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

Forward-Looking Statements

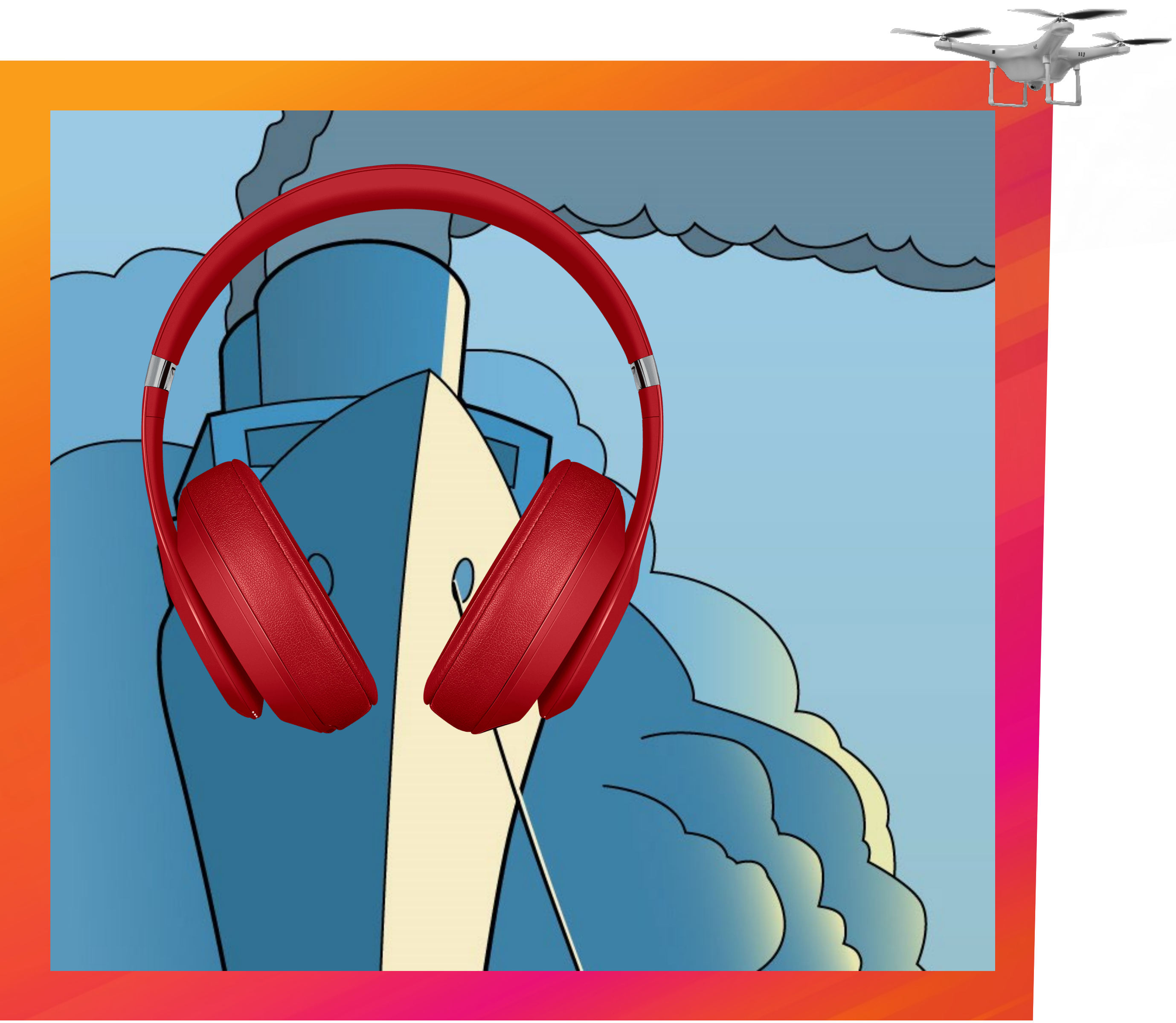
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the 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.

Mike McGrail

Sr. Infrastructure Specialist | Canada Life

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



PIZZA
PIZZA
PIZZA
A Splunktern's some kind of bird, right?

Agenda

INCLUDES NELLY, N.O.R.E., EVE FEATURING ALICIA KEYS, BEENIE MAN FEATURING JANET, DIRTY VEGAS,
KYLIE MINOGUE, SHAKIRA, NO DOUBT FEATURING LADY SAW, JENNIFER LOVE HEWITT,
VANESSA CARLTON, DIXIE CHICKS, AALIYAH, GINUWINE, NORAH JONES,
CHAD KROEGER FEATURING JOSEY SCOTT, HOOBASTANK, COLDPLAY, CREED, OUR LADY PEACE, BON JOVI
NOW
THAT'S WHAT I CALL MUSIC!
11
20 CHART-TOPPING HITS!

1) Background

💔

2) Why Splunk ITSI?

♡

3) Tech Deets

🤓

4) Where Are We Now?

👀

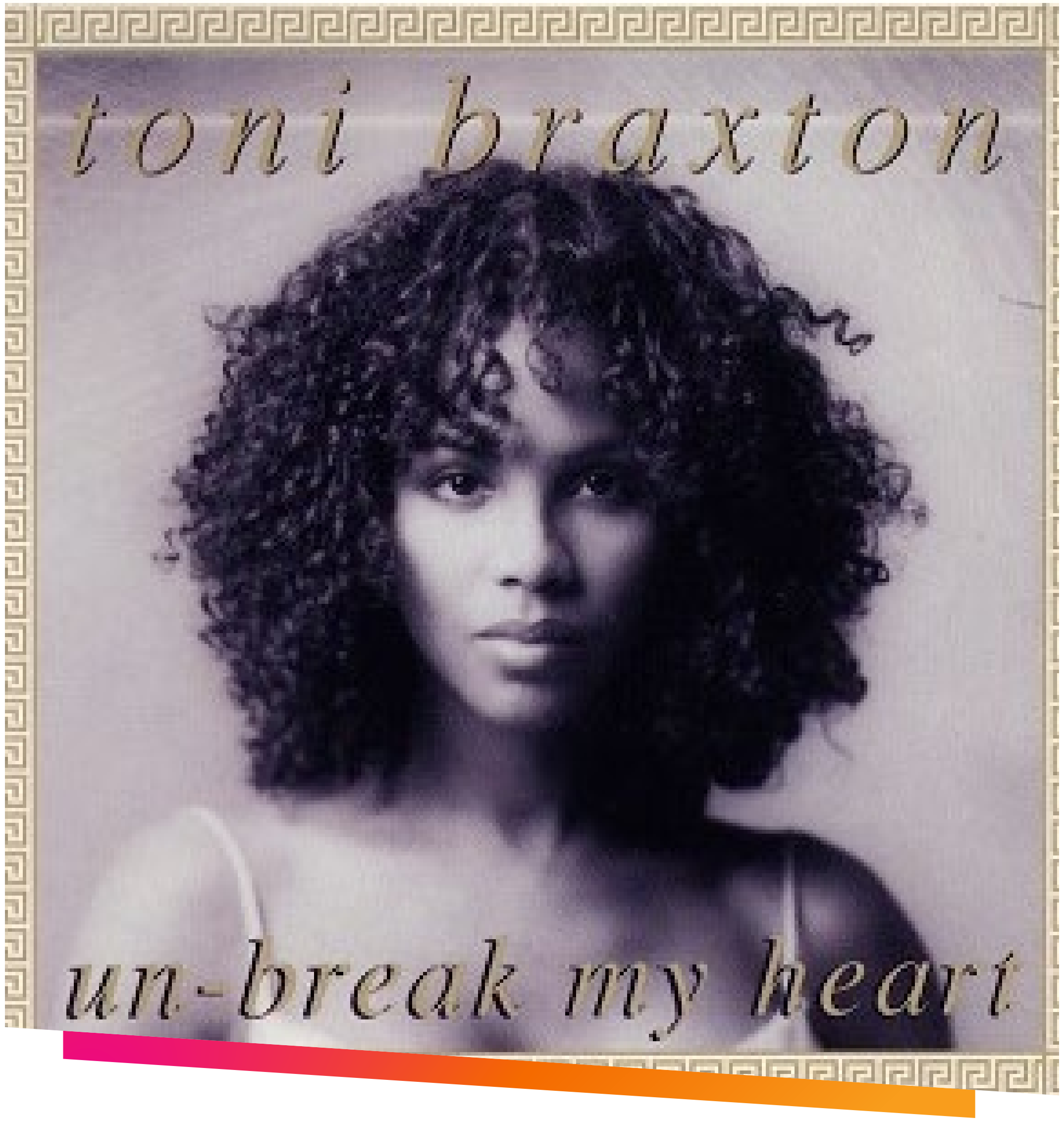
5) Where Are We Headed?

🧹

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

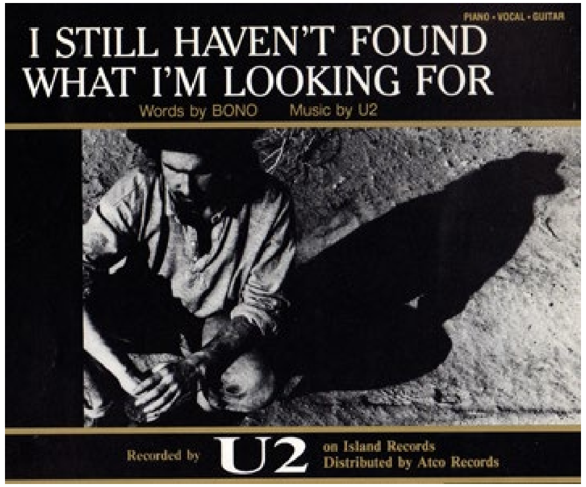


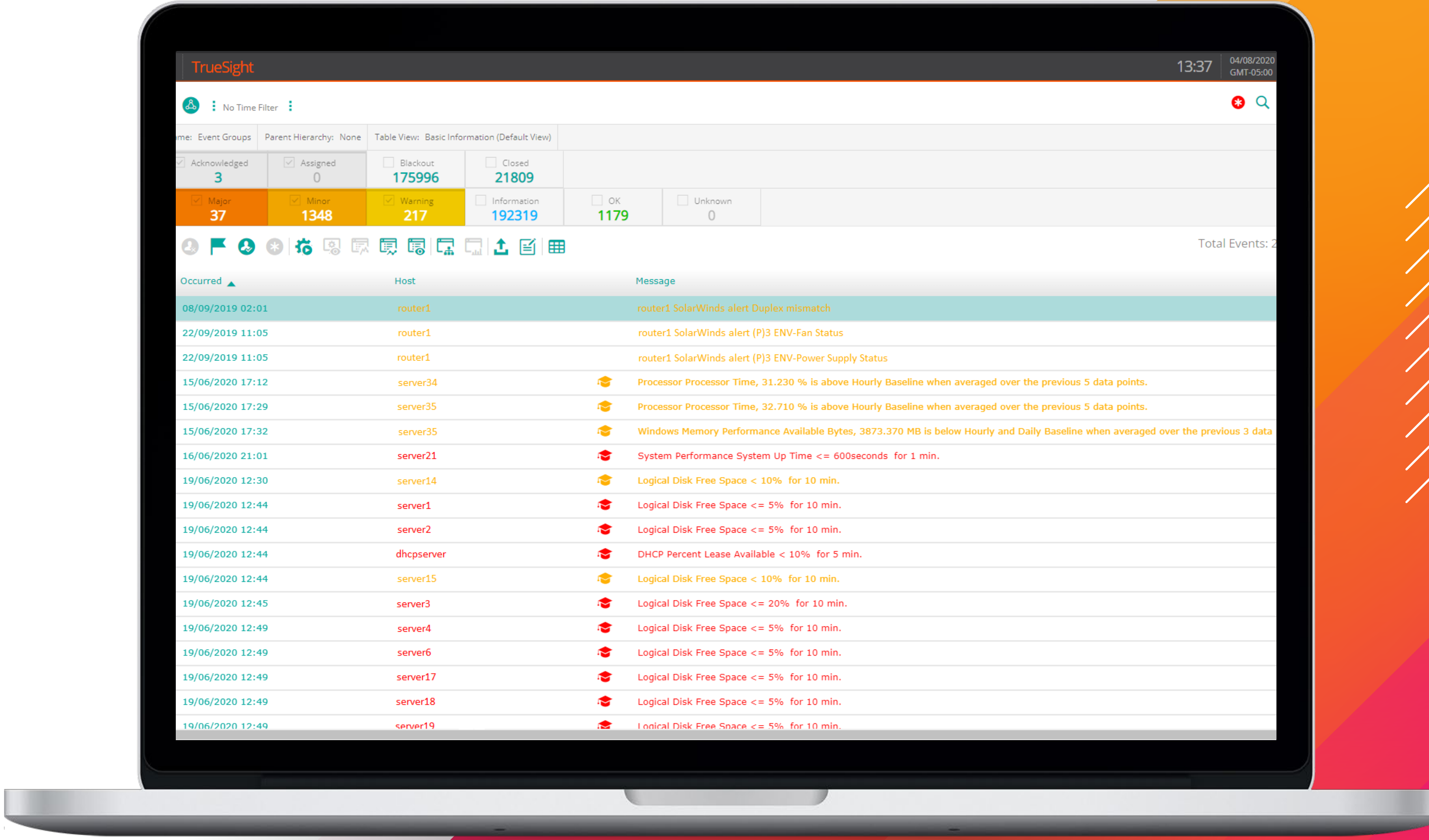
splunk> .conf20

Background

TrueSight events

Line by line


PIANO • VOCAL • GUITAR
I STILL HAVEN'T FOUND WHAT I'M LOOKING FOR
Words by BONO Music by U2
Recorded by U2 on Island Records
Distributed by Atco Records



me: Event Groups | Parent Hierarchy: None | Table View: Basic Information (Default View)

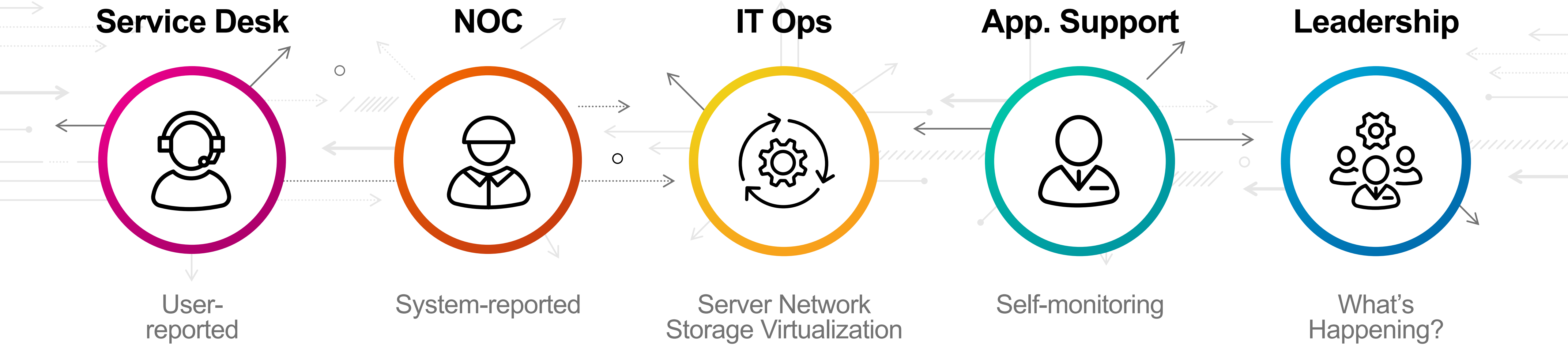
☑ Acknowledged	☑ Assigned	□ Blackout	□ Closed		
3	0	175996	21809		
☑ Major	☑ Minor	☑ Warning	□ Information	□ OK	□ Unknown
37	1348	217	192319	1179	0

Total Events: 2

Occurred ▲	Host	Message
08/09/2019 02:01	router1	router1 SolarWinds alert Duplex mismatch
22/09/2019 11:05	router1	router1 SolarWinds alert (P)3 ENV-Fan Status
22/09/2019 11:05	router1	router1 SolarWinds alert (P)3 ENV-Power Supply Status
15/06/2020 17:12	server34	Processor Processor Time, 31.230 % is above Hourly Baseline when averaged over the previous 5 data points.
15/06/2020 17:29	server35	Processor Processor Time, 32.710 % is above Hourly Baseline when averaged over the previous 5 data points.
15/06/2020 17:32	server35	Windows Memory Performance Available Bytes, 3873.370 MB is below Hourly and Daily Baseline when averaged over the previous 3 data
16/06/2020 21:01	server21	System Performance System Up Time <= 600seconds for 1 min.
19/06/2020 12:30	server14	Logical Disk Free Space < 10% for 10 min.
19/06/2020 12:44	server1	Logical Disk Free Space <= 5% for 10 min.
19/06/2020 12:44	server2	Logical Disk Free Space <= 5% for 10 min.
19/06/2020 12:44	dhcpserver	DHCP Percent Lease Available < 10% for 5 min.
19/06/2020 12:44	server15	Logical Disk Free Space < 10% for 10 min.
19/06/2020 12:45	server3	Logical Disk Free Space <= 20% for 10 min.
19/06/2020 12:49	server4	Logical Disk Free Space <= 5% for 10 min.
19/06/2020 12:49	server6	Logical Disk Free Space <= 5% for 10 min.
19/06/2020 12:49	server17	Logical Disk Free Space <= 5% for 10 min.
19/06/2020 12:49	server18	Logical Disk Free Space <= 5% for 10 min.
19/06/2020 12:49	server19	Logical Disk Free Space <= 5% for 10 min.

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

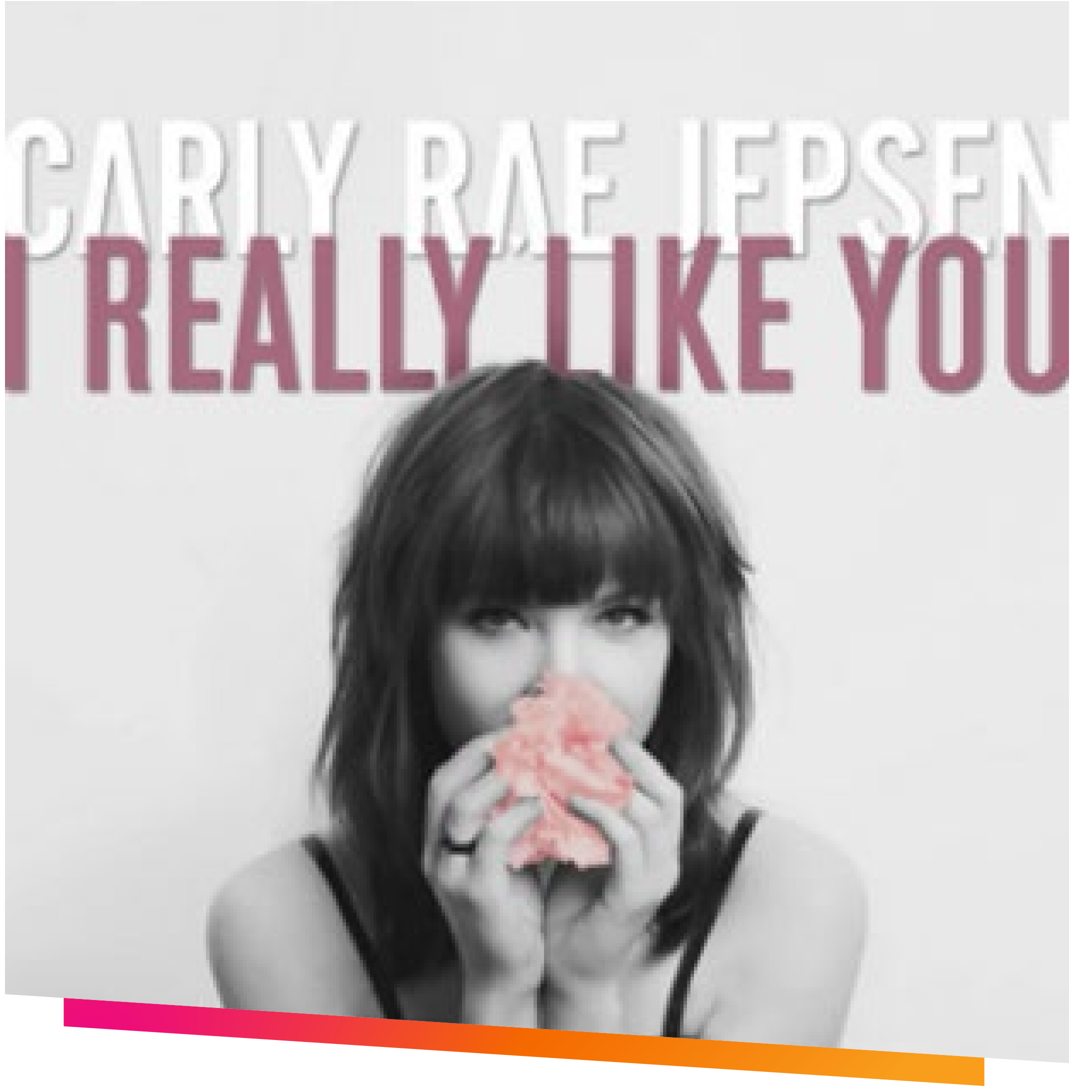
- Some users & data
- New use case ▶ infrastructure monitoring

POC Numerous AIOps Vendors

- Point solutions
- “TrueSight 2.0” ▶ same thing, new tool

ITSI

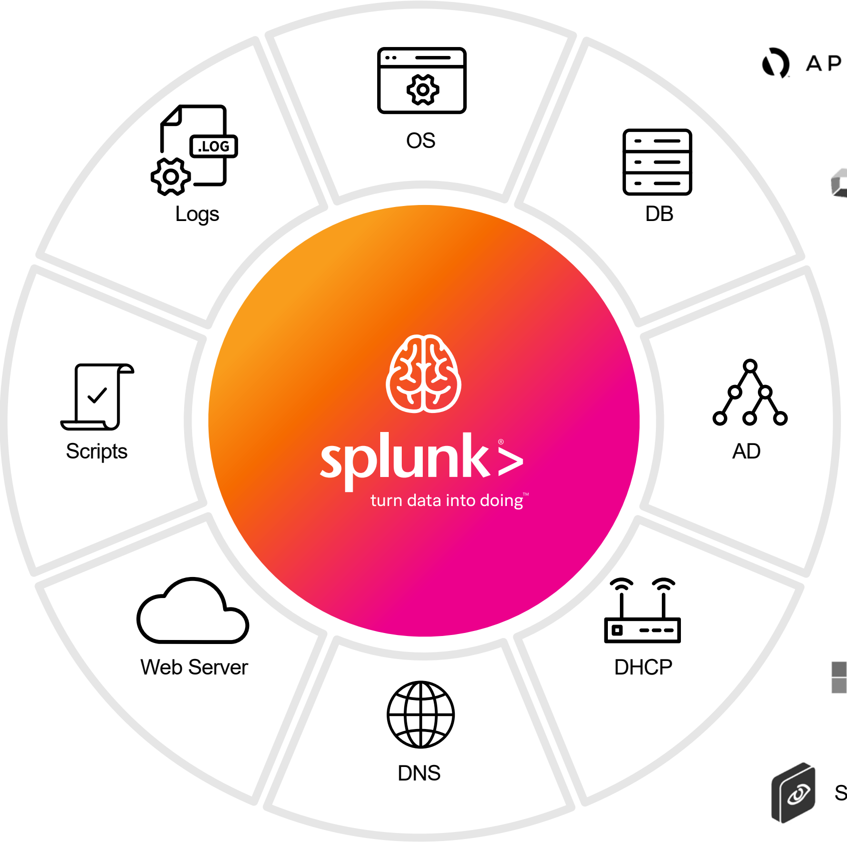
- Service analyzer ▶ green/yellow/red
- Glass tables
- Drill-down to Splunk viz.



splunk> .conf20

Tech Deets

Get data in



SB

APPDYNAMICS

dynatrace

solarwinds

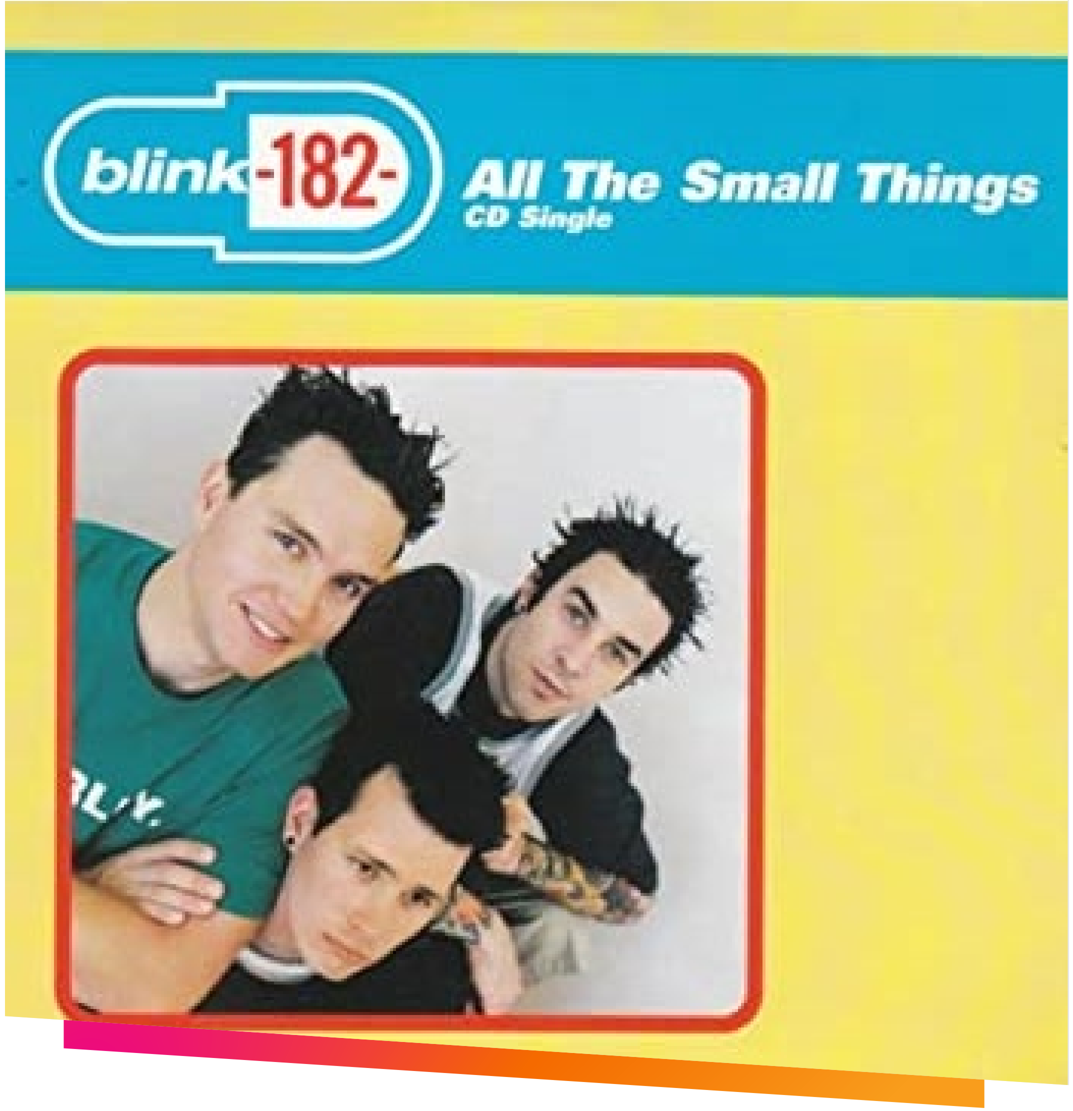
vmware

VMAX

proofpoint.

Microsoft 365

StruxureWare DCE



splunk> .conf20

Tech Deets

Environment

- Data globally visible when sensible
- Intermediate HF masking as necessary
- Summary indexes
  - Consolidated retention
  - Expose non-sensitive data subset

1.1
TB data

11
Indexers

6
Search heads
(2 clusters of 3)

81
Users

117
Concurrent searches

How Much Data?

Interval = 60 Seconds	Windows TA Metrics	Linux collectd Metrics	AIX *nix TA Events
OS performance	52 mb	87 mb	42 mb
Services	7.5 mb		
Domain Controller	1.2 gb		

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

.conf20

splunk>

Technical Debt Ahead

Lift and Shift TrueSight -> Splunk (fast)

No investment from other teams (non-invasive)

© 2020 SPLUNK INC.

Tech Deets

Lift & shift – search based

1 **Lookups**
Enrich data

2 **Core Splunk Search**
Output to custom summary index

3 **Correlation Search**
Query custom summary index, create episode

4 **NEAP**
Send alert to team

ts_env	ts_kpi	ts_entity	ts_instance	ts_support_team	ts_alert	ts_ticket	kba
prod	splunk_health	splunkserv*	*	Splunk Ninjas	1	0	KBA12345
prod	logicaldisk_free_percent	myserverabc*	*	Redmond	1	0	KBA45678
prod	status	splunkservice*	*	Application A Team	1	0	
prod	filesystem_used_percent	opt*	*	Bell Labs	1	0	
prod	security_violation	ADACCOUNT	*	Whoever Handles Active Directory	1	0	Nobody Knows
prod	cpu_utilization	myserverghi*	total_cpu	Bell Labs	0	1	
prod	error	server10	access_log	Application B Team	1	0	
prod	memory_available_megabytes	myserverjkl*	Memory	Redmond	1	0	
prod	memory_used_percent	myservermno*	total_memory	Tux Penguins	1	0	
non_prod	swap_used_percent	myserverpqr*	total_swap	Tux Penguins	1	0	
non_prod	system_uptime	myserverstu*	unix_os	Bell Labs	1	0	

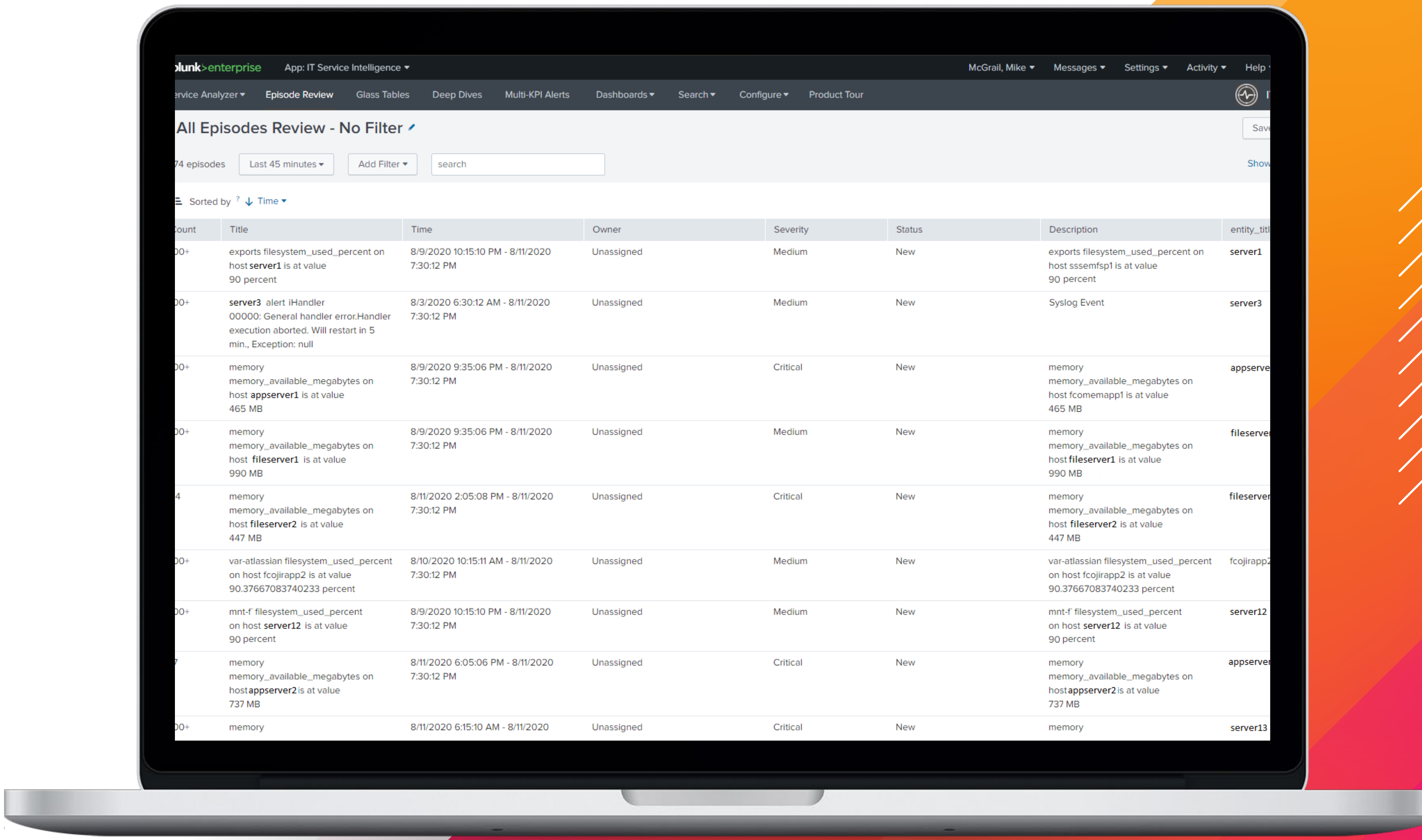
```
index=os sourcetype=cpu sourcetype=cpu cpu_instance=all
| fields cpu_load_percent host
| eval ts_instance="total_cpu",ts_kpi="cpu_utilization"
| stats avg(cpu_load_percent) as cpu_utilization
      latest(_time) as _time by ts_instance host ts_kpi
| where cpu_utilization>=95
| `ts_enrich_alert_details(host,ts_instance,ts_kpi)`
| 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)`
```

splunk> .conf20

Tech Deets

ITSI episodes

Lifted & shifted



All Episodes Review - No Filter

ount	Title	Time	Owner	Severity	Status	Description	entity_titl
00+	exports filesystem_used_percent on host **server1** is at value 90 percent	8/9/2020 10:15:10 PM - 8/11/2020 7:30:12 PM	Unassigned	Medium	New	exports filesystem_used_percent on host sssemfsp1 is at value 90 percent	server1
00+	**server3** alert iHandler 00000: General handler error.Handler execution aborted. Will restart in 5 min., Exception: null	8/3/2020 6:30:12 AM - 8/11/2020 7:30:12 PM	Unassigned	Medium	New	Syslog Event	server3
00+	memory memory_available_megabytes on host **appserver1** is at value 465 MB	8/9/2020 9:35:06 PM - 8/11/2020 7:30:12 PM	Unassigned	Critical	New	memory memory_available_megabytes on host fcomemapp1 is at value 465 MB	appserve
00+	memory memory_available_megabytes on host **fileserver1** is at value 990 MB	8/9/2020 9:35:06 PM - 8/11/2020 7:30:12 PM	Unassigned	Medium	New	memory memory_available_megabytes on host **fileserver1** is at value 990 MB	fileserve
4	memory memory_available_megabytes on host **fileserver2** is at value 447 MB	8/11/2020 2:05:08 PM - 8/11/2020 7:30:12 PM	Unassigned	Critical	New	memory memory_available_megabytes on host **fileserver2** is at value 447 MB	fileserver
00+	var-atlassian filesystem_used_percent on host fcojirapp2 is at value 90.37667083740233 percent	8/10/2020 10:15:11 AM - 8/11/2020 7:30:12 PM	Unassigned	Medium	New	var-atlassian filesystem_used_percent on host fcojirapp2 is at value 90.37667083740233 percent	fcojirapp2
00+	mnt-f filesystem_used_percent on host **server12** is at value 90 percent	8/9/2020 10:15:10 PM - 8/11/2020 7:30:12 PM	Unassigned	Medium	New	mnt-f filesystem_used_percent on host **server12** is at value 90 percent	server12
7	memory memory_available_megabytes on host**appserver2**is at value 737 MB	8/11/2020 6:05:06 PM - 8/11/2020 7:30:12 PM	Unassigned	Critical	New	memory memory_available_megabytes on host**appserver2**is at value 737 MB	appserver
00+	memory	8/11/2020 6:15:10 AM - 8/11/2020	Unassigned	Critical	New	memory	server13

Where Are We Now?

- All episodes & alerting through ITSI
- Decom. Patrol & TrueSight

368

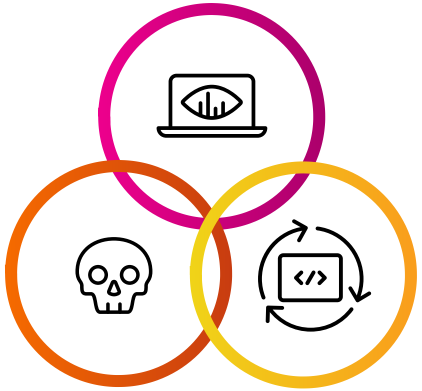
TrueSight Policies

33

Splunk Searches

Where Are We Headed?

Turn the ship



+ Services & KPIs

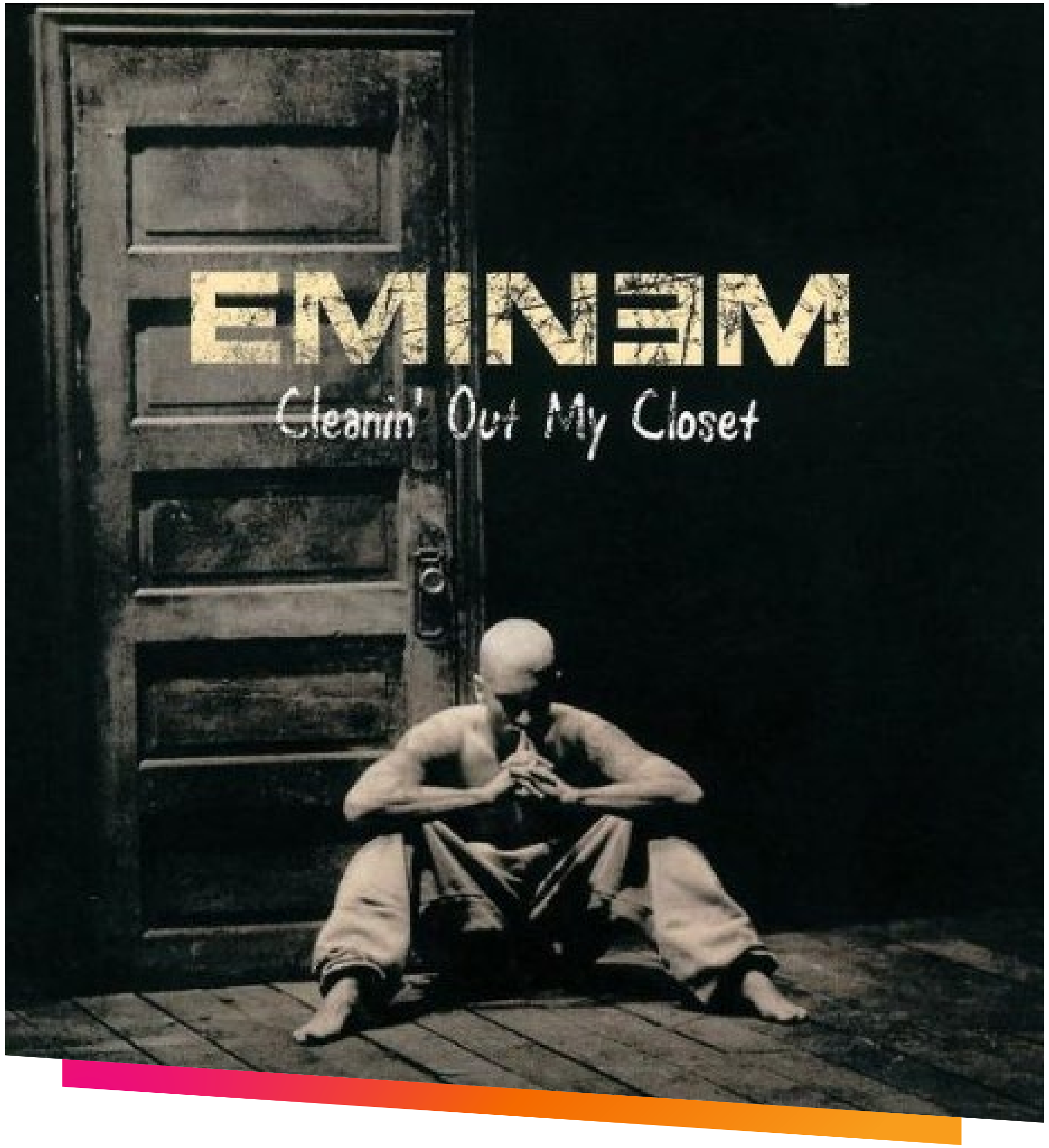
Visibility end silos

- Core Searches

complexity
contextless alerts

+ AIOps

adaptive thresholds
smart mode
data-driven decisions



splunk> .conf20

canada life™

splunk>®

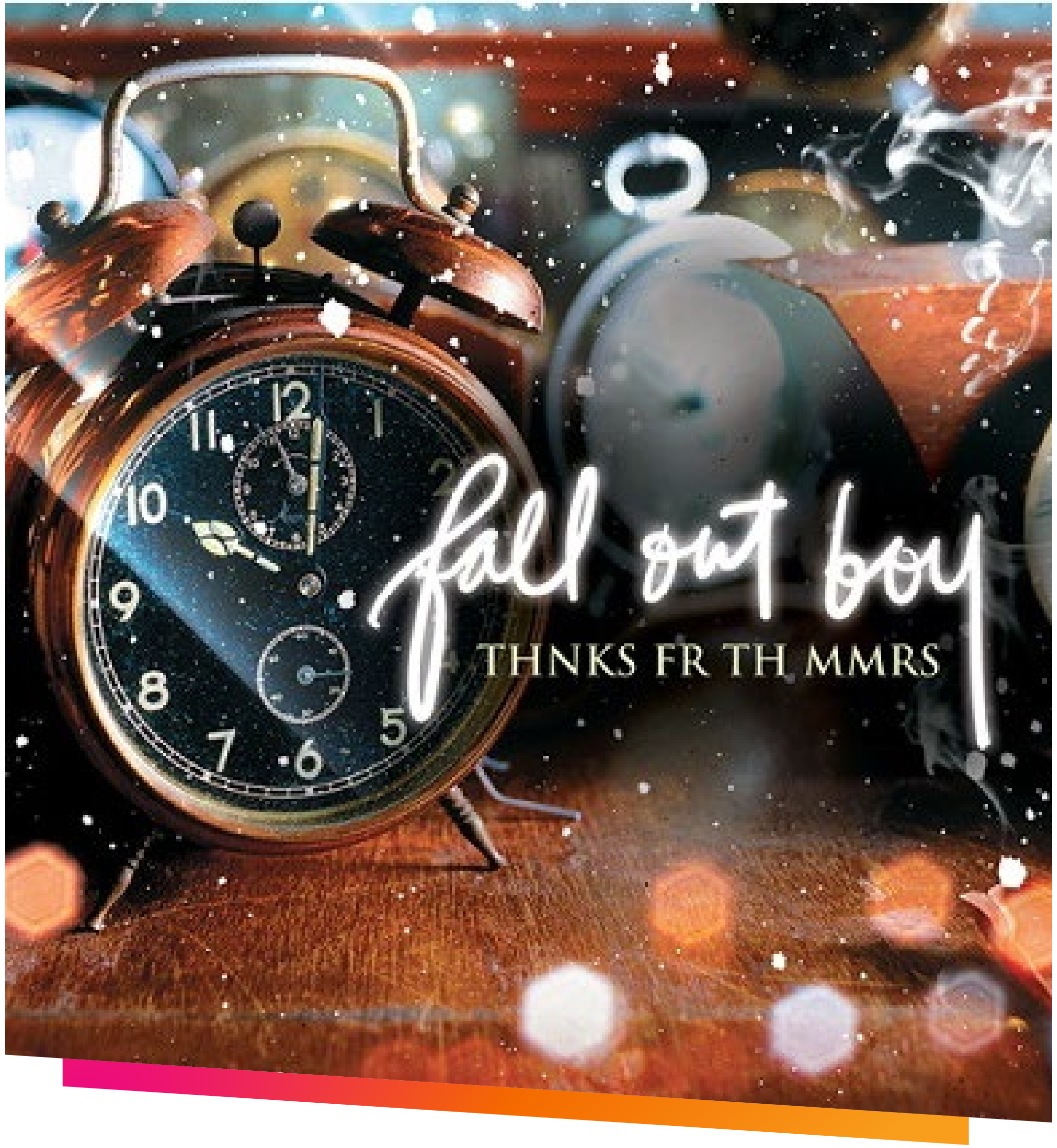


Image Credits

- Delp, David. (2011). Turning the Ship [Cartoon]. Pilot Fire. https://pilotfire.com/first-post-in-turning-a-big-ship-there%E2%80%99s-hope-for-us/.
- Now That's What I Call Music! 11. Universal, 2002.
- Toni Braxton. "Un-Break My Heart." Secrets. LaFace Records, 1996.
- U2. "I Still Haven't Found What I'm Looking For." The Joshua Tree. Island Records, 1987.
- Carly Rae Jepsen. "I Really Like You." Emotion. Interscope Records, 2015.
- Blink-182. "All The Small Things." Enema of the State. MCA Records, 1999.
- Bee Gees. "How Deep Is Your Love." Saturday Night Fever. Reprise Records, 1977.
- Green Day. "Warning." Warning. Reprise Records, 2000.
- Blue Swede. "Hooked on a Feeling." Hooked on a Feeling. EMI Records, 1974.
- Foreigner. "Feels Like The First Time." Foreigner. Atlantic Records, 1977.
- Eminem. "Cleanin' Out My Closet." The Eminem Show. Interscope Records, 2002.
- Fall Out Boy. "Thnks fr th Mmrs." Infinity on High. Island Records, 2007.

Thank You

Please provide feedback via the

SESSION SURVEY