Event Management Is Dead

Event Analytics Is Revolutionizing IT

David Millis | Splunk Staff Architect, IT Operations Analytics

September 26-28, 2017 | Washington, DC
Your Event Manager Is Driving In Circles

Time for a New Driver

David Millis | Splunk Staff Architect, IT Operations Analytics

September 26-28, 2017 | Washington, DC
Disclaimer

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.
But First, a Terminology Check
Terminology within the "Event Management" space is loose

- event, alert, notification, alarm, incident, time-series message, ...
- event mgr, element mgr, monitor, fault mgr, manager of managers, ...

We have to speak the same language

- at least during this session
Data Terms

"Event" - time-series message describing a change of state for a target entity

- often generated by a 3rd party entity
- usually includes target component (server17), alert description ("node is down"), state/status/severity ("down")
- **NOTE**: This is different than most Splunkers think of an "event"

"Logged Data" - time-series message from an entity, describing something that occurred to the entity itself

- app log, O/S log, win-event, syslog (usually)
"Metric Data" - time-series message with a performance value. Usually a number.

- Collected on a regular basis (every minute, every 15 minutes, etc)
- "CPU % usage", "Filesystem capacity", "Interface bytes received"

"Wire Data" - time-series message collected indirectly by capturing raw network traffic "off the wire".

- Often metrics
- Splunk Stream, wireshark, etc
"Time-Series Data" - The stuff that Splunk indexes
  • Formerly called "events" by many Splunkers
  • Includes all of the previous data types

"Notable Event" - an actionable message
  • intended specifically for humans in Operations
  • Splunk ITSI & ES

"Incident" - Unplanned interruption or reduction in quality of an IT or Business service
  • Service Now, Remedy
Other Terms

- "Event Manager" - monitors stuff and spews "events"
- "Element Manager"
- "Monitor"

- "Manager of Managers" - a tool which correlates events
- "Fault Manager"

- "AI Ops" - The Latest Thing, uses Machine Learning

- "Event Analytics" - Splunk's vision for next-gen IT Ops
IT Operations' Mission:

Find What's Broken, then Fix It
A Brief History of Event Management

Remind Me: Why Are We Doing This?
A long time ago, there were very few events and they mostly came directly from a few large computers. The IT Folks could handle it.
But the Rate of Events Began Increasing
But the Rate of Events Began Increasing

SNMP Traps

App Errors

Host Events

Syslog

Until the IT folks couldn't handle it
The Event Manager is Born

- SNMP Traps
- App Errors
- Host Events
- Syslog

Server 5 is down

The IT Folks could handle it, again
... along with the IT Silo!

Server5 is down

SNMP Traps
App Errors
Host Events
Syslog
But the Rate of Events Kept Going Up

Event Mgr Events
SNMP Traps
App Errors
Host Events
Syslog

and Event Managers Multiplied
MoM to the Rescue

Event Mgr Events
SNMP Traps
App Errors
Host Events
Syslog

More Filtering & Reducing
Environments Became More Complex
Environments Became More Complex

Network
Environments Became More Complex

Virtualization

Network
Environments Became More Complex
Environments Became More Complex

Cloud
Virtualization
Storage
Network
Environments Became More Complex

Highly Available
Environments Became More Complex

Highly Available

On Demand
Environments Became More Complex

- Highly Available
- On Demand
- * As a Service
Environments Became More Complex

- Highly Available
- On Demand
- Software Defined
- As a Service
And the number of Events increased--
... Exponentially
When a component fails in such an environment, what does it even mean?
When a component fails in such an environment, How does it affect the Bottom Line?
A Story about Denver Traffic

Managing Events is Lot Like Managing Vehicles
Welcome to the Vehicle Operations Center (VOC)
We Just Received 11 Car-Won't-Start events

Which one should we handle first?
Machine Learning identifies a cluster!
Machine Learning identifies a cluster!

Which isn't particularly interesting: it's raining in that area.
Let's Apply Context:

5 of the Car-Won't-Start Vehicles are in House Garages
Let's Apply Context:

4 of the Car-Won't-Start Vehicles are in Parking Lots
1 of the Car-Won't-Start Vehicles is in a Mechanic's Shop
1 of the Car-Won't-Start Vehicles is in the Middle Lane of Interstate-25
Which One Should We Handle First?
(Service) Context is Everything!
What Are the Important Services?
What Are the Important Services?

- Mail & Package Delivery
What Are the Important Services?

- Mail & Package Delivery
- Mass Transit
What Are the Important Services?

- Mail & Package Delivery
- Mass Transit
- Emergency Services
What Are the Important Services?

- Mail & Package Delivery
- Mass Transit
- Emergency Services
- Pizza Delivery
What Are the Important Services?

- Mail & Package Delivery
- Mass Transit
- Emergency Services
- Pizza Delivery
- Interstate Highway
Interstate Highway Service
Creative KPIs allow us to move beyond traditional events

- KPI: Average vehicle speed (metric data)
- KPI: Vehicle throughput (wire data)
- KPI: Count of 911 calls tagged with "Interstate-25" (logged data)

Machine Learning–based thresholding allows us to see "normal" vs "not normal"

- Slower vehicle speeds during rush hour are normal
Notable Events at Human Scale
Notable Events at Human Scale

1000s to 100s – Events with important service contexts
Notable Events at Human Scale

100s to Dozens – Events within the specific service context of interest
Notable Events at Human Scale

Dozens to Handfuls – Use ML to find "not normal" within this specific service context.
The Old IT Ways Don't Work Anymore
The Old IT Ways Don't Work Anymore

• Event Fatigue
The Old IT Ways Don't Work Anymore

- Event Fatigue
- Complex Environments
The Old IT Ways Don't Work Anymore

- Event Fatigue
- Complex Environments
- Components multiply, Silos abound
Help!

▶ Which busted components should we focus on?
▶ When a component fails in such a complex environment, what does it even mean?
▶ What important services are impacted, if any?
▶ How do we identify those failures which are actually impacting the business -- customers, clients & revenue?
Machine Learning Won't Save Us

- ML is the latest approach to magically reduce the huge volume to find that "elusive root cause event"

- ML is a powerful new capability which can be useful, but...

- ML alone will not solve our fundamental problems

- Without a service context, adding ML to the old deluge of events isn't enough
A Better Way: Splunk ITSI for Event Analytics
Apply a Flexible Service Context

Focusing on High Value Services
Apply a Flexible Service Context
Focusing on High Value Services

- Customer Purchases
Apply a Flexible Service Context

Focusing on High Value Services

- Customer Purchases
- Financial Transactions
Apply a Flexible Service Context
Focusing on High Value Services

- Customer Purchases
- Financial Transactions
- Claims Processing
Use All the Data—At Scale

• No more filtering, reducing
Use All the Data—At Scale

- No more filtering, reducing
- Use all types of data:
  - Traditional events
Use All the Data—At Scale

- No more filtering, reducing
- Use all types of data:
  - Traditional events
  - Metrics
Use All the Data—At Scale

- No more filtering, reducing
- Use all types of data:
  - Traditional events
  - Metrics
  - Wire data
Use All the Data—At Scale

- No more filtering, reducing
- Use all types of data:
  - Traditional events
  - Metrics
  - Wire data
- "OK" & "Not OK" info
Dealing with Gigabytes is easy

Must be able to handle Terabytes and even Petabytes per day

If You Can't Scale, You'll Fail
Use Machine Learning the Right Way
Use Machine Learning the Right Way

- At Every Step
- On All Types of Data
Use Machine Learning the Right Way

• At Every Step
• On All Types of Data
• From High vs Low to Normal vs Not Normal
Use Machine Learning the Right Way

- At Every Step
- On All Types of Data
- From High vs Low to Normal vs Not Normal
- Move Beyond Alerts
Use Machine Learning the Right Way

- At Every Step
- On All Types of Data
- From High vs Low to Normal vs Not Normal
- Move Beyond Alerts
- Get Proactive
Let's Drive!
Life Gets Better for IT Ops

- Reduce complexity
- Produce Human-Scale, Prioritized, Actionable events
- Improve MTTR
- Simplify Operations
Empower IT Ops to

Find What's Broken, then Fix It
Thank You

Don't forget to rate this session in the .conf2017 mobile app

David Millis | dmillis@splunk.com