splunk> .conf2017

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

splunk> .conf2017

The Road to Splunk ITSI

Donald Mahler I 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> .conf2017

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

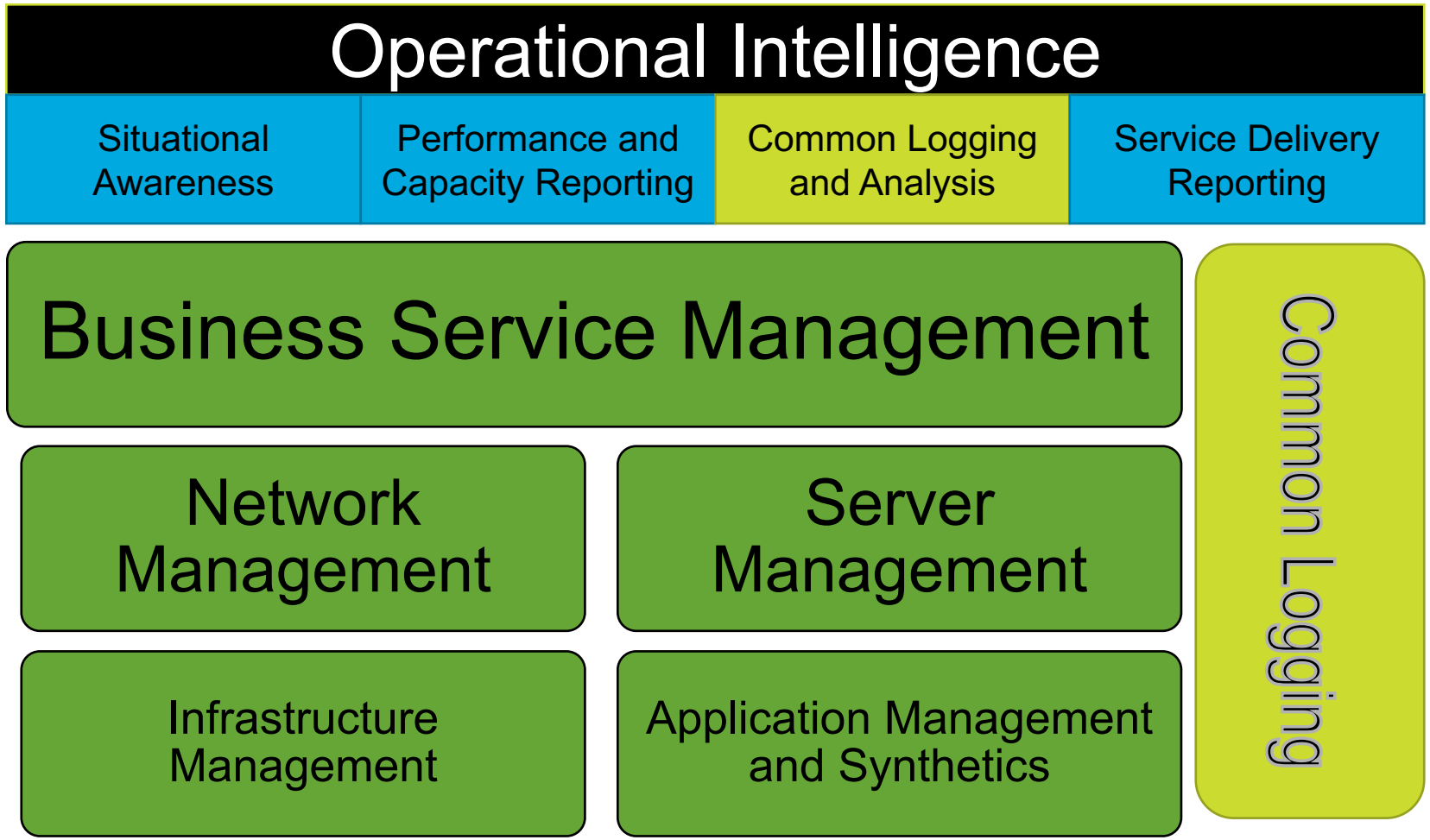
splunk> .conf2017

Agenda

- 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

splunk> .conf2017

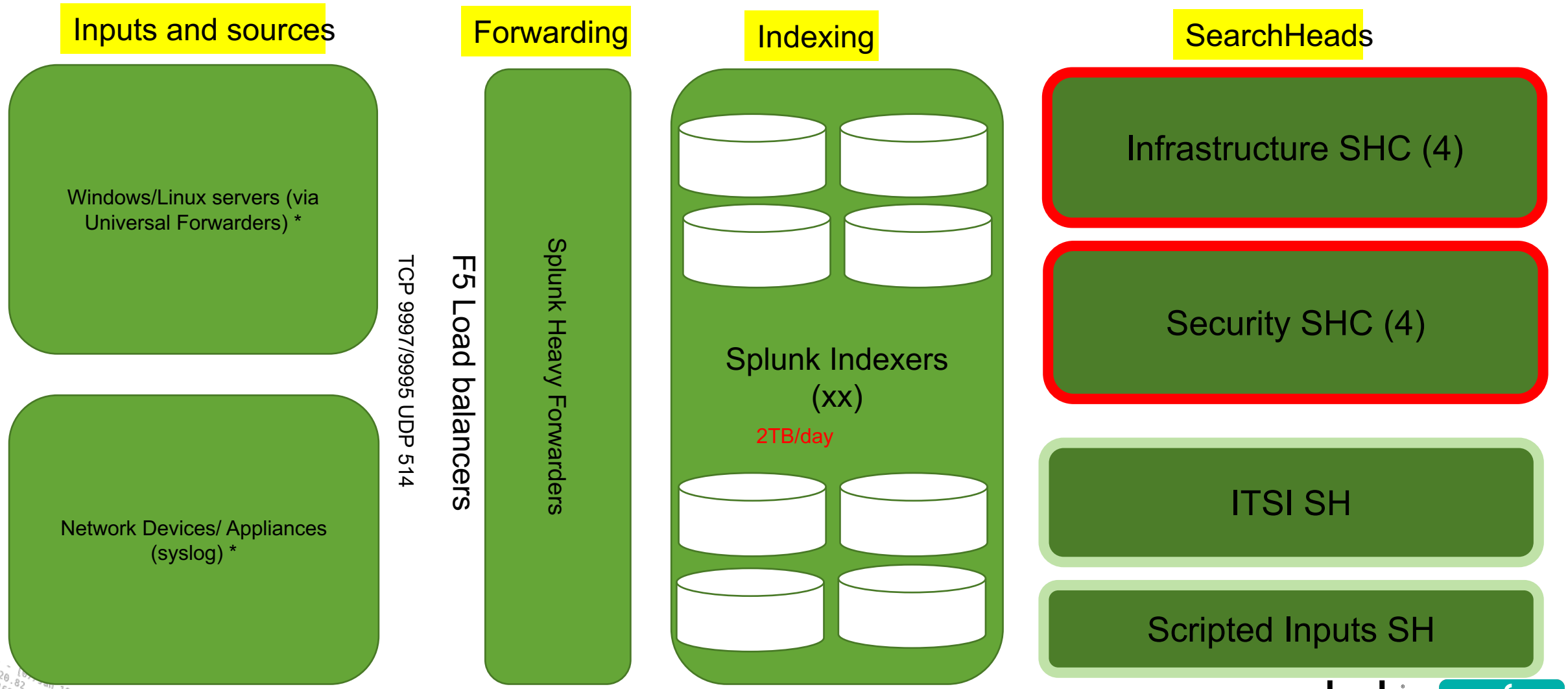
Management and Monitoring Services



Our Splunk journey

- Pre 2010
  - Syslog servers - Grep and spit
- 2010 – Splunk 10GB
  - Routers, switches
- 2012 – Splunk 400GB
  - Router, 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 Des



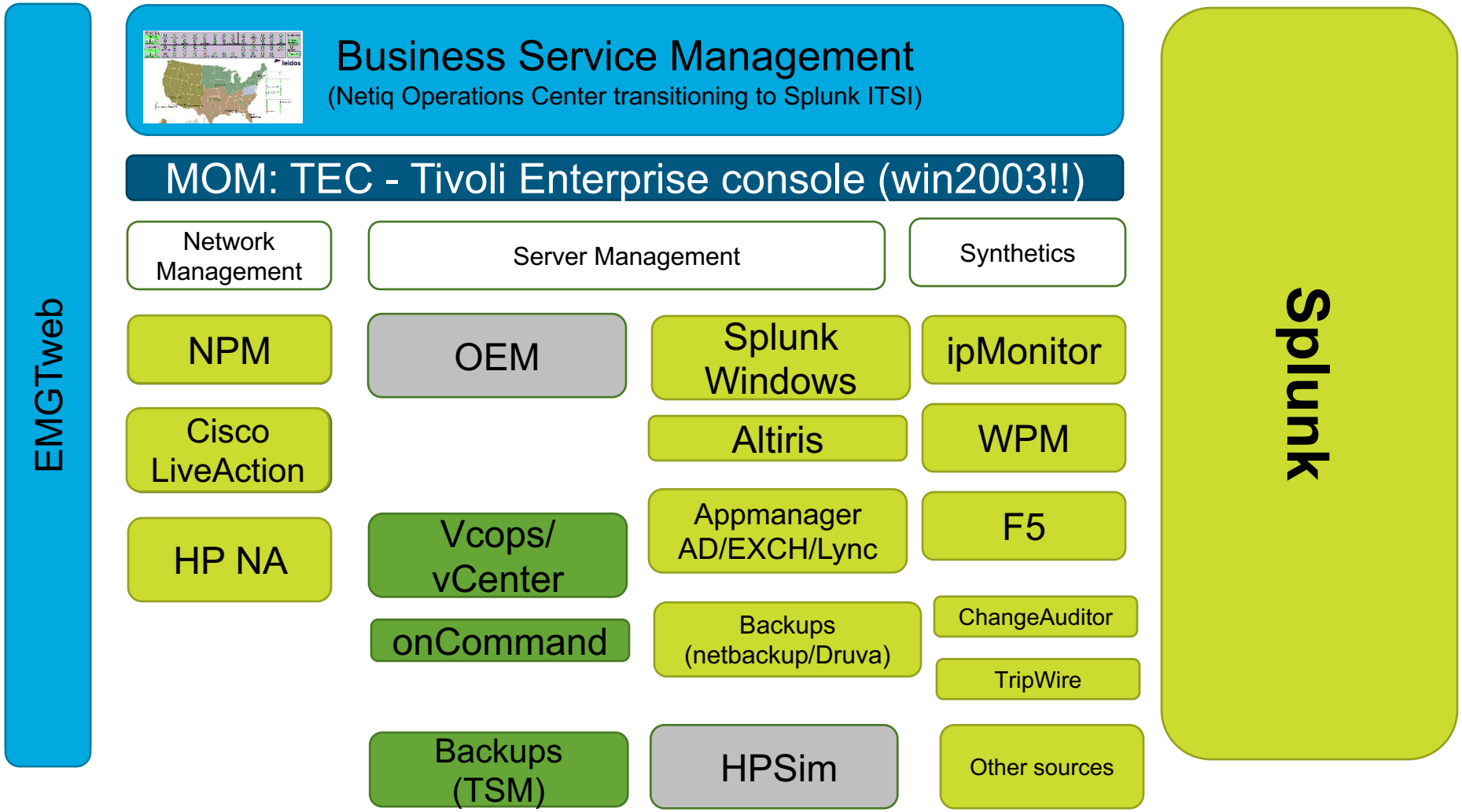
splunk> .conf2017

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

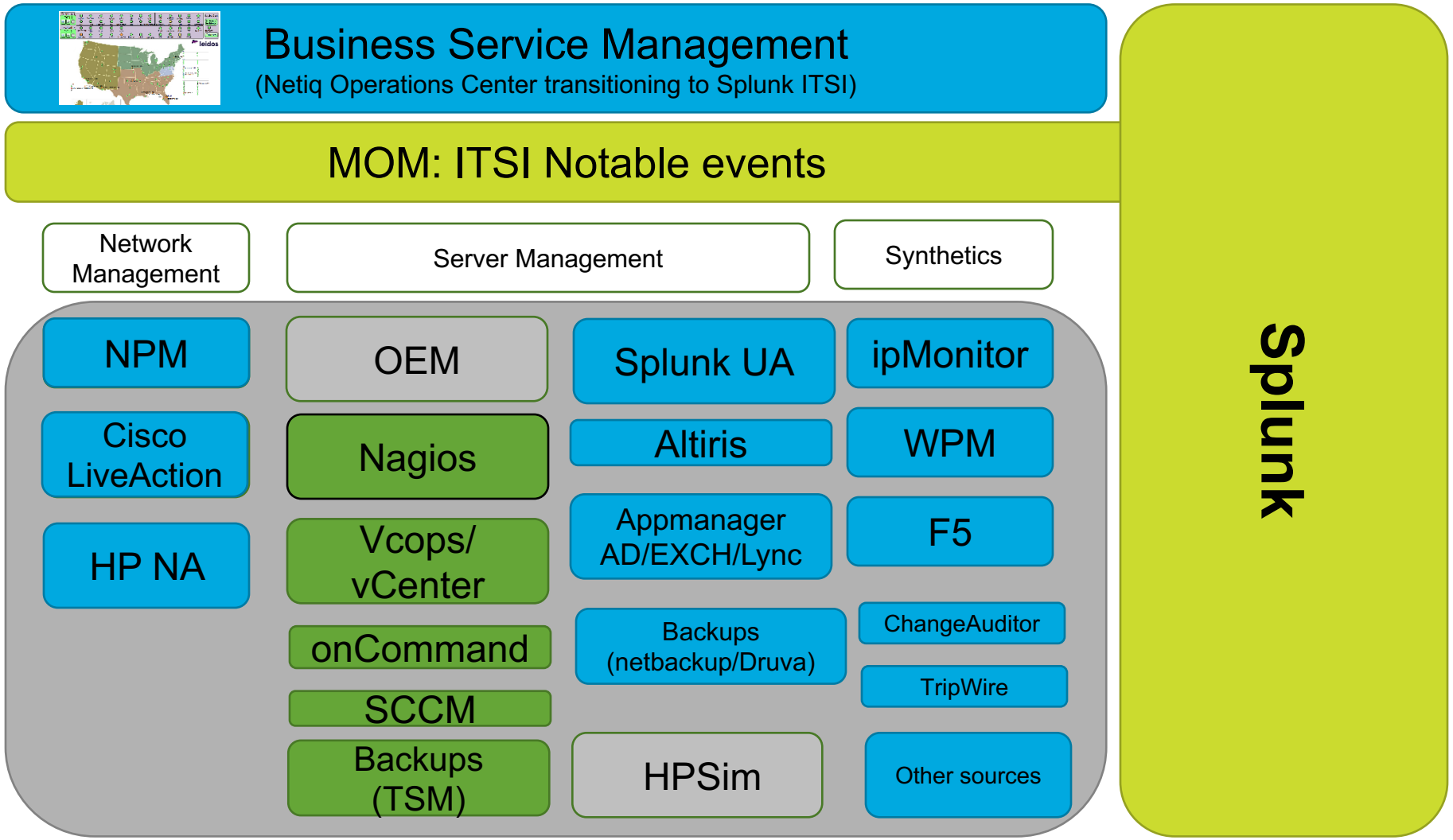
Monitoring products (previous)

- 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



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 measurements



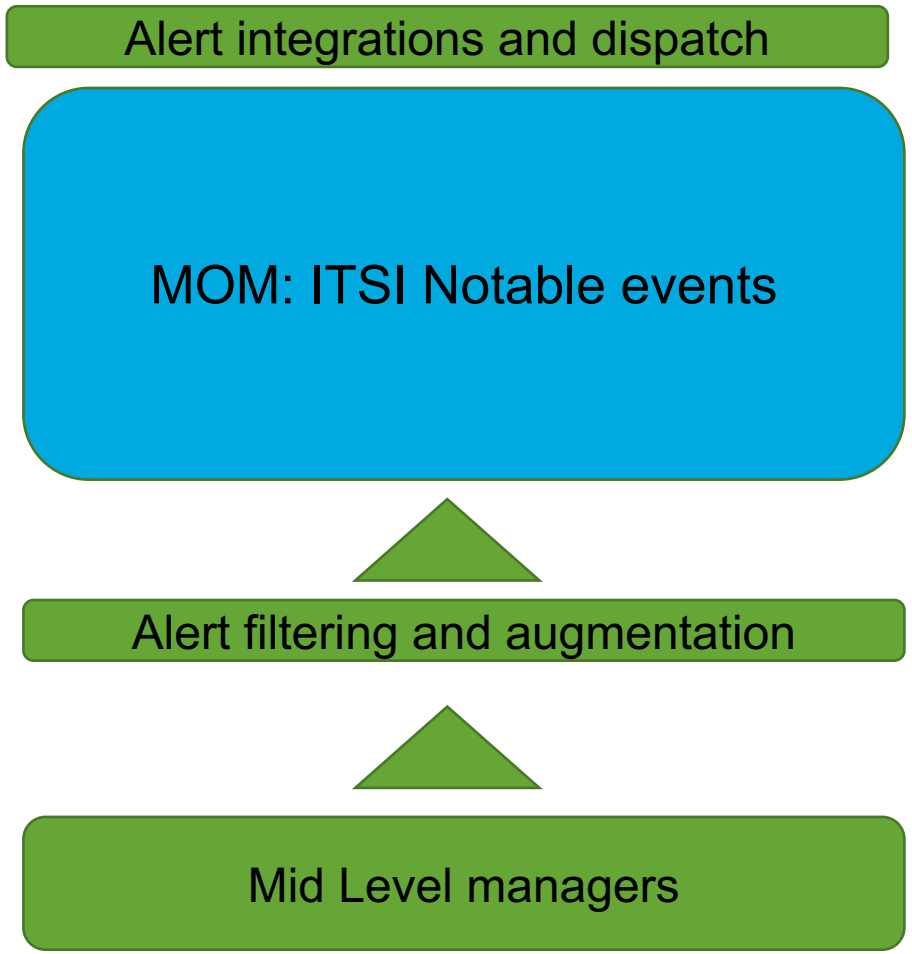
Requirements of an Event Manager

- 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
  - Closein 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

Splunk – IT Service Intelligence

- **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

splunk> .conf2017

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

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

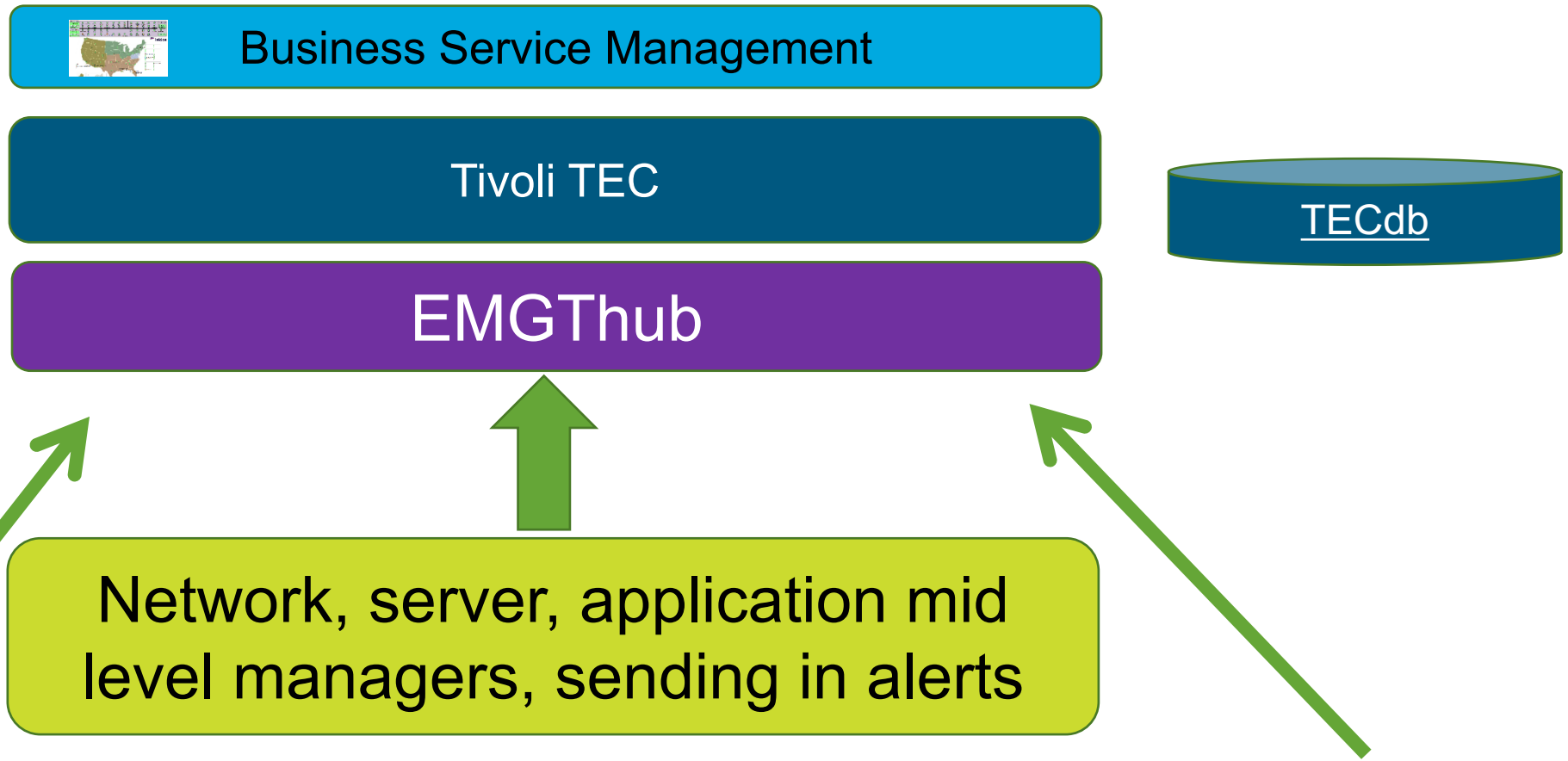
Centralize in ITSI

- 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: Splunk collects NPM perf data via Dbconnect. Correlation search watches for router uplink util >95% . Generates notable event to ITSI.

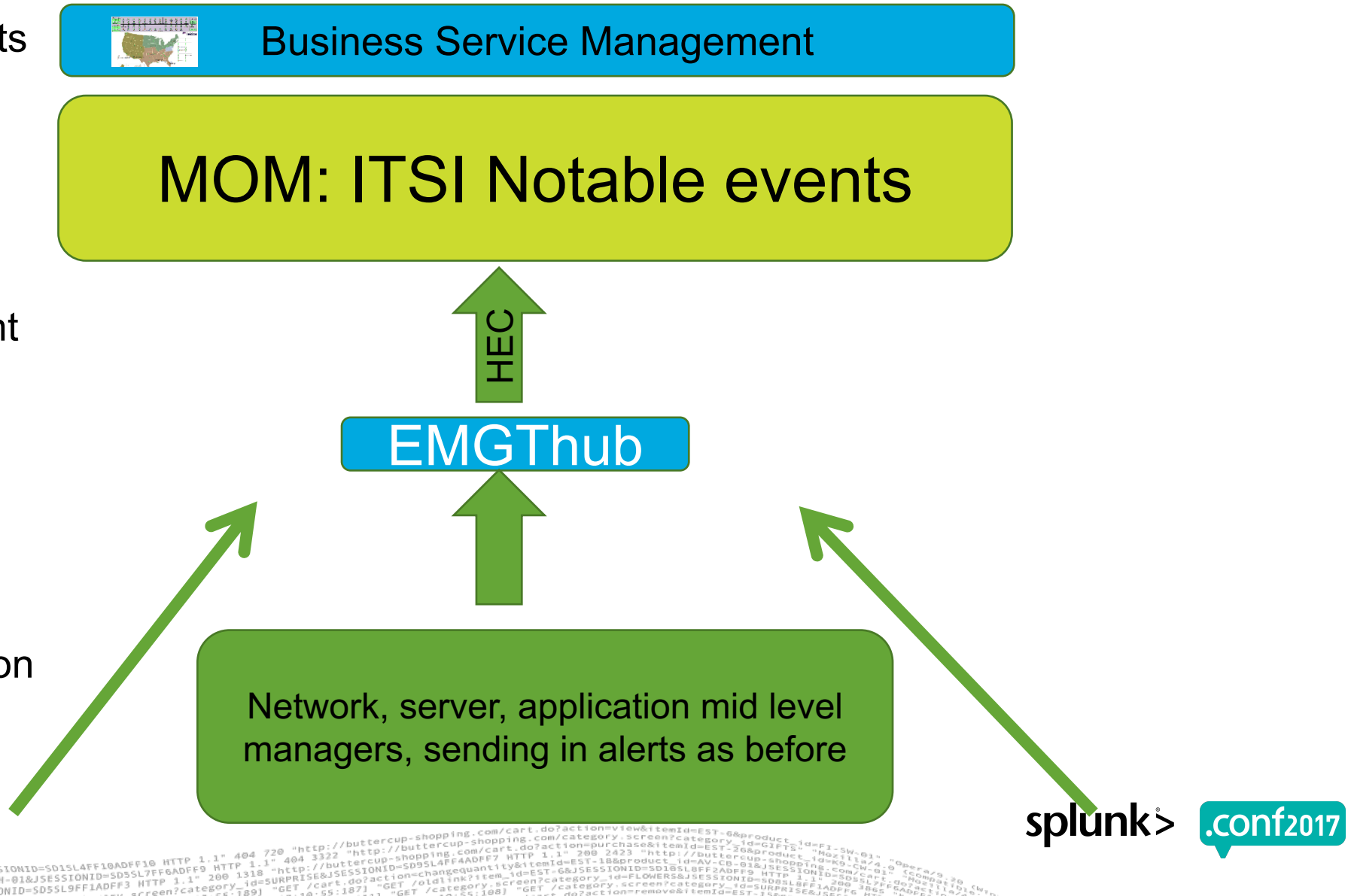
Event flow (before)

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



Event Flow with ITSI

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



Business Service Managemen 7

5 MOM: ITSI Notable events (via ITSI_grouped_alerts)

postemsg

ITSI2BSM

ITSI2EMGT

6

EMGThub

Tellemgt()

ITSI Rules 4

curl

2

http event collector

emgtmlm2splunk

3 Itsi_tracked_alerts

curl

Emgthub2splunk.mlm

tellitsi

1

Network, server, application MLM Alerts

ITSI and EMGT in 7 easy steps

splunk> .conf2017

What we need the rules to do

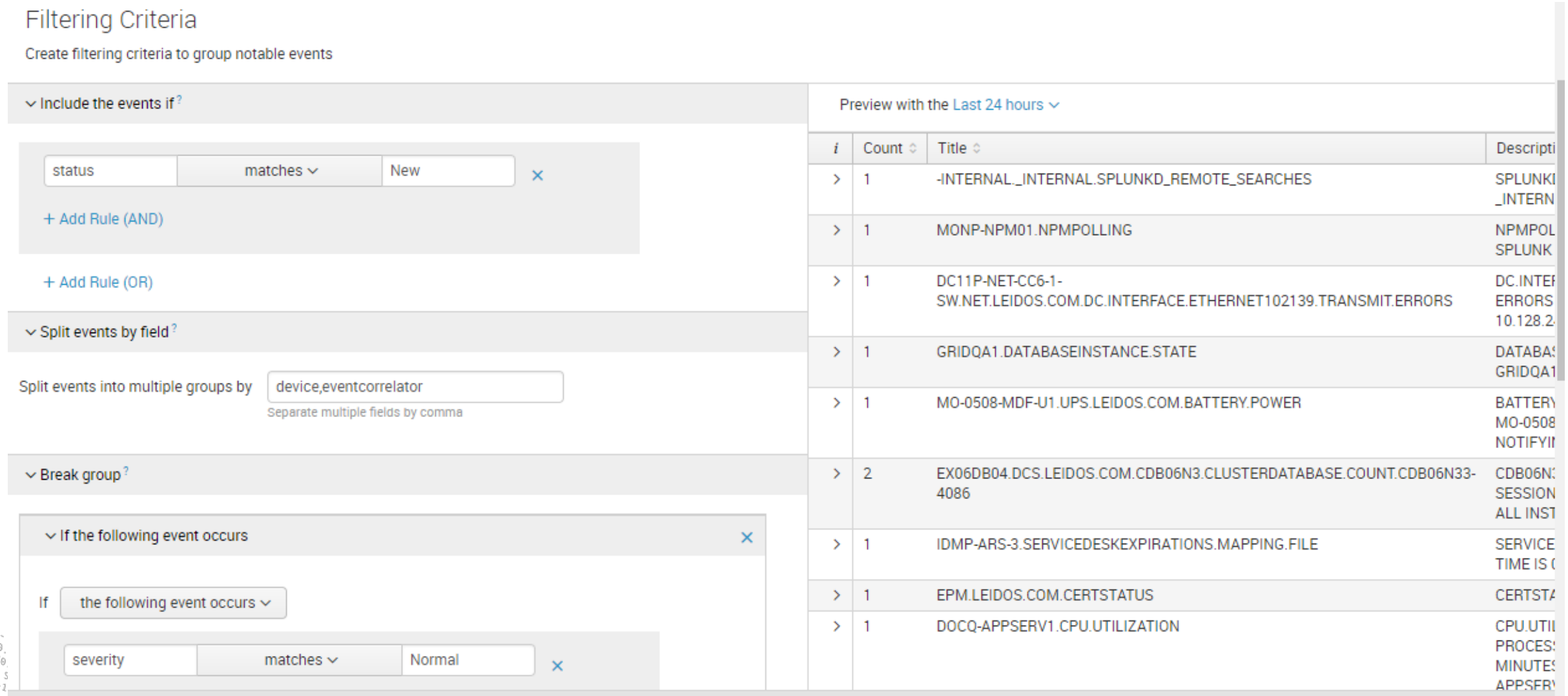
Basics

- 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

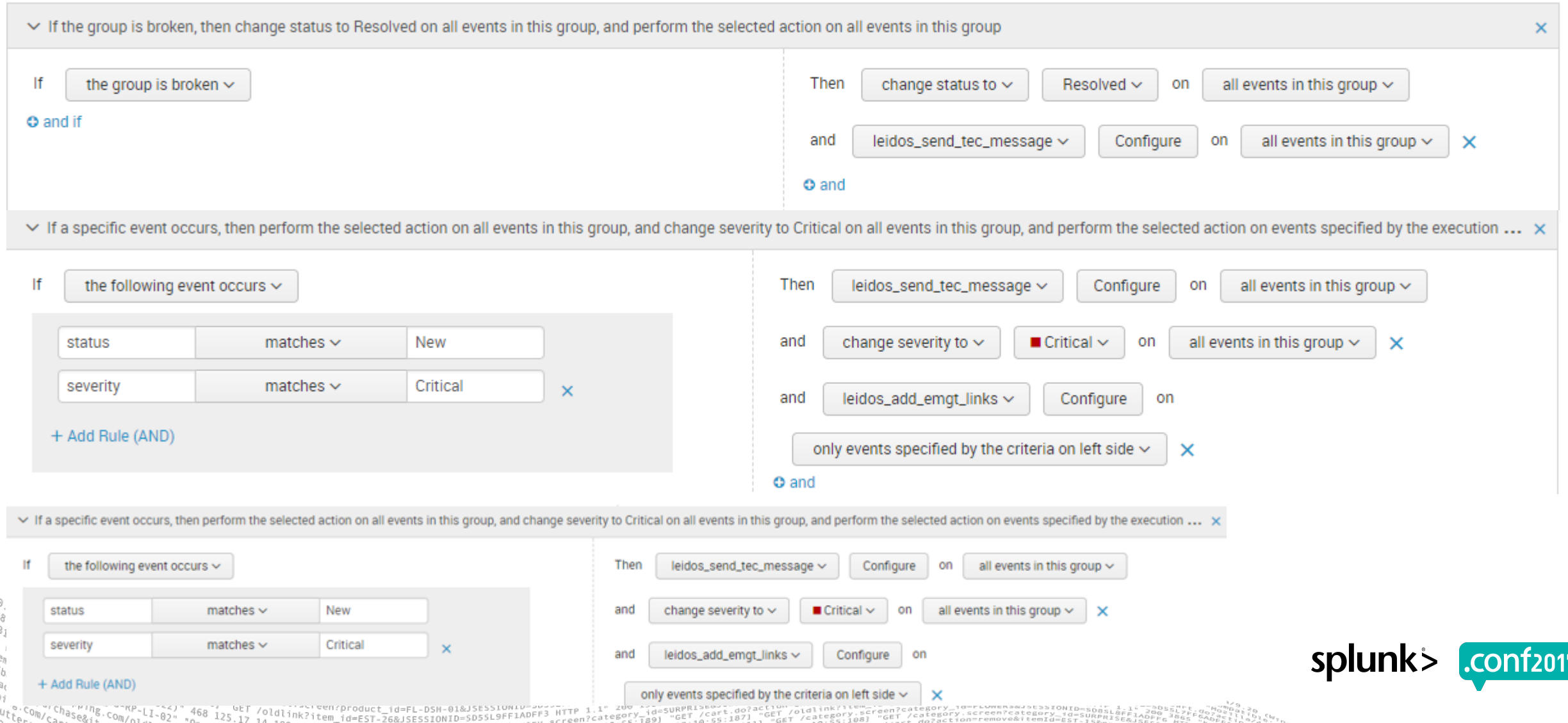
Escalations and Timed

- 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 - Matching Criteria

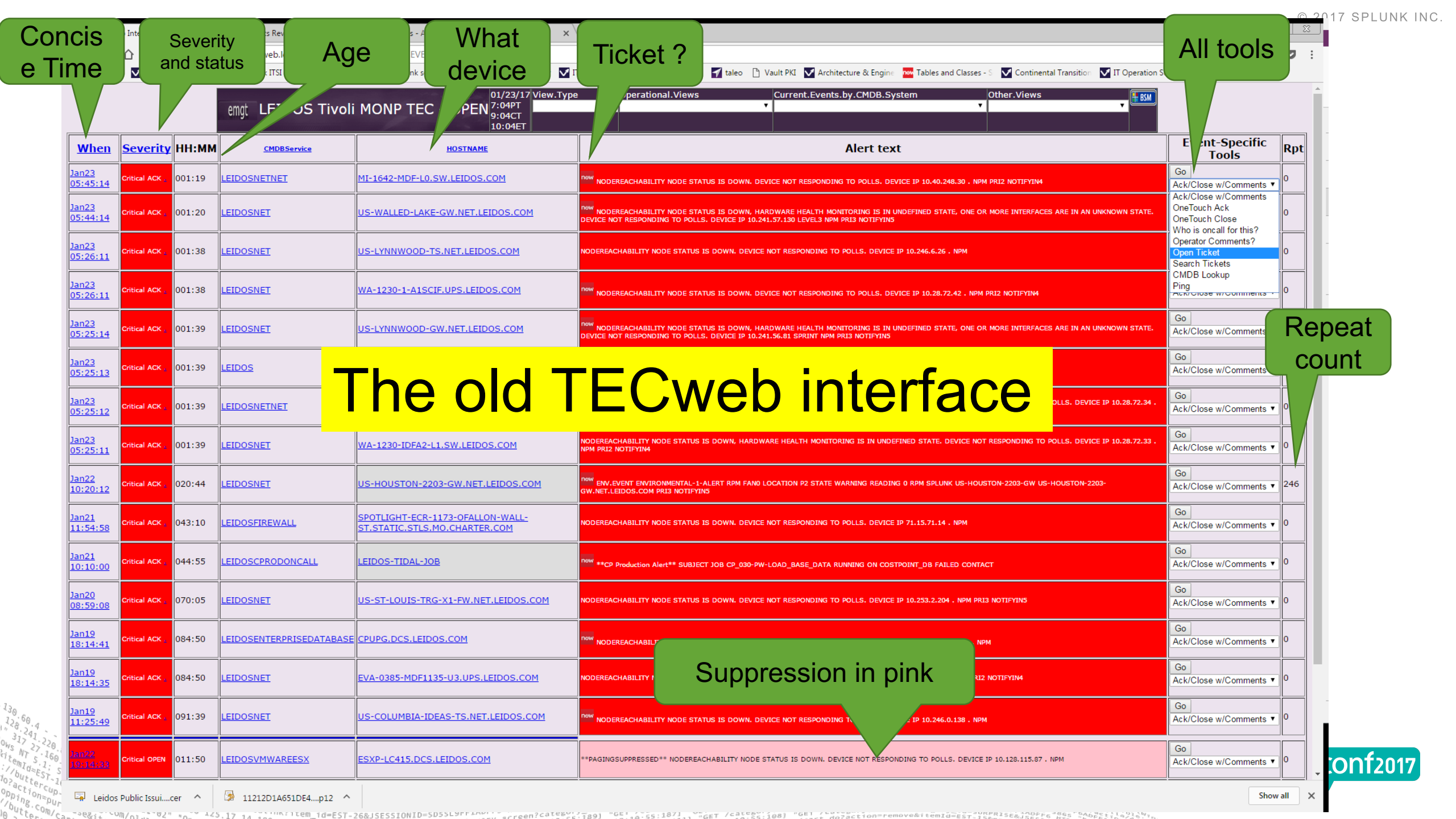


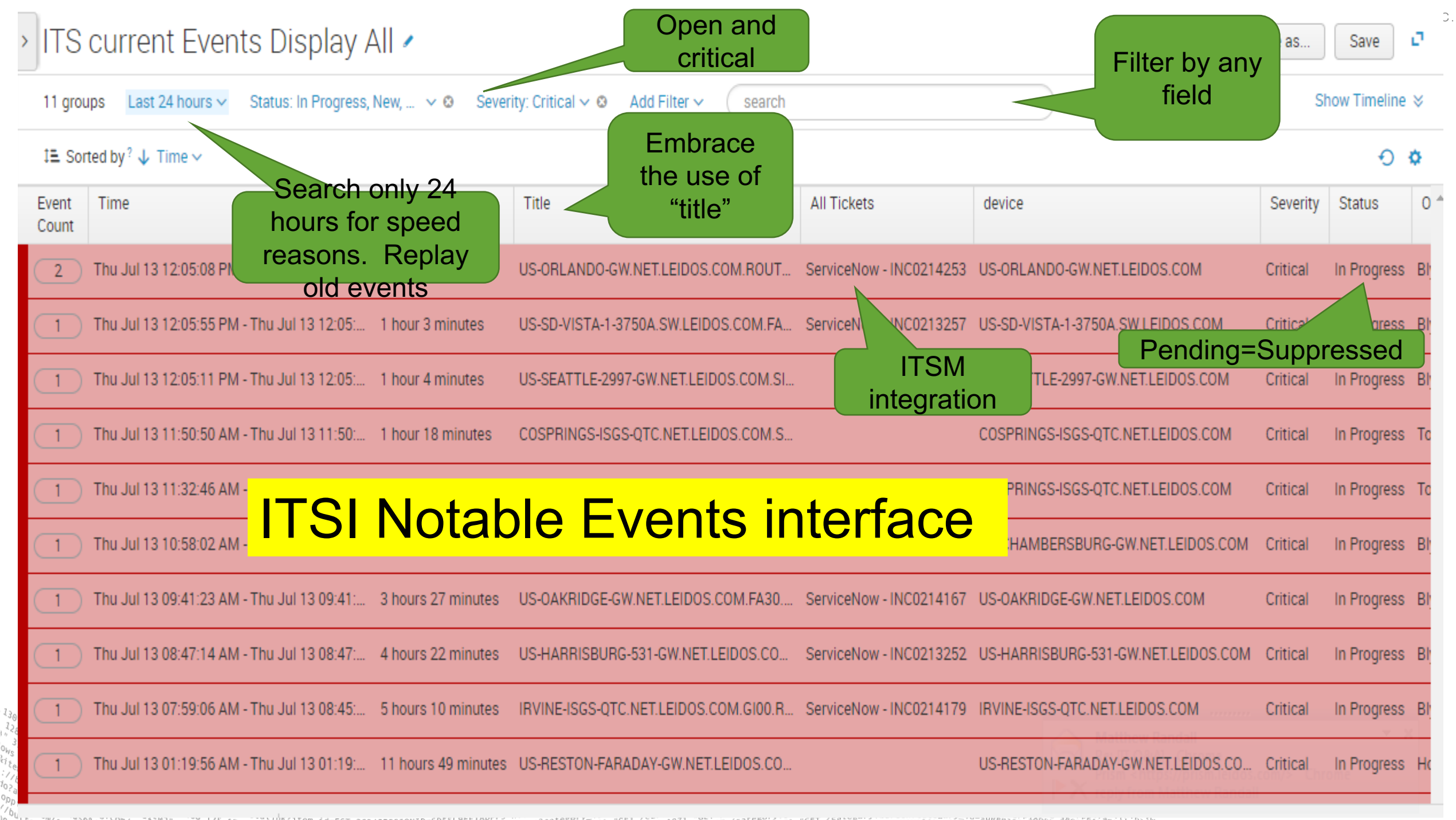
Rules Engine- incoming - actions



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 ...
If
the following event occurs
status
matches
New
severity
matches
Critical
+ Add Rule (AND)
Then
leidos_send_tec_message
Configure
on
all events in this group
and
change severity to
Critical
on
all events in this group
and
leidos_add_emgt_links
Configure
on
only events specified by the criteria on left side

splunk> .conf2017




ITS current Events Display All
Open and critical
Filter by any field
11 groups
Last 24 hours
Status: In Progress, New, ...
Severity: Critical
Add Filter
search
Show Timeline
Sorted by Time
Search only 24 hours for speed reasons. Replay old events
Embrace the use of "title"
Event Count
Time
Title
All Tickets
device
Severity
Status
ITSM integration
Pending=Suppressed
ITSI Notable Events interface

ITS current Events Display All

Save as... Save

11 groups | Last 24 hours | Status: In Progress, New, ... | Severity: Critical | Add Filter | search | Show Timeline

Changing state

Sorted by Time

2	US-ORLANDO-G...	Thu Jul 13 2017 12:05:08 GMT-0400 (ED...	BL
	All Tickets: ServiceNow - INC0214253	**device:** US-ORLAN...	
1	US-SD-VISTA-1-3...	Thu Jul 13 2017 12:05:55 GMT-0400 (ED...	BL
	All Tickets: ServiceNow - INC0213257	**device:** US-SD-VIST...	
1	US-SEATTLE-29...	Thu Jul 13 2017 12:05:11 GMT-0400 (ED...	BL
	device: US-SEATTLE-2997-GW.NET.LEIDOS.COM	**Severity:**...	
1	COSPRINGS-ISG...	Thu Jul 13 2017 11:50:50 GMT-0400 (ED...	TC
	device: COSPRINGS-ISGS-QTC.NET.LEIDOS.COM	**Severity**...	
1	COSPRINGS-ISG...	Thu Jul 13 2017 11:32:46 GMT-0400 (ED...	TC
	device: COSPRINGS-ISGS-QTC.NET.LEIDOS.COM	**Severity**...	
1	US-CHAMBERSB...	Thu Jul 13 2017 10:58:02 GMT-0400 (ED...	BL
	All Tickets: ServiceNow - INC0214239	**device:** US-CHAMB...	
1	US-OAKRIDGE-G...	Thu Jul 13 2017 09:41:23 GMT-0400 (ED...	BL
	All Tickets: ServiceNow - INC0214167	**device:** US-OAKRID...	
1	US-HARRISBUR...	Thu Jul 13 2017 08:47:14 GMT-0400 (ED...	BL
	All Tickets: ServiceNow - INC0213252	**device:** US-HARRIS...	

Critical | In Progress | Bly, Jefferson L. | Actions

US-ORLANDO-GW.NET.LEIDOS.COM.ROUTER.IPMCAST.RPF.LOOKUP.LOOP

Thu Jul 13 2017 12:05:08 GMT-0400 (EDT) - Thu Jul 13 2017 13:05:10 GMT-0400 (EDT)

Overview | Grouped Events | Comments | Activity

Open tickets, etc…

Description

ROUTER.IPMCAST.RPF.LOOKUP.LOOP RPF ROUTE LOOKUP LOOP FOR 10.11.228.4 SPLUNK US-ORLAND
GW.NET.LEIDOS.COM PRI3 NOTIFYIN5

2 Notable Events are grouped based on the aggregation policy: incomingnew

● 2

All Tickets

- Cmdb_Lookup - ExternalLink
- Log_File_Lookup - ExternalLink
- who is oncall - ExternalLink
- ServiceNow - INC0214253

All links

Contributing KPIs Open all in Deep Dive

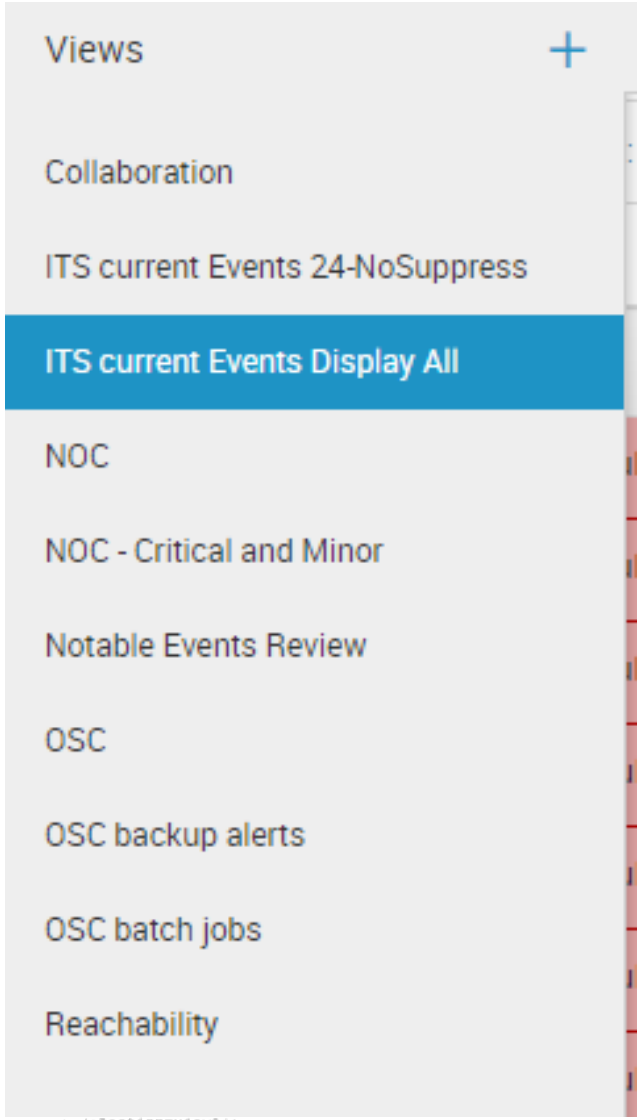
Possible Affected Services Open all in Deep Dive

- WAN

Tie to the service

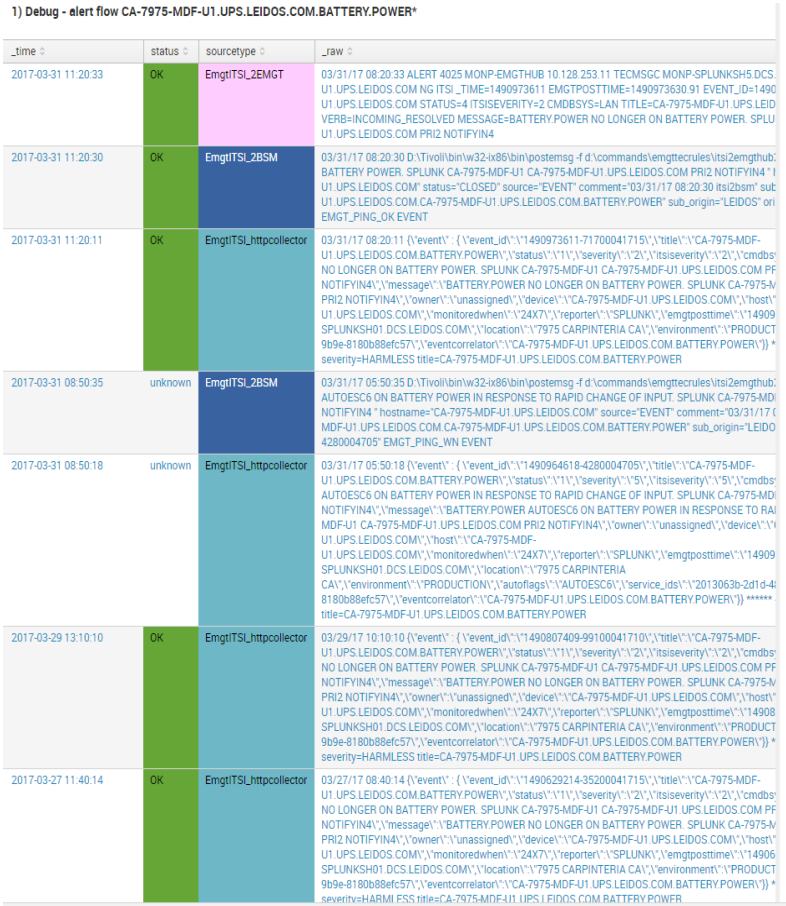
ITSI Views Of Alerts

- 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



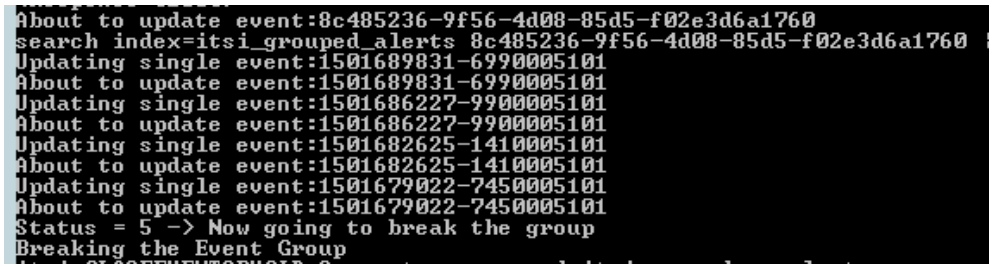
1) Debug - alert flow CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER*

_time	status	sourcetype	_raw
2017-03-31 11:20:33	OK	EmgtITSI_2EMGT	03/31/17 08:20:33 ALERT 4025 MONP-EMGTHUB 10.128.253.11 TECMSGC MONP-SPLUNKSH5.DCS. U1.UPS.LEIDOS.COM NG ITSI _TIME=1490973611 EMGTPOSTTIME=1490973630.91 EVENT_ID=1490 U1.UPS.LEIDOS.COM STATUS=4 ITSISEVERITY=2 CMDBSYS=LAN TITLE=CA-7975-MDF-U1.UPS.LEID VERB=INCOMING_RESOLVED MESSAGE=BATTERY.POWER NO LONGER ON BATTERY POWER. SPLU U1.UPS.LEIDOS.COM PRI2 NOTIFYIN4
2017-03-31 11:20:30	OK	EmgtITSI_2BSM	03/31/17 08:20:30 D:\Tivoli\bin\w32-ix86\bin\postemsg -f d:\commands\emgttecrules\itsi2emgthub: BATTERY POWER. SPLUNK CA-7975-MDF-U1 CA-7975-MDF-U1.UPS.LEIDOS.COM PRI2 NOTIFYIN4 " U1.UPS.LEIDOS.COM" status="CLOSED" source="EVENT" comment="03/31/17 08:20:30 itsi2bsm" sub U1.UPS.LEIDOS.COM.CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER" sub_origin="LEIDOS" ori EMGT_PING_OK EVENT
2017-03-31 11:20:11	OK	EmgtITSI_httpcollector	03/31/17 08:20:11 {\"event\" : { \"event_id\":\"1490973611-71700041715\",\"title\":\"CA-7975-MDF- U1.UPS.LEIDOS.COM.BATTERY.POWER\",\"status\":\"1\",\"severity\":\"2\",\"itsiseverity\":\"2\",\"cmdbs NO LONGER ON BATTERY POWER. SPLUNK CA-7975-MDF-U1 CA-7975-MDF-U1.UPS.LEIDOS.COM PF NOTIFYIN4\",\"message\":\"BATTERY.POWER NO LONGER ON BATTERY POWER. SPLUNK CA-7975-M PRI2 NOTIFYIN4\",\"owner\":\"unassigned\",\"device\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM\",\"host\" U1.UPS.LEIDOS.COM\",\"monitoredwhen\":\"24X7\",\"reporter\":\"SPLUNK\",\"emgtposttime\":\"14909 SPLUNKSH01.DCS.LEIDOS.COM\",\"location\":\"7975 CARPINTERIA CA\",\"environment\":\"PRODUCT 9b9e-8180b88efc57\",\"eventcorrelator\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER\"}} * severity=HARMLESS title=CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER
2017-03-31 08:50:35	unknown	EmgtITSI_2BSM	03/31/17 05:50:35 D:\Tivoli\bin\w32-ix86\bin\postemsg -f d:\commands\emgttecrules\itsi2emgthub: AUTOESC6 ON BATTERY POWER IN RESPONSE TO RAPID CHANGE OF INPUT. SPLUNK CA-7975-MD NOTIFYIN4 " hostname="CA-7975-MDF-U1.UPS.LEIDOS.COM" source="EVENT" comment="03/31/17 (MDF-U1.UPS.LEIDOS.COM.CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER" sub_origin="LEIDO 4280004705" EMGT_PING_WN EVENT
2017-03-31 08:50:18	unknown	EmgtITSI_httpcollector	03/31/17 05:50:18 {\"event\" : { \"event_id\":\"1490964618-4280004705\",\"title\":\"CA-7975-MDF- U1.UPS.LEIDOS.COM.BATTERY.POWER\",\"status\":\"1\",\"severity\":\"5\",\"itsiseverity\":\"5\",\"cmdbs AUTOESC6 ON BATTERY POWER IN RESPONSE TO RAPID CHANGE OF INPUT. SPLUNK CA-7975-MD NOTIFYIN4\",\"message\":\"BATTERY.POWER AUTOESC6 ON BATTERY POWER IN RESPONSE TO RA MDF-U1 CA-7975-MDF-U1.UPS.LEIDOS.COM PRI2 NOTIFYIN4\",\"owner\":\"unassigned\",\"device\":\" U1.UPS.LEIDOS.COM\",\"host\":\"CA-7975-MDF- U1.UPS.LEIDOS.COM\",\"monitoredwhen\":\"24X7\",\"reporter\":\"SPLUNK\",\"emgtposttime\":\"14909 SPLUNKSH01.DCS.LEIDOS.COM\",\"location\":\"7975 CARPINTERIA CA\",\"environment\":\"PRODUCTION\",\"autoflags\":\"AUTOESC6\",\"service_ids\":\"2013063b-2d1d-4 8180b88efc57\",\"eventcorrelator\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER\"}} ****** title=CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER
2017-03-29 13:10:10	OK	EmgtITSI_httpcollector	03/29/17 10:10:10 {\"event\" : { \"event_id\":\"1490807409-99100041710\",\"title\":\"CA-7975-MDF- U1.UPS.LEIDOS.COM.BATTERY.POWER\",\"status\":\"1\",\"severity\":\"2\",\"itsiseverity\":\"2\",\"cmdbs NO LONGER ON BATTERY POWER. SPLUNK CA-7975-MDF-U1 CA-7975-MDF-U1.UPS.LEIDOS.COM PF NOTIFYIN4\",\"message\":\"BATTERY.POWER NO LONGER ON BATTERY POWER. SPLUNK CA-7975-M PRI2 NOTIFYIN4\",\"owner\":\"unassigned\",\"device\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM\",\"host\" U1.UPS.LEIDOS.COM\",\"monitoredwhen\":\"24X7\",\"reporter\":\"SPLUNK\",\"emgtposttime\":\"14908 SPLUNKSH01.DCS.LEIDOS.COM\",\"location\":\"7975 CARPINTERIA CA\",\"environment\":\"PRODUCT 9b9e-8180b88efc57\",\"eventcorrelator\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER\"}} * severity=HARMLESS title=CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER
2017-03-27 11:40:14	OK	EmgtITSI_httpcollector	03/27/17 08:40:14 {\"event\" : { \"event_id\":\"1490629214-35200041715\",\"title\":\"CA-7975-MDF- U1.UPS.LEIDOS.COM.BATTERY.POWER\",\"status\":\"1\",\"severity\":\"2\",\"itsiseverity\":\"2\",\"cmdbs NO LONGER ON BATTERY POWER. SPLUNK CA-7975-MDF-U1 CA-7975-MDF-U1.UPS.LEIDOS.COM PF NOTIFYIN4\",\"message\":\"BATTERY.POWER NO LONGER ON BATTERY POWER. SPLUNK CA-7975-M PRI2 NOTIFYIN4\",\"owner\":\"unassigned\",\"device\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM\",\"host\" U1.UPS.LEIDOS.COM\",\"monitoredwhen\":\"24X7\",\"reporter\":\"SPLUNK\",\"emgtposttime\":\"14906 SPLUNKSH01.DCS.LEIDOS.COM\",\"location\":\"7975 CARPINTERIA CA\",\"environment\":\"PRODUCT 9b9e-8180b88efc57\",\"eventcorrelator\":\"CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER\"}} * severity=HARMLESS title=CA-7975-MDF-U1.UPS.LEIDOS.COM.BATTERY.POWER

splunk> .conf2017

ITSI - The Every 5 Min Job (Via alertutil.py)

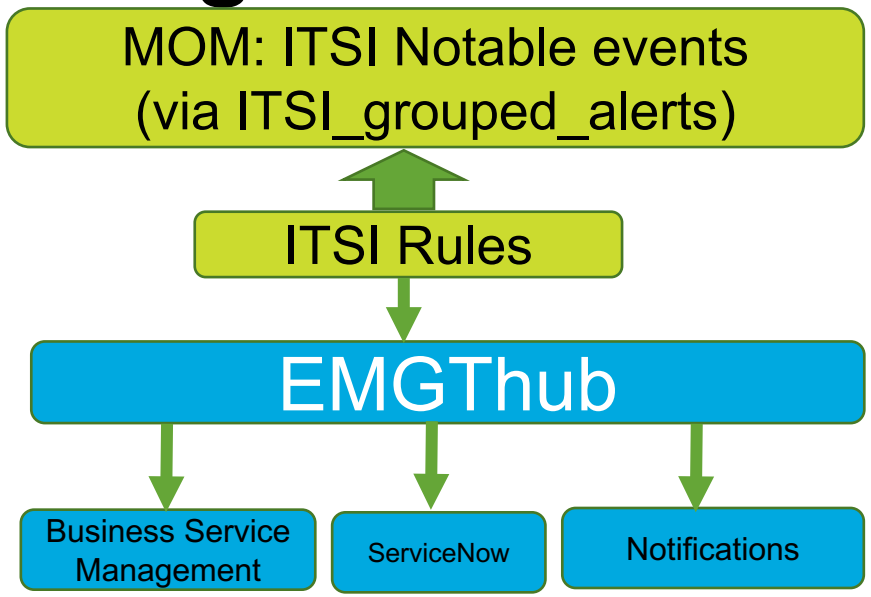
- Gather critical events
  - earliest=-7d latest=now `itsigroupedopenalerts` | search * | sort itsi_first_event_time desc | table ztime event_id itsi_group_id itsi_first_event_time title device severitynum statusnum autoflags monitoredwhen eventage cmdbsys location environment incident itsi_group_count description
- Process thru critical events
  - Close duplicates (setstatus), Closein (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 autoescxx min (setseverity)



splunk> .conf2017

ITSI - The Notification Engine

- 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

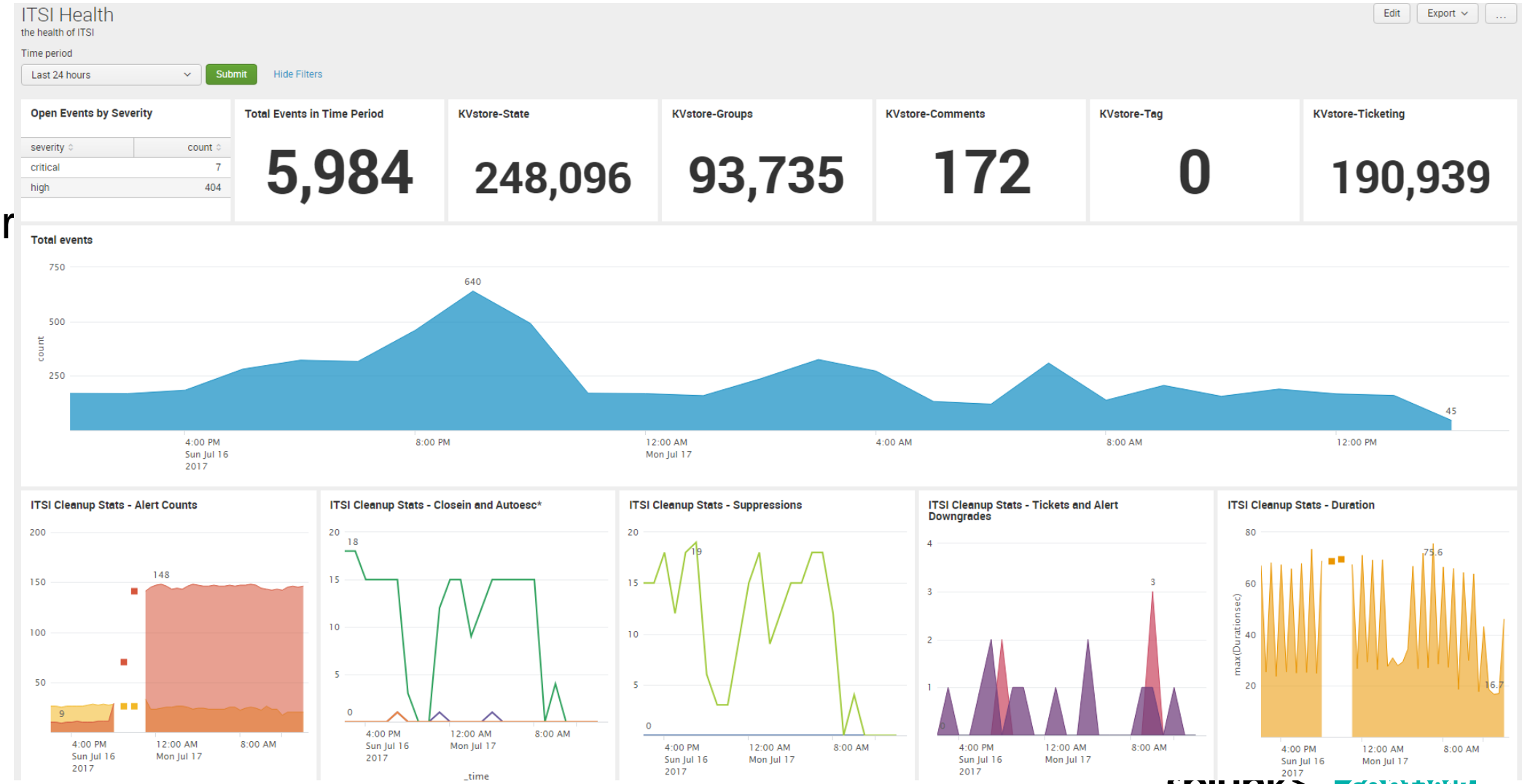


Alert flow

_time	sourcetype	verb	device	severity
2017-07-18 17:11:39	emgt_mim_alerts	EMGTEVENTFLOW	EMP-EXMR250	MINOR
2017-07-18 17:11:32	EmgtITSI_2EMGT	INCOMING_CRITICAL	EX06DB03.DCS.LEIDOS.COM	CRITICAL
2017-07-18 17:10:58	EmgtITSI_2EMGT	INCOMING_CRITICAL	US-SD-VISTA-1-3750A.SW.LEIDOS.COM	CRITICAL
2017-07-18 17:10:17	EmgtITSI_2EMGT	INCOMING_RESOLVED	VA-1471-IDF3104-U1.UPS.LEIDOS.COM	HARMLESS
2017-07-18 17:10:15	EmgtITSI_2BSM	ITSI2BSM	ORAPP-12.DCS.LEIDOS.COM	CRITICAL
2017-07-18 17:10:15	EmgtITSI_2BSM	ITSI2BSM	VA-1471-IDF3104-U1.UPS.LEIDOS.COM	HARMLESS
2017-07-18 17:10:13	emgt_mim_alerts	EMGTEVENTFLOW	ORAPP-12.DCS.LEIDOS.COM	CRITICAL
2017-07-18 17:10:09	emgt_mim_alerts	EMGTEVENTFLOW	VA-1471-IDF3104-U1.UPS.LEIDOS.COM	HARMLESS
2017-07-18 17:09:50	emgt_mim_alerts	EMGTEVENTFLOW	EMP-MX01.DCS.LEIDOS.COM	MINOR
2017-07-18 17:09:41	EmgtITSI_2EMGT	INCOMING_CRITICAL	US-HARRISBURG-531-GW.NET.LEIDOS.COM	CRITICAL
2017-07-18 17:09:22	EmgtITSI_2EMGT	INCOMING_MINOR	VA-1887-IDF2-L1.SW.LEIDOS.COM	MINOR
2017-07-18 17:09:22	EmgtITSI_2BSM	ITSI2BSM	VA-1887-IDF2-L1.SW.LEIDOS.COM	MINOR
2017-07-18 17:09:12	EmgtITSI_2BSM	ITSI2BSM	US-SD-VISTA-1-3750A.SW.LEIDOS.COM	CRITICAL
2017-07-18 17:09:11	EmgtITSI_2EMGT	INCOMING_CRITICAL	DC11P-NET-TRUSTED1-SW	CRITICAL
2017-07-18 17:09:07	emgt_mim_alerts	EMGTEVENTFLOW	VA-1887-IDF2-L1.SW.LEIDOS.COM	MINOR
2017-07-18 17:09:07	EmgtITSI_2EMGT	INCOMING_CRITICAL	PA-0069-MDF-L0.SW.LEIDOS.COM	CRITICAL
2017-07-18 17:09:06	EmgtITSI_2EMGT	INCOMING_CRITICAL	DC11P-NET-CC6-0-SW.NET.LEIDOS.COM	CRITICAL
2017-07-18 17:09:06	EmgtITSI_2BSM	ITSI2BSM	PA-0069-MDF-L0.SW.LEIDOS.COM	CRITICAL
2017-07-18 17:09:05	EmgtITSI_2BSM	ITSI2BSM	DC11P-NET-TRUSTED1-SW	CRITICAL
2017-07-18 17:08:59	EmgtITSI_2BSM	ITSI2BSM	EX06DB01.DCS.LEIDOS.COM	CRITICAL

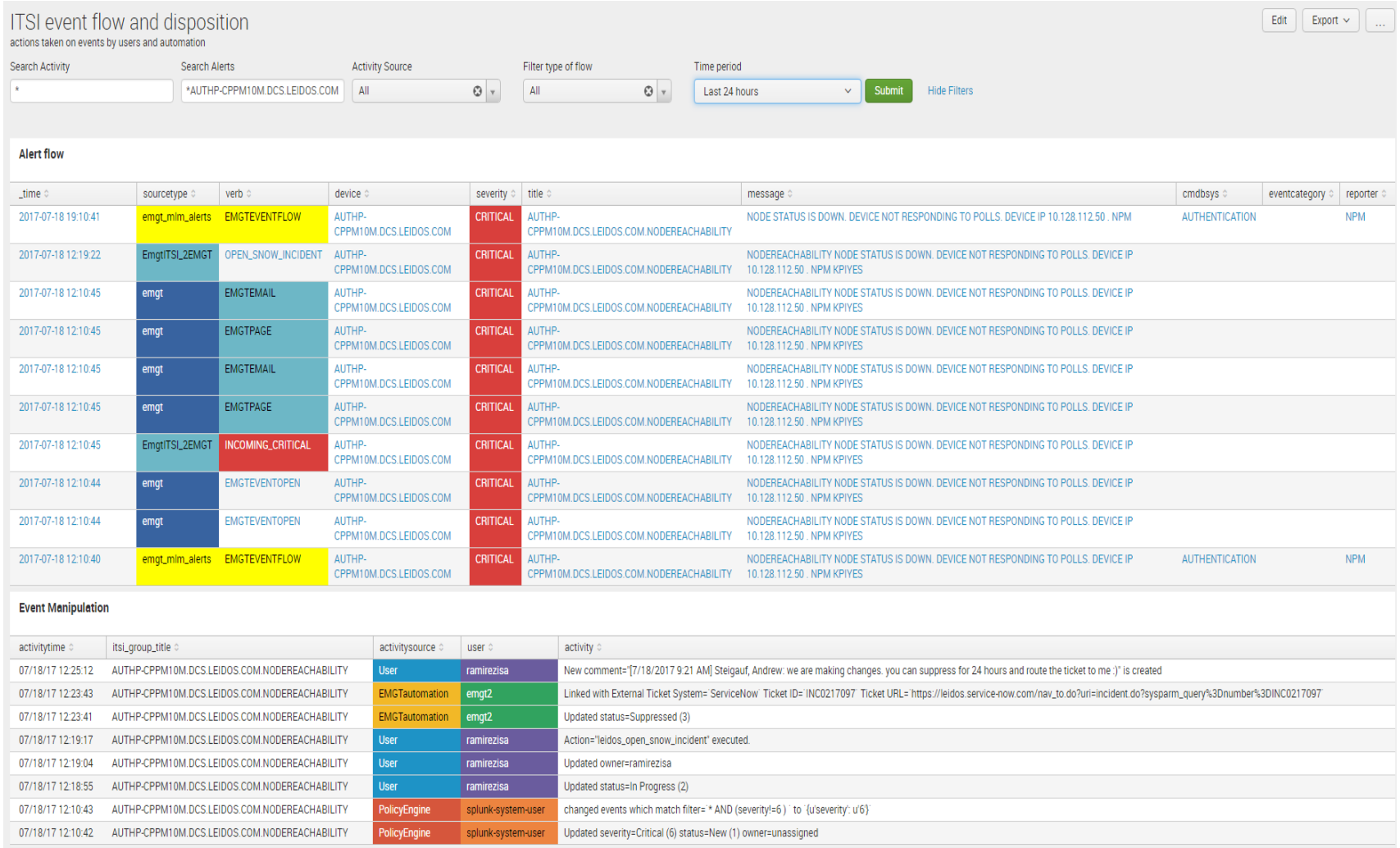
ITSI Health

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



ITSI - Event Disposition

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



ITSI event flow and disposition

actions taken on events by users and automation

Edit | Export | ...

Search Activity: * | Search Alerts: *AUTHP-CPPM10M.DCS.LEIDOS.COM | Activity Source: All | Filter type of flow: All | Time period: Last 24 hours | Submit | Hide Filters

Alert flow

_time	sourcetype	verb	device	severity	title	message	cmdbsys	eventcategory	reporter
2017-07-18 19:10:41	emgt_mim_alerts	EMGTEVENTFLOW	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM	AUTHENTICATION		NPM
2017-07-18 12:19:22	EmgtITSI_2EMGT	OPEN_SNOW_INCIDENT	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:45	emgt	EMGTEMAIL	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:45	emgt	EMGTPAGE	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:45	emgt	EMGTEMAIL	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:45	emgt	EMGTPAGE	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:45	EmgtITSI_2EMGT	INCOMING_CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:44	emgt	EMGTEVENTOPEN	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:44	emgt	EMGTEVENTOPEN	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES			
2017-07-18 12:10:40	emgt_mim_alerts	EMGTEVENTFLOW	AUTHP-CPPM10M.DCS.LEIDOS.COM	CRITICAL	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.128.112.50 . NPM KPIYES	AUTHENTICATION		NPM

Event Manipulation

activitytime	itsi_group_title	activitysource	user	activity
07/18/17 12:25:12	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	User	ramirezisa	New comment="[7/18/2017 9:21 AM] Steigauf, Andrew: we are making changes. you can suppress for 24 hours and route the ticket to me :)" is created
07/18/17 12:23:43	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	EMGTautomation	emgt2	Linked with External Ticket System=`ServiceNow` Ticket ID=`INC0217097` Ticket URL=`https://leidos.service-now.com/nav_to.do?uri=incident.do?sysparm_query%3Dnumber%3DINC0217097`
07/18/17 12:23:41	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	EMGTautomation	emgt2	Updated status=Suppressed (3)
07/18/17 12:19:17	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	User	ramirezisa	Action="leidos_open_snow_incident" executed.
07/18/17 12:19:04	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	User	ramirezisa	Updated owner=ramirezisa
07/18/17 12:18:55	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	User	ramirezisa	Updated status=In Progress (2)
07/18/17 12:10:43	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	PolicyEngine	splunk-system-user	changed events which match filter=`* AND (severity!=6 )` to `{u'severity': u'6'}`
07/18/17 12:10:42	AUTHP-CPPM10M.DCS.LEIDOS.COM.NODEREACHABILITY	PolicyEngine	splunk-system-user	Updated severity=Critical (6) status=New (1) owner=unassigned

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

{\"event\" : { \“
event_id\":\"1500408105-8910004091\",\“
title\":\"SWITCH1.INTERFACE.TRANSMIT.ERRORS\",\“
status\":\"1\",\"severity\":\"2\",\"itsiseverity\":\"2\",\"cmdbsys\":\"WAN\",\“
description\":\"DC.INTERFACE.ETHERNET101/1/15.TRANSMIT.ERROR
S NBUP-DD6800, ETHM-A MGMT HAS CLEARED NPM\",\“
message\":\"INTERFACE.ETHERNET101/1/15.TRANSMIT.ERRORS
HAS CLEARED NPM\",\“
owner\":\"unassigned\",\"device\":\"SWITCH1\",\"host\":\"SWITCH1\",\“
monitoredwhen\":\"24X7\",\"reporter\":\
"NPM\",\"emgtposttime\":\"1500408105\",\“
eventsource\":\"NPM01\",\"location\":\"2079 datacenter\",\“
environment\":\"PRODUCTION\",\"autoflags\":\".\",\“
service_ids\":\"8d8ba168-b320-4dff-8b85-2987371fde8e\",\“
eventcorrelator\":\“SWITCH1.INTERFACE.ETHERNET101115.TRANSMI
T.ERRORS\"}}

```
index=itsi_tracked_alerts|eval AlertMessage=message | join  type=left
event_id appendcols [search index=itsi_grouped_alerts|eval
TickMessage=itsi_group_description] | search *    *   |  sort _time desc  |
search NOT itsi_group_id=* | table _time, event_id, title
itsiseverity,,itsi_group_id
```

splunk> .conf2017

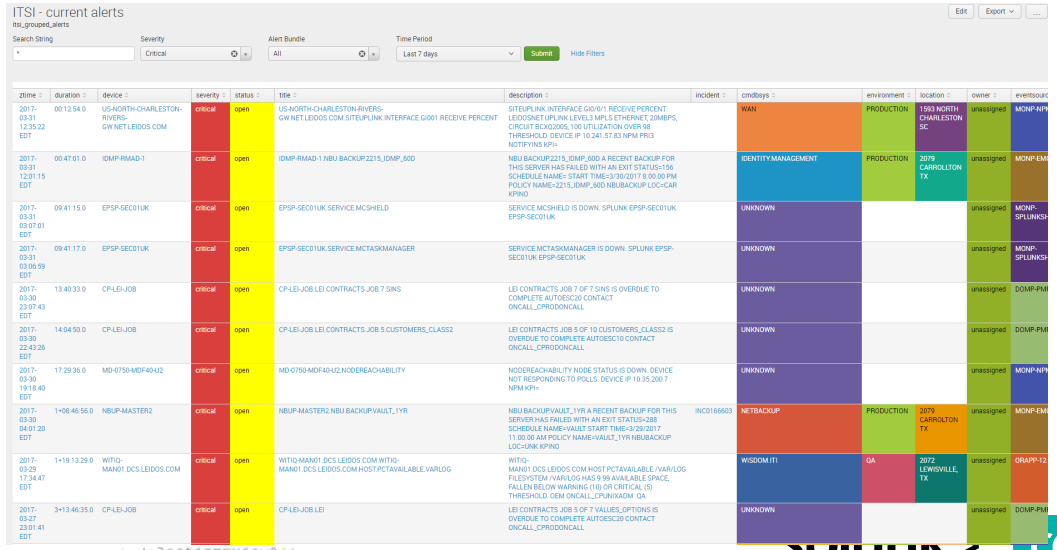
A Few Wish List Items

- 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

Outcome

- 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

Event Count	Title	Time	Owner	Status	device	All Tickets	Severity	Description
1	COMMANDER.LEIDOS.COM.SYNTH.USER.ACCESS.COMMANDER.LOGON	Fri Mar 31 12:35:46 PM - Fri Mar 31 12:35:46 PM	Unassigned	Suppressed	COMMANDER.LEIDOS.COM		Critical	SYNTH.USER.ACCESS.COMMANDER.LOGON REASO
1	US-NORTH-CHARLESTON-RIVERS-GW.NET.LEIDOS.COM.SITEUPLINK.INTERFACE.GI001.RECEIVE.PERCENT	Fri Mar 31 12:35:22 PM - Fri Mar 31 12:35:22 PM	Unassigned	New	US-NORTH-CHARLESTON-RIVERS-GW.NET.LEIDOS.COM		Critical	SITEUPLINK.INTERFACE.GI0/0/1.RECEIVE.PERCENT
1	IDMP-RMAD-1.NBU.BACKUP.2215_IDMP_60D	Fri Mar 31 12:01:15 PM - Fri Mar 31 12:01:15 PM	Unassigned	New	IDMP-RMAD-1		Critical	NBU.BACKUP.2215_IDMP_60D A RECENT BACKUP FO
41	WITIQ-MAN01.DCS.LEIDOS.COM.WITIQ-MAN01.DCS.LEIDOS.COM.HOST.PCTAVAILABLE.VARLOG	Wed Mar 29 17:34:47 PM - Fri Mar 31 11:49:05 AM	Unassigned	New	WITIQ-MAN01.DCS.LEIDOS.COM	ServiceNow - INC0167159	Critical	WITIQ-MAN01.DCS.LEIDOS.COM.HOST.PCTAVAILABL
1	EPSP-SEC01UK.SERVICE.MCSHIELD	Fri Mar 31 03:07:01 AM - Fri Mar 31 03:07:01 AM	Unassigned	New	EPSP-SEC01UK		Critical	SERVICE.MCSHIELD IS DOWN. SPLUNK EPSP-SEC01
1	EPSP-SEC01UK.SERVICE.MCTASKMANAGER	Fri Mar 31 03:06:59 AM - Fri Mar 31 03:06:59 AM	Unassigned	New	EPSP-SEC01UK		Critical	SERVICE.MCTASKMANAGER IS DOWN. SPLUNK EPSI
1	CP-LEI-JOB.LEI.CONTRACTS.JOB.7.SINS	Thu Mar 30 23:07:43 PM - Thu Mar 30 23:07:43 PM	Unassigned	New	CP-LEI-JOB		Critical	LEI CONTRACTS JOB 7 OF 7 SINS IS OVERDUE TO CO
1	CP-LEI-JOB.LEI.CONTRACTS.JOB.5.CUSTOMERS_CLASS2	Thu Mar 30 22:43:26 PM - Thu Mar 30 22:43:26 PM	Unassigned	New	CP-LEI-JOB		Critical	LEI CONTRACTS JOB 5 OF 10 CUSTOMERS_CLASS2 I
1	MD-0750-MDF40-U2.NODEREACHABILITY	Thu Mar 30 19:18:40 PM - Thu Mar 30 19:18:40 PM	Unassigned	New	MD-0750-MDF40-U2		Critical	NODEREACHABILITY NODE STATUS IS DOWN. DEVIC
1	NBUP-MASTER2.NBU.BACKUPVAULT_1YR	Thu Mar 30 04:01:20 AM - Thu Mar 30 04:01:20 AM	Unassigned	New	NBUP-MASTER2	ServiceNow - INC0166603	Critical	NBU.BACKUPVAULT_1YR A RECENT BACKUP FOR TH
1	WR-1230-1-3750F.SW.LEIDOS.COM.NODEREACHABILITY	Mon Mar 27 17:19:05 PM - Mon Mar 27 17:19:05 PM	Unassigned	New	WR-1230-1-3750F.SW.LEIDOS.COM	ServiceNow - INC0155760	Critical	NODEREACHABILITY NODE STATUS IS DOWN, HARD
1	VDIP-DHCP01.CORP.LEIDOS.COM.NODEREACHABILITY	Mon Mar 27 17:19:05 PM - Mon Mar 27 17:19:05 PM	Unassigned	New	VDIP-DHCP01.CORP.LEIDOS.COM		Critical	NODEREACHABILITY NODE STATUS IS DOWN. DEVIC
1	MA-2142-MDF104-U1.UPS.LEIDOS.COM.NODEREACHABILITY	Mon Mar 27 17:19:04 PM - Mon Mar 27 17:19:04 PM	Unassigned	New	MA-2142-MDF104-U1.UPS.LEIDOS.COM	ServiceNow - INC0161908	Critical	NODEREACHABILITY NODE STATUS IS DOWN. DEVIC
1	MAMD-0591-LAN-UPS-1.UPS.LEIDOS.COM.NODEREACHABILITY	Mon Mar 27 17:19:04 PM - Mon Mar 27 17:19:04 PM	Unassigned	New	MAMD-0591-LAN-UPS-1.UPS.LEIDOS.COM	ServiceNow - INC0165260	Critical	NODEREACHABILITY NODE STATUS IS DOWN. DEVIC



ITSI - current alerts

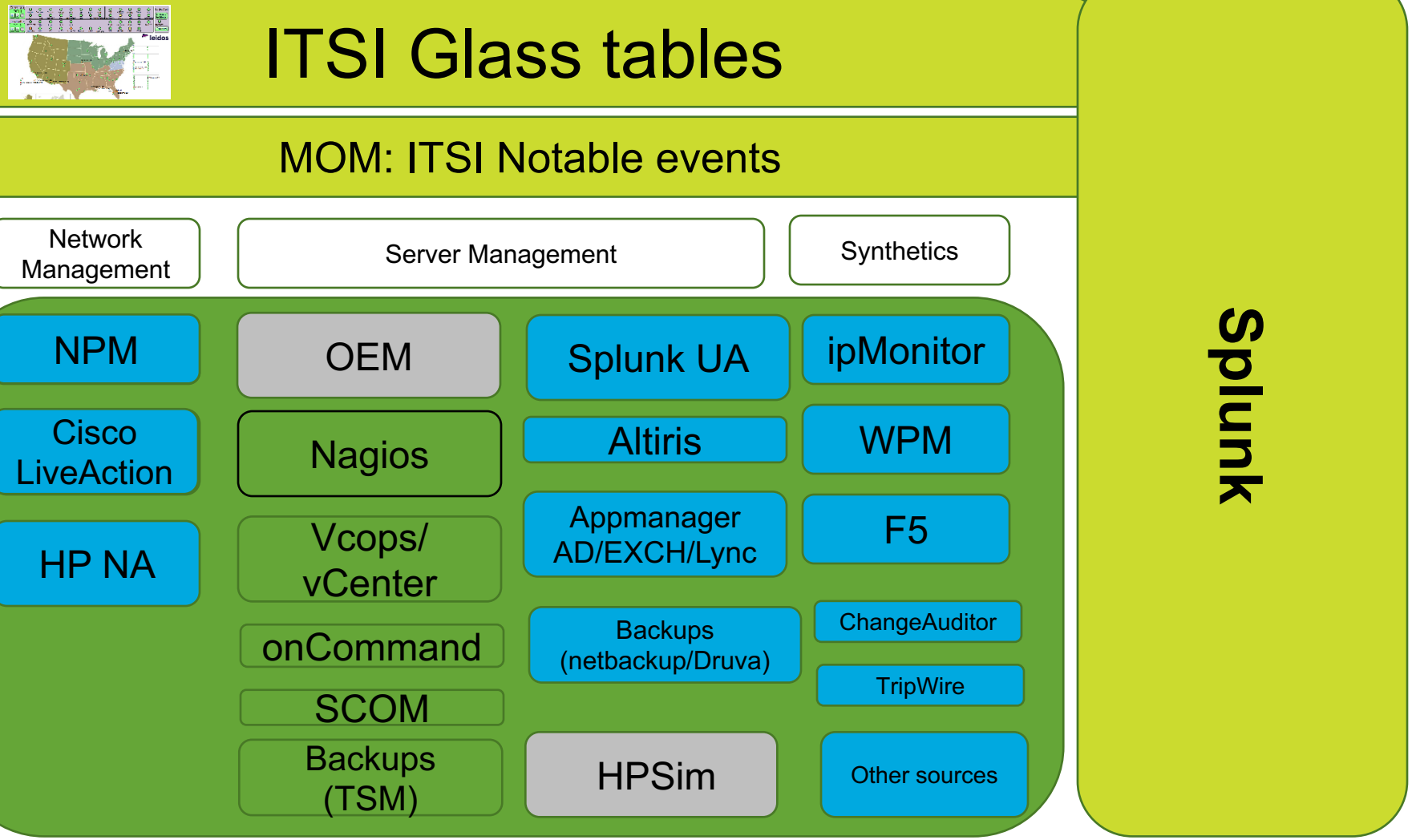
itsi_grouped_alerts

Search String | Severity: Critical | Alert Bundle: All | Time Period: Last 7 days | Submit | Hide Filters

ztime	duration	device	severity	status	title	description	incident	cmdbsys	environment	location	owner	eventsourc
2017-03-31 12:35:22 EDT	00:12:54.0	US-NORTH-CHARLESTON-RIVERS-GW.NET.LEIDOS.COM	critical	open	US-NORTH-CHARLESTON-RIVERS-GW.NET.LEIDOS.COM.SITEUPLINK.INTERFACE.GI001.RECEIVE.PERCENT	SITEUPLINK.INTERFACE.GI0/0/1.RECEIVE.PERCENT LEIDOSNET.UPLINK.LEVEL3.MPLS ETHERNET, 20MBPS, CIRCUIT BCXO2005, 100 UTILIZATION OVER 98 THRESHOLD. DEVICE IP 10.241.57.83 NPM PRI3 NOTIFYINS KPI=		WAN	PRODUCTION	1503 NORTH CHARLESTON SC	unassigned	MONP-NPI
2017-03-31 12:01:15 EDT	00:47:01.0	IDMP-RMAD-1	critical	open	IDMP-RMAD-1.NBU.BACKUP.2215_IDMP_60D	NBU.BACKUP.2215_IDMP_60D A RECENT BACKUP FOR THIS SERVER HAS FAILED WITH AN EXIT STATUS=156. SCHEDULE NAME= START TIME=3/30/2017 8:00:00 PM POLICY NAME=2215_IDMP_60D NBUBACKUP.LOC=CAR KPINO		IDENTITY.MANAGEMENT	PRODUCTION	2079 CARROLLTON TX	unassigned	MONP-EMI
2017-03-31 03:07:01 EDT	09:41:15.0	EPSP-SEC01UK	critical	open	EPSP-SEC01UK.SERVICE.MCSHIELD	SERVICE.MCSHIELD IS DOWN. SPLUNK EPSP-SEC01UK EPSP-SEC01UK		UNKNOWN			unassigned	MONP-SPLUNKSH
2017-03-31 03:06:59 EDT	09:41:17.0	EPSP-SEC01UK	critical	open	EPSP-SEC01UK.SERVICE.MCTASKMANAGER	SERVICE.MCTASKMANAGER IS DOWN. SPLUNK EPSP-SEC01UK EPSP-SEC01UK		UNKNOWN			unassigned	MONP-SPLUNKSH
2017-03-30 23:07:43 EDT	13:40:33.0	CP-LEI-JOB	critical	open	CP-LEI-JOB.LEI.CONTRACTS.JOB.7.SINS	LEI CONTRACTS JOB 7 OF 7 SINS IS OVERDUE TO COMPLETE AUTOESC20 CONTACT ONCALL_CPRODONCALL		UNKNOWN			unassigned	DOMP-PMI
2017-03-30 22:43:26 EDT	14:04:50.0	CP-LEI-JOB	critical	open	CP-LEI-JOB.LEI.CONTRACTS.JOB.5.CUSTOMERS_CLASS2	LEI CONTRACTS JOB 5 OF 10 CUSTOMERS_CLASS2 IS OVERDUE TO COMPLETE AUTOESC10 CONTACT ONCALL_CPRODONCALL		UNKNOWN			unassigned	DOMP-PMI
2017-03-30 19:18:40 EDT	17:29:36.0	MD-0750-MDF40-U2	critical	open	MD-0750-MDF40-U2.NODEREACHABILITY	NODEREACHABILITY NODE STATUS IS DOWN. DEVICE NOT RESPONDING TO POLLS. DEVICE IP 10.35.200.7 NPM KPI=		UNKNOWN			unassigned	MONP-NPI
2017-03-30 04:01:20 EDT	1+08:46:56.0	NBUP-MASTER2	critical	open	NBUP-MASTER2.NBU.BACKUPVAULT_1YR	NBU.BACKUPVAULT_1YR A RECENT BACKUP FOR THIS SERVER HAS FAILED WITH AN EXIT STATUS=288. SCHEDULE NAME=VAULT START TIME=3/29/2017 11:00:00 AM POLICY NAME=VAULT_1YR NBUBACKUP LOC=UNK KPINO	INC0166603	NETBACKUP	PRODUCTION	2079 CARROLLTON TX	unassigned	MONP-EMI
2017-03-29 17:34:47 EDT	1+19:13:29.0	WITIQ-MAN01.DCS.LEIDOS.COM	critical	open	WITIQ-MAN01.DCS.LEIDOS.COM.WITIQ-MAN01.DCS.LEIDOS.COM.HOST.PCTAVAILABLE.VARLOG	WITIQ-MAN01.DCS.LEIDOS.COM.HOST.PCTAVAILABLE./VAR/LOG FILESYSTEM /VAR/LOG HAS 9.99 AVAILABLE SPACE, FALLEN BELOW WARNING (10) OR CRITICAL (5) THRESHOLD. OEM ONCALL_CPUNIXADM QA		WISDOM.ITI	QA	2072 LEWISVILLE, TX	unassigned	ORAPP-12
2017-03-27 23:01:41 EDT	3+13:46:35.0	CP-LEI-JOB	critical	open	CP-LEI-JOB.LEI	LEI CONTRACTS JOB 5 OF 7 VALUES_OPTIONS IS OVERDUE TO COMPLETE AUTOESC20 CONTACT ONCALL_CPRODONCALL		UNKNOWN			unassigned	DOMP-PMI

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



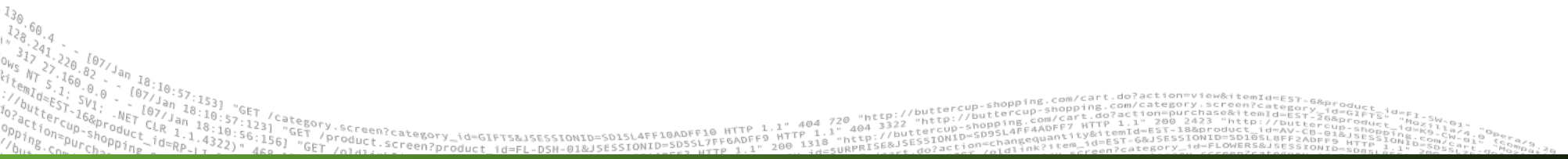
splunk> .conf2017

Thanks

Donald Mahler

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

Visit us at www.leidos.com



splunk> .conf2017

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, 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