Break Down Silos

Ingesting Multi Purpose Data in Splunk

10-24-2019

Ben Marcus | Sr. Staff Engineer | Qualcomm

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.

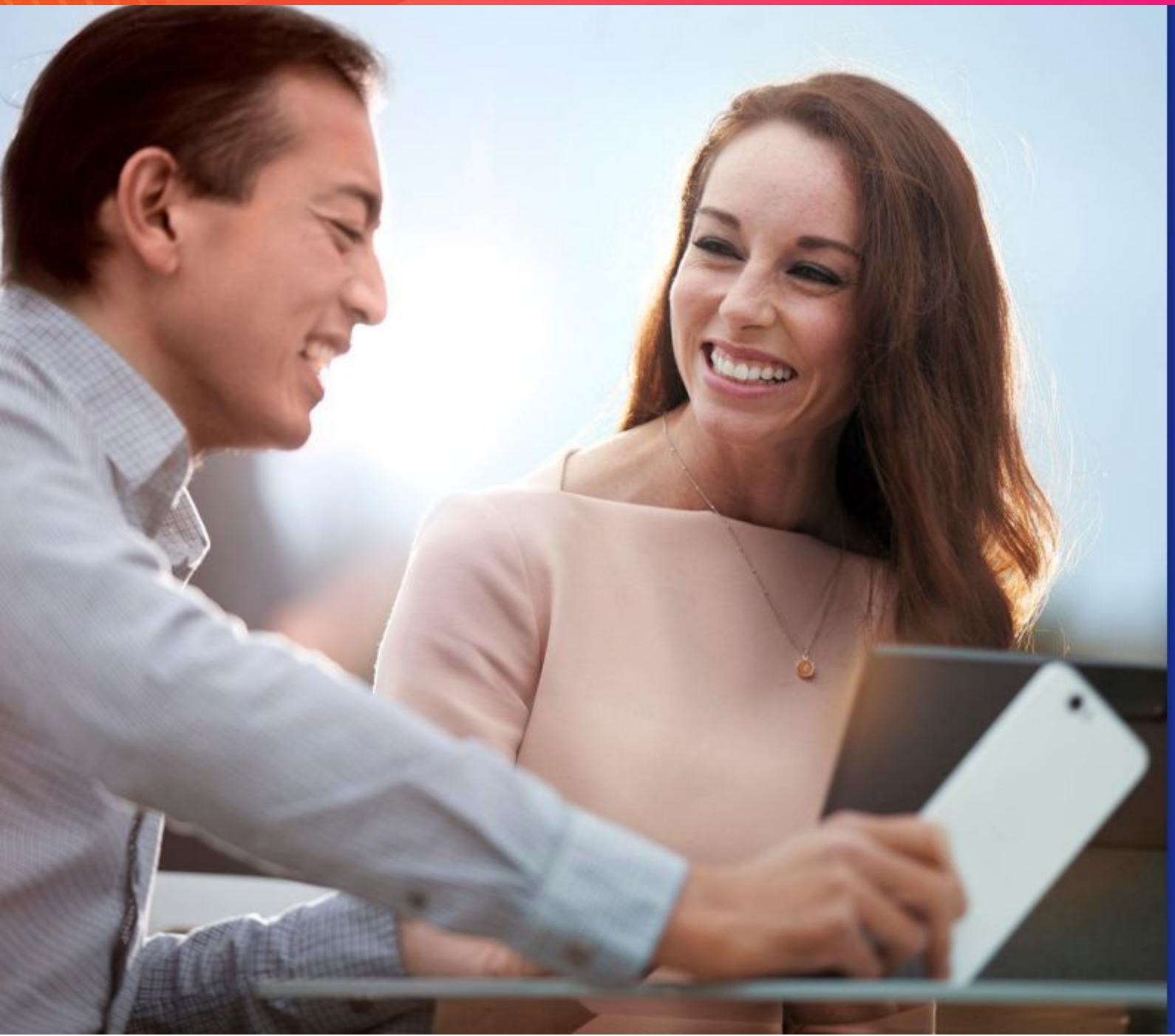
Introduction

splunk> .conf19

BEN MARCUS

Software Engineer
Large Scale System Administrator
10+ years using Splunk
https://www.linkedin.com/in/heybigben

splunk> .conf19



Qualcomm

#1

Fabless semiconductor company

#1

In 3G/4G LTE modem

30+

Years of driving the evolution of wireless

804M

MSM™ chipsets shipped FY ‘17

Sources: Qualcomm Incorporated data, as of Q4 FY17; IHS, May ’18; Strategy Analytics, Mar. ’18. MSM is a product of Qualcomm Technologies, Inc. and/or its subsidiaries.

Leading mobile innovation for over 30 years

Digitized mobile communications

Analog to digital

Redefined computing

Desktop to smartphones

Transforming industries

Connecting virtually everything

Redefining how the world connects, computes and communicates

Engineering Design Center Infrastructure Overview

Large and Complex

Large numbers of just about everything

- Compute servers globally connected
- Storage (thousands of mount points/volumes)
- Directory Services (LDAP and AD)
- Job Scheduling Software
- Revision Control Systems
- Tool License Servers
- Virtual Desktop Infrastructure
- Remote Display Software

Visibility

Logs + Metrics + Services = Answers

Linux Syslogs

Sudo
Syslog
Auditd

Application Logs

Webserver
Revision Control
Job Scheduler
Database
LDAP
DNS
Build System
Config

Appliance Logs

Storage
VMware
Load Balancer
Firewall
VPN
Router
NTP
Web Proxy

Server Management Logs

HP ILO
HP VC
HP OA
Dell IDrac

Linux Server Metrics

Memory
CPU
Network
Collectd
Telegraf
OSQuery

Multi Purpose Data Sources

Examples that span multiple use cases and business units

splunk> .conf19

HP ILO Syslogs

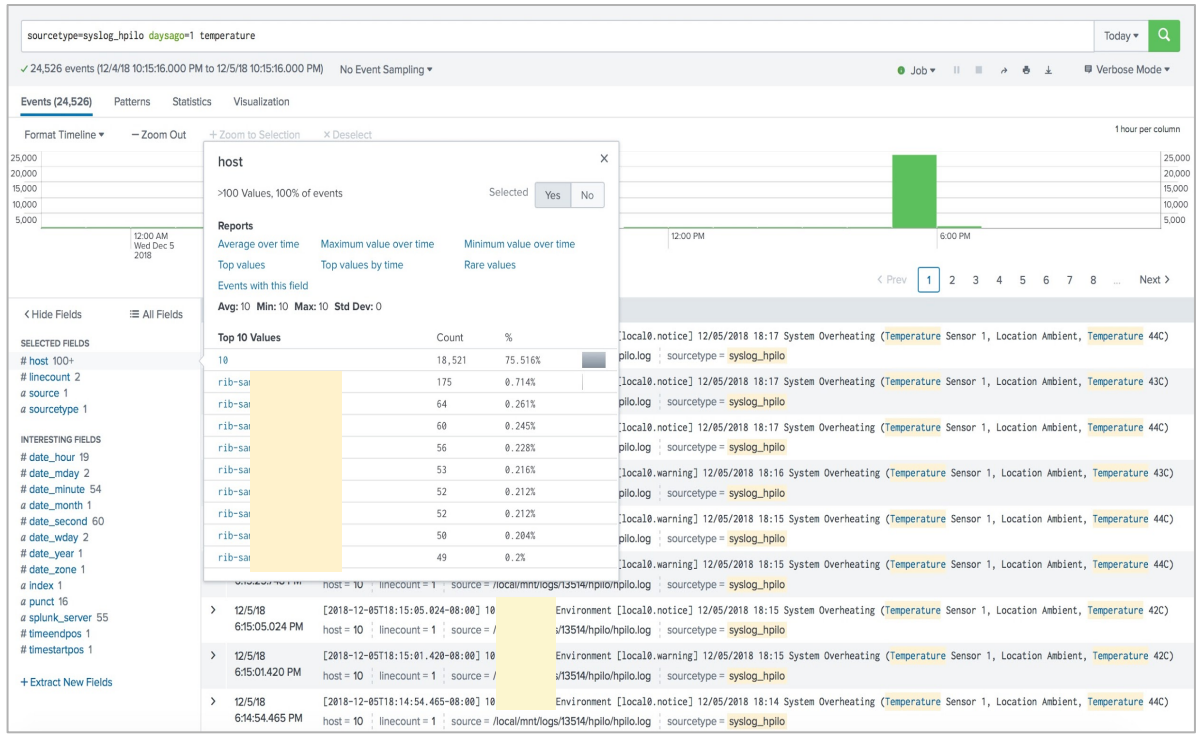
Server Administrators & Data Center Team

Use Cases: **Server Administrators**

- Monitoring servers for hardware issues (broken fans, disk drives, memory)

Use Cases: **Data Center Team**

- Overheating servers in datacenters
- Impacted hosts



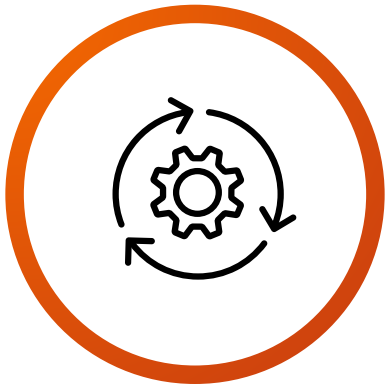
Firewall Logs

Multi Purpose Benefits

Security

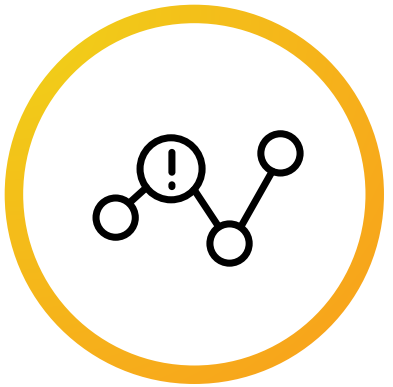
Original Use Case
Traffic Policies

Operations



Use Case:
Bringing up a new site
Servers would not image
Firewall logs showed DNS blocked

Network



Use Case:
Traffic Patterns

Netstat

Use Cases: System Operations

Use Cases: **System Operations**

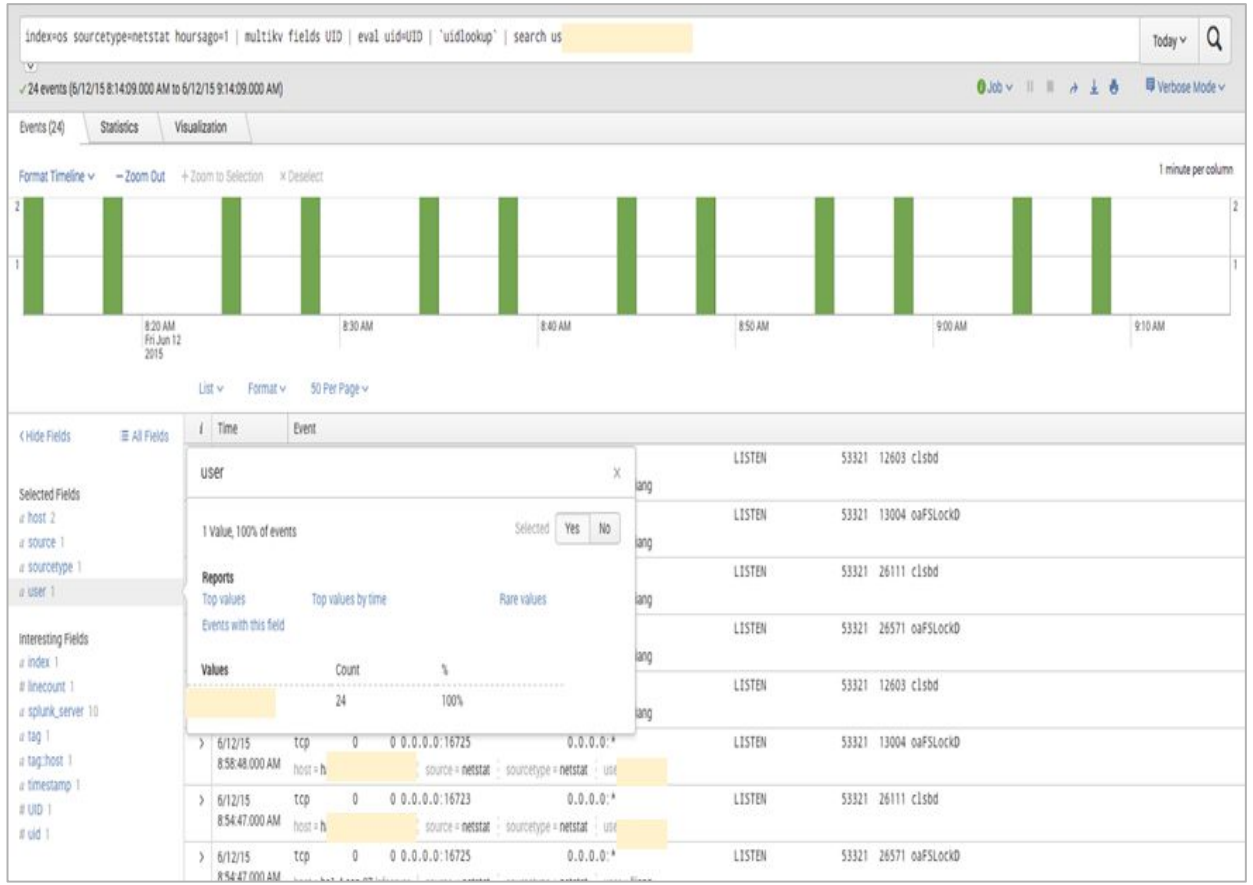
- Debug programs and associated sockets

Use Cases: **Security**

- What hosts are connecting to other hosts?

Use Cases: **Finance**

- Long running jobs to license servers
- Save $$$



splunk> .conf19

DNS

Security & IT Operations

Use Cases: **Security**

- Improve command and control
- Track DNS client requests & zone transfers

Use Cases: **IT Operations**

- Avoided outages by finding misconfigured hosts
- Decommissioning DNS servers without client downtime
- Improved incident resolution with job scheduler

NFSMountStat

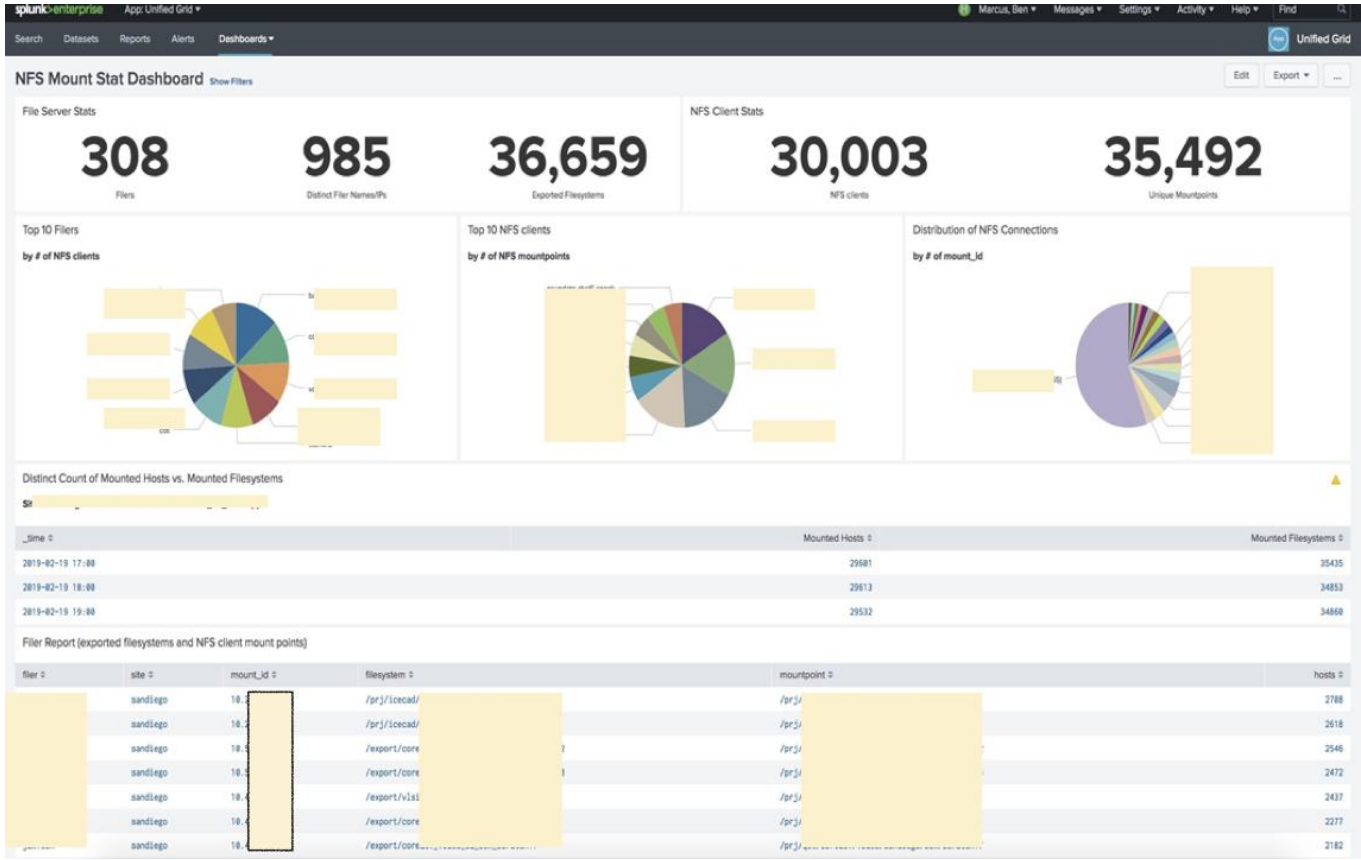
Use Cases: IT Operations (Storage)

Use Cases: **IT Operations (Storage)**

- Identify hosts affected by storage outages

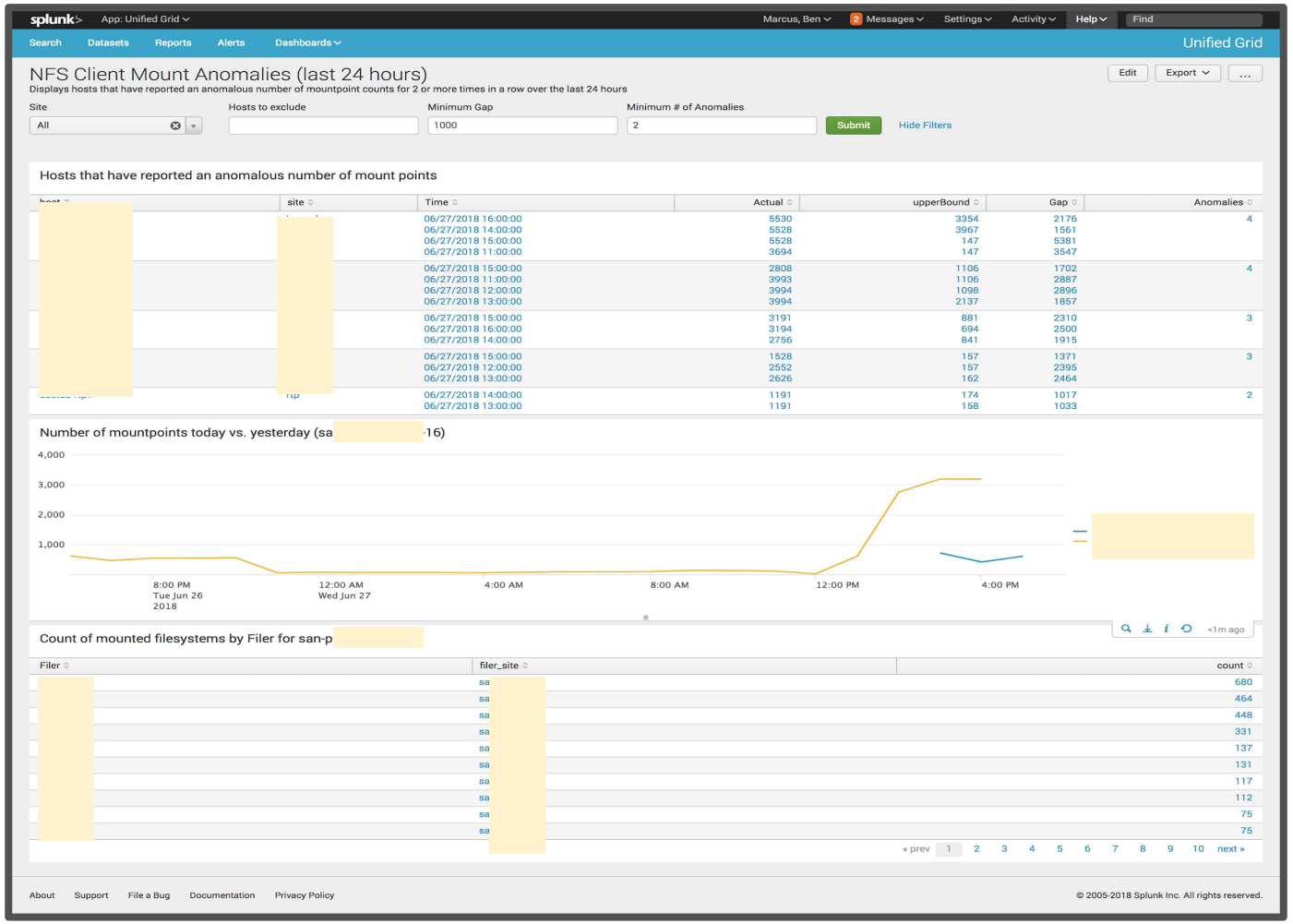
Use Cases: **Security**

- Anomaly Dashboard
- User mounting many paths
- Cross site/region mounting



NFS Mount Screen Shot

Anomaly Dashboard for Security & Operations



splunk> .conf19

NFS: Cross site example

Security

50 Per Page ▾ Format ▾ Preview ▾ < Prev 1 2 Next >

	lsf_filer	mount	lsfcluster	DistinctUsers	user	count
1	sandiego:lasvegas	/prj	CRD	1		4865
2	sandiego:lasvegas	/prj	CRD ICEng	1		3537
3	sandiego:rtp	/prj	ICEng	18		3004
4	sandiego:lasvegas	/prj	CRD ICEng	3		1264
5	sandiego:lasvegas	/prj	CRD	2		1209
6	sandiego:santaclara	/prj	GBC ICEng	3		1122
7	encnaa:rtp	/prj	GRIDECDCA	5		942
8	sandiego:lasvegas	/prj	CRD	3		572

Netflow

Networking

Use Case:

User Activity Insight

Grid

Use Case:

User Activity Insight

Security

Use Case:

Data Protection

Traffic for Protocol 6 (tcp) reported by 1[redacted] IP/Host Name

1m ago

Source IP	Source Host	Source Port	Destination IP	Destination Host	Destination Port	Max Mbps	Average Mbps	Total Traffic MB	% of Total	Average Packets/s	Total Packets	Conne
[redacted]	linux[redacted]	47658/tcp (unknown)	10.[redacted]	unknown	22/tcp (ssh)	5,289.38	72.36	31,054.13	3.19	6,332.41	22,796,667	
[redacted]	cron-[redacted]	60385/tcp (unknown)	10.[redacted]	[redacted]	22/tcp (ssh)	2,780.16	40.11	17,214.12	1.77	3,385.84	12,189,027	

splunk> .conf19

Filer audit data

Storage Admins & Security & Grid Admins

Use Cases: **Storage Admins**

- Determining who deleted files

_time	filer	action	type	path	uidresolved	client
2019-09-05T08::	C	Del	FILE	/usr2/cX_0016/userx/..tool/mcr_v92/.deploy_lock.339	613	10.x
2019-09-05T08::	C	Add	FILE	/usr2/cXt_0044/usery/..tool/mcr_v85/.deploy_lock.663	713	10.x
2019-09-05T08::	C	Ren	FILE	/usr2/cX_0044/usery/..tool/mcr_v85/b.settings.tmp	82285	10.x
2019-09-05T08::	C	Del	FILE	/usr2/cX_0082/userr/..tool/mcr_v85/.deploy_lock.164	316269	10.x
2019-09-05T08::	C	Add	FILE	/usr2/cX_0044/usery/..tool/mcr_v85/.deploy_lock.206	382285	10.x
2019-09-05T08::	C	Del	FILE	/usr2/cX_0051/userz/..tool/mcr_v92/.deploy_lock.220	1242	10.x
2019-09-05T08::	C	Del	FILE	/usr2/cX_0051/userv/..tool/mcr_v92/.deploy_lock.49	1242	10.x

Use Cases: **Security**

- Who is accessing files?

Use Cases: **Grid Admins**

- Tool information – running IO intensive workloads in home directories

Remote Display Software

Operations & Finance & Security

Use Cases: **IT Operations (Remote Display)**

- Track remote users login in

Use Cases: **Security**

- Who was accessing the system and how

Use Cases: **Finance**

- Tie license usage to department
- License renewal

1	User authenticated using user credentials. Client origin: 10.	5056. Windows username	lient type:	Client version:	SSL protocol: TLSv1.2.
2	User authenticated using user credentials. Client origin: 10.	57188. Windows username	lient type:	Client version:	SSL protocol: TLSv1.2.
3	User authenticated using user credentials. Client origin: 10.	57827. Windows username	ient type: E	lient version:	SL protocol: TLSv1.2.
4	User authenticated using user credentials. Client origin: 10.	58712. Windows username	Client type	. Client versio	. SSL protocol: TLSv1.2.
5	User authenticated using user credentials. Client origin: 10.	57592. Windows username	Client type	. Client versio	. SSL protocol: TLSv1.2.
6	User authenticated using user credentials. Client origin: 10.	59313. Windows username	Client type	. Client versio	SSL protocol: TLSv1.2.
7	User authenticated using user credentials. Client origin: 10.	5556. Windows username	lient type:	Client version:	SSL protocol: TLSv1.2.
8	User authenticated using user credentials. Client origin: 10.	61460. Windows username	Client type	. Client versio	SSL protocol: TLSv1.2.
9	User authenticated using user credentials. Client origin: 10.	8684. Windows username	Client type:	Client version	SSL protocol: TLSv1.2.

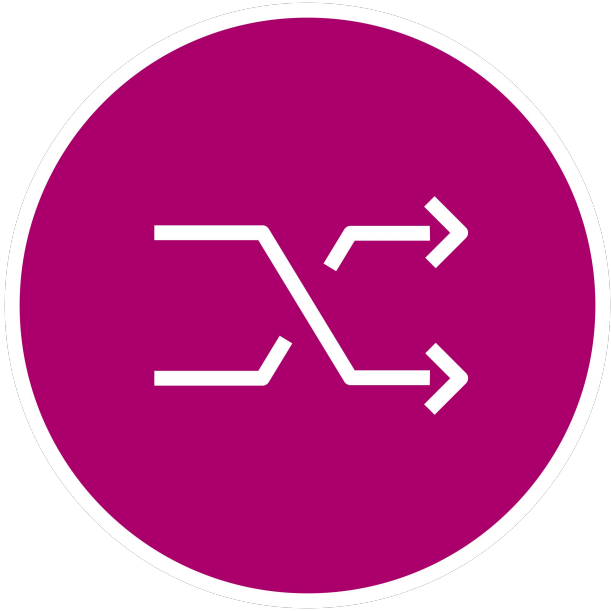
Integrations and Enrichment

Integrating with people data to understand departmental use cases

People directory (LDAP, AD)

Server directory (CMDB)

Network inventory



Documenting Data Sources

- Data source catalog – document as part of onboarding
- Periodic Splunk meetings with representatives from different teams/groups
- Splunk app
- Blog

“The alchemists in their search for gold found many other things of greater value”

Arthur Schopenhauer, German Philosopher

Q&A

Ben Marcus | Sr. Staff Engineer
Qualcomm

splunk> .conf19

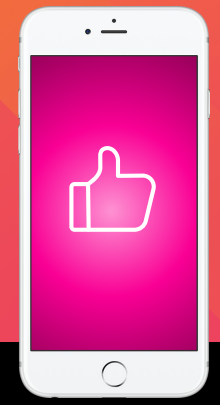
.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION



Visability

Metrics…More sourcetypes = > Visibility

Linux Server metrics

- Custom *nix Technology Add On
  - Memory, load, uptime, cpu, network, interfaces, disk, etc.
  - System command data - process (extended), netstat (extended), top
  - Custom command output – nfsmountstat, linux file handles (/proc), lscpu, etc.
- Collectd/Telegraf
- Osquery

Visability

Lots of Sourcetypes

- Linux syslogs, sudo logs, audit logs, etc.
- Application logs
  - Webserver (apache, nginx)
  - Revision control (Perforce, ClearCase)
  - Job scheduling (LSF, UGE)
  - Database
  - LDAP (access/error/replication)
  - DNS
  - Build and automation logs
  - System configuration logs.
- Appliance syslogs
  - Netapp logs, VMware ESX logs, LoadBalancer logs, Firewall logs, VPN logs, Router logs, NTP logs, Webproxy logs
- “Lights Out” management server logs (HP ILO, HP Virtual Connect, HP OA Dell iDRAC, etc)