Splunk and IT Service Intelligence

SIG-NOC, 27th November 2017

Graham Parsons, Operations Specialist
Splunk turns machine data into answers

Splunk’s trusted analytics platform empowers people to dive into their machine data so they can find answers quickly and see opportunities in real-time.
What is Machine Data?

- **Flight and airport data**
  American Airlines operates 6,700 flights daily to 350 destinations

- **Customer generated data**
  Airlines can get more than 15,000 tweets a day

- **Back office data**
  The support systems used to run the business i.e. HR software

- **Baggage data**
  Airlines check >150M bags per year, many with RFID sensors

- **Device data**
  A Boeing 737 produces 20 TB of data per hour
Nearly All the Answers You Need Are In Your Machine Data
OUR MISSION

Making machine data accessible, usable and valuable to everyone.
Machine Learning with Machine Data Unlocks Even More Value

Security | IT Ops | Network Ops | IoT
AI, Deep Learning, And Machine Learning

- Sentient Machines
- Intelligent Agents
- No Human Involvement
- Guided Data Driven Decisions
- Augmenting Human Reasoning
- Operational Intelligence
- Tensorflow
- Data sets are large and unknowable
- Neural Networks

Splunk ML offerings today
Splunk Positioned as a Leader
IDC Worldwide IT Operations Analytics Software*

- Market share leader in first IDC ITOA report
- Predictive analytics, anomaly detection, business impact analysis
- Recommended for variety & volume of data, use case breadth, pre-packaged content, visualizations and data management.

Splunk Positioned as a Leader
Gartner 2016 Magic Quadrant for Security Information and Event Management*

▶ Four Years in a Row as a Leader
▶ Furthest overall in Completeness of Vision
▶ Splunk also scores highest in 2016 Critical Capabilities for SIEM report in all three Use Cases

*Gartner, Inc., 2016 Magic Quadrant for Security Information and Event Management, and Critical Capabilities for Security Information and Event Management, Oliver Rochford, Kelly M. Kavanagh, Toby Busa. 10 August 2016 This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Splunk. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Splunk IT Service Intelligence
Splunk IT Service Intelligence

Data-driven service monitoring and analytics

Dynamic Service Models
At-a-Glance Problem Analysis
Early Warning on Deviations
Event Analytics
Simplified Incident Workflows

SPLUNK IT SERVICE INTELLIGENCE

Platform for Machine Data

Time-Series Index
Schema-on-Read
Data Model
Common Information Model
Splunk IT Service Intelligence

Data-driven service monitoring and analytics

Dynamic Service Models
At-a-Glance Problem Analysis
Early Warning on Deviations
Event Analytics
Simplified Incident Workflows

SPLUNK IT SERVICE INTELLIGENCE

Platform for Machine Data

Time-Series Index
Schema-on-Read
Data Model
Common Information Model

© 2017 SPLUNK INC.
Delivering Consistent Outcomes

- Improve Customer Experience
- Provide End-to-End Visibility
- Decrease Incidents and MTTR
- Redeploy IT Effort to Proactive Tasks

Common IT Operational Analytics Outcomes (2000+ Customers Analysed, 300+ with ITSI)

- **30%-45%** Proactive reduction in No of incidents
- **70%-90%** Faster Incident Investigation (MTTI) & resolution (MTTR)
- **55%-75%** Automation of low value manual IT tasks
- **55%-70%** Reduction of Financial Impact associated to outages
- **10%-15%** Increase in Optimization of Hardware Capacity
- **65%-85%** Effort reduction associated with Root Cause Analysis

SPLUNK IT SERVICE INTELLIGENCE

Customer Facing Data
- Windows
- Log files
- Linux/Unix
- Configs
- Messages
- Virtualization & Cloud
- Traps
- Alerts
- Metrics
- Applications
- Scripts
- Changes
- Databases
- Tickets

Outside the Datacenter

Networking
**ITSI Terminology**

**Logical grouping of operations**
- Online banking
- Authentication
- Virtualization

**Set of actions performed with specific business goals**
- Sell products
- Fulfill orders
- Process payroll

**Component required to deliver a service**
- Hosts
- Users
- OS Processes

**Metrics used to evaluate success**
- Service health
- Order revenue
- Latency
The Possibilities:
IT Glass Tables
Federal Credit Union - Glass table
Sterling Metrics

Data Services Health Score: 80
Authentication Health Score: 58.6
Response Time Health Score: 80
Deposits Health Score: 80

DANGER ZONE

- Hourly Deposits Sum: 172k
- Response Time: 0.308 sec
- Beta Response Time: 0.369 sec
- Response Time: 16
- Authentication: 67
- Deposits: 2k
The Possibilities: Business Glass Tables
Healthcare Service Delivery Overview

HEALTHCARE DELIVERY SCORECARD

OVERALL STATUS

CARE PATHWAYS

TERTIARY SERVICES

TERTIARY SERVICES

SPECIALIST SERVICES

SPECIALIST SERVICES

HOSPITAL STATUS LAST 7 DAYS
ER Patient Journey

Emergency Patient Visits: 9

Triage: 23

Treatment Wait Time: 0

Blood Test: 108

Pathology Wait Times: 0

X-Ray: 31

Treatment: 13

Prescriptions: 130

Pharmacy Dispensing: 74

Discharge: 130
Demo
A lot of companies are using their machine data...
Thank You!

Any questions?

gparsons@splunk.com