype
- BSM replaced by Glass tables and Deep Dives
- ITSI provides MOM (alert list, dedup, dispatch, automation)
- ITSI provides situational awareness, SLA availability measurements
Thanks

Donald Mahler
ITS Performance Engineering and Systems Monitoring
Email: donald.mahler@leidos.com

Visit us at www.leidos.com
Don't forget to rate this session in the .conf2017 mobile app
## Ready, Set, Go! Learn From Others - The First 30 Day Experiences of ITSI Customers
- **Tuesday, September 26th, 2017**
  - Room Salon C

## Splunk ITSI Overview
- **Tuesday, September 26th, 2017**
  - Room 147 AB

## PWC: End-to-End Customer Experience
- **Tuesday, September 26th, 2017**
  - 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**
  - Room 147AB

## Cardinal Health: Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring Using Splunk ITSI
- **Tuesday, September 26th, 2017**
  - Room 143ABC

## ITSI in the Wild - Why Micron Chose ITSI and Lessons Learned From Real World Experiences
- **Tuesday, September 26th, 2017**
  - 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, 2017**
  - Room Salon C

## Triggering Alerting (xMatters) and Automated Recovery Actions from ITSI
- **Wednesday, September 27th, 2017**
  - Room Salon C

## Leidos - Our Journey to ITSI
- **Wednesday, September 27th, 2017**
  - 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**
  - Room 147AB

## Here Comes the Renaissance: Digital Transformation of the IT Management Approach
- **Wednesday, September 27th, 2017**
  - Room Salon C

## The ITSI ‘Top 20’ KPI’s
- **Thursday, September 28th, 2017**
  - Room Salon C

## Automation of Event Correlation and Clustering with Machine Learning Algorithms – An ITSI Tool
- **Thursday, September 28th, 2017**
  - 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**
  - Room Ballroom B

## IT Service Intelligence for When Your Service Spans Your Mainframe and Distributed ITSI
- **Thursday, September 28th, 2017**
  - Room Salon C