

# Moving From Data To Wisdom

Mark Runals

Lead Security Engineer, The Ohio State University

.conf2016

splunk >

# Disclaimer

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 the 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.

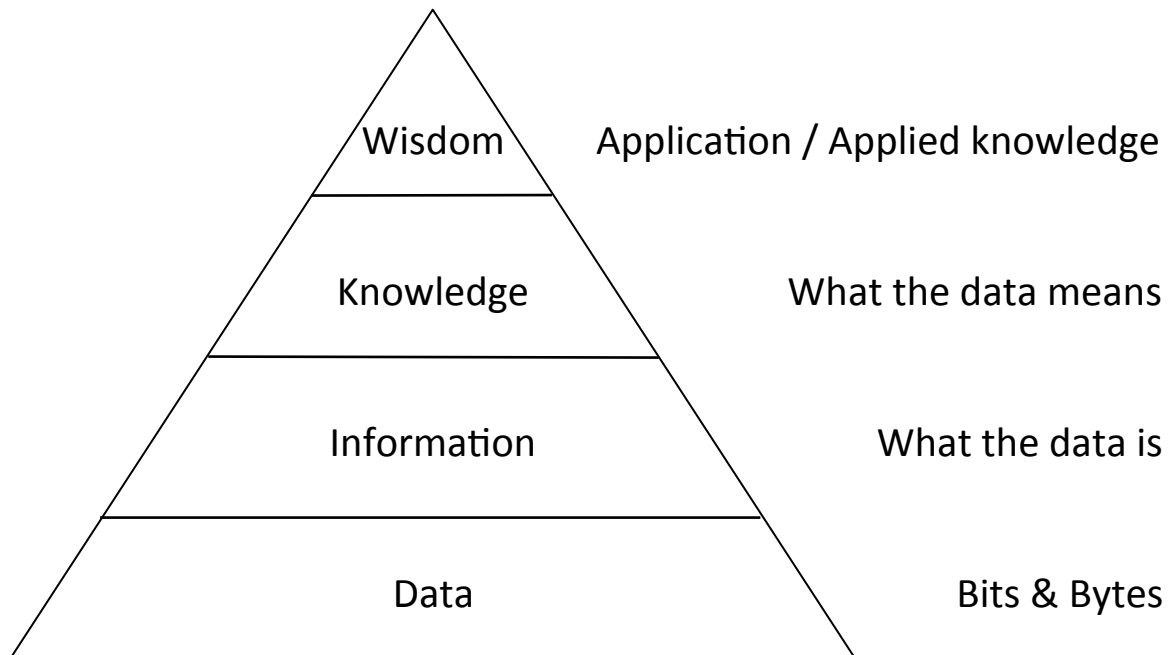
# Mark Runals

- 4 yr Splunk User
- ArcSight admin for 3 yrs
- Worked in InfoSec for 10+ yrs
- 2015 SplunkTrust Member
- Getting data into Splunk isn't the end game!

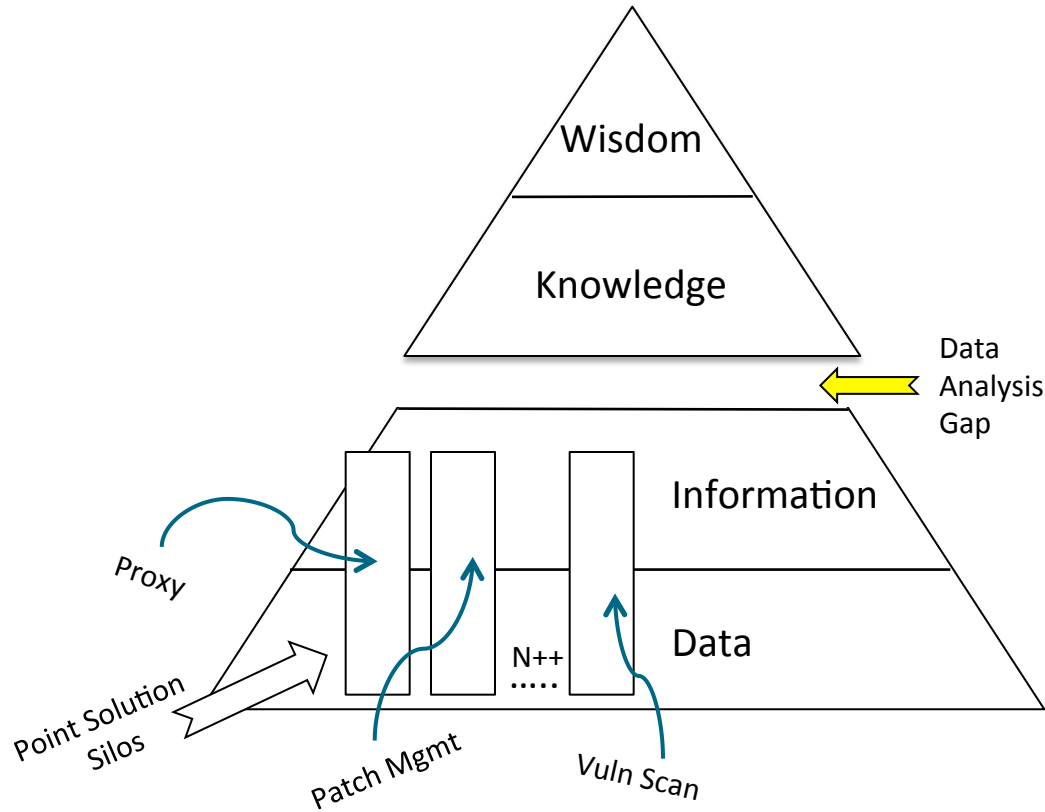
# Outcomes

- Paradigm to rethink data/analysis
- Common framework for Admins & 'Management'
- Deeper appreciation for what Splunk is

# DIKW Pyramid



# Typical Business



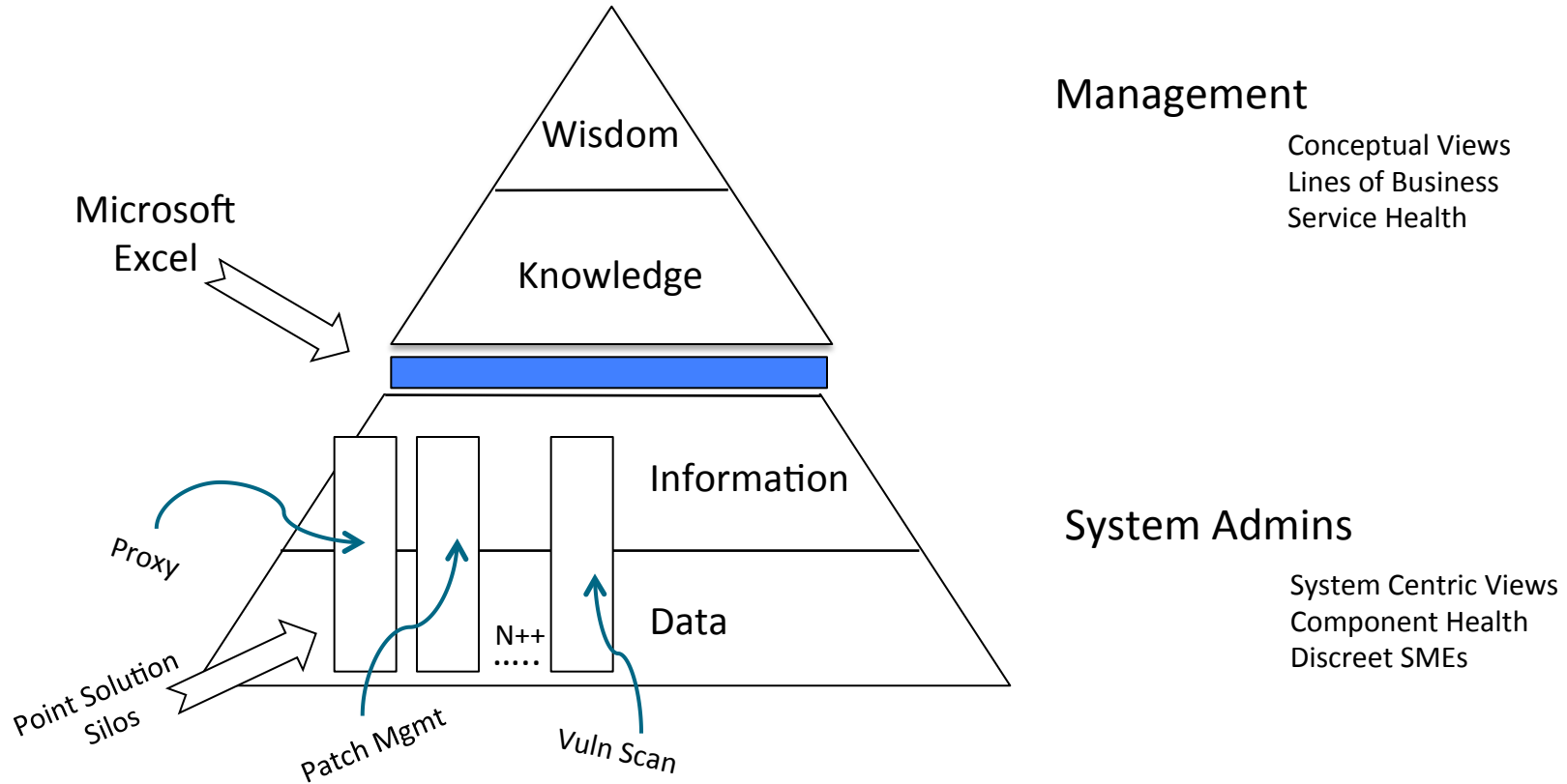
## Management

Conceptual Views  
Lines of Business  
Service Health

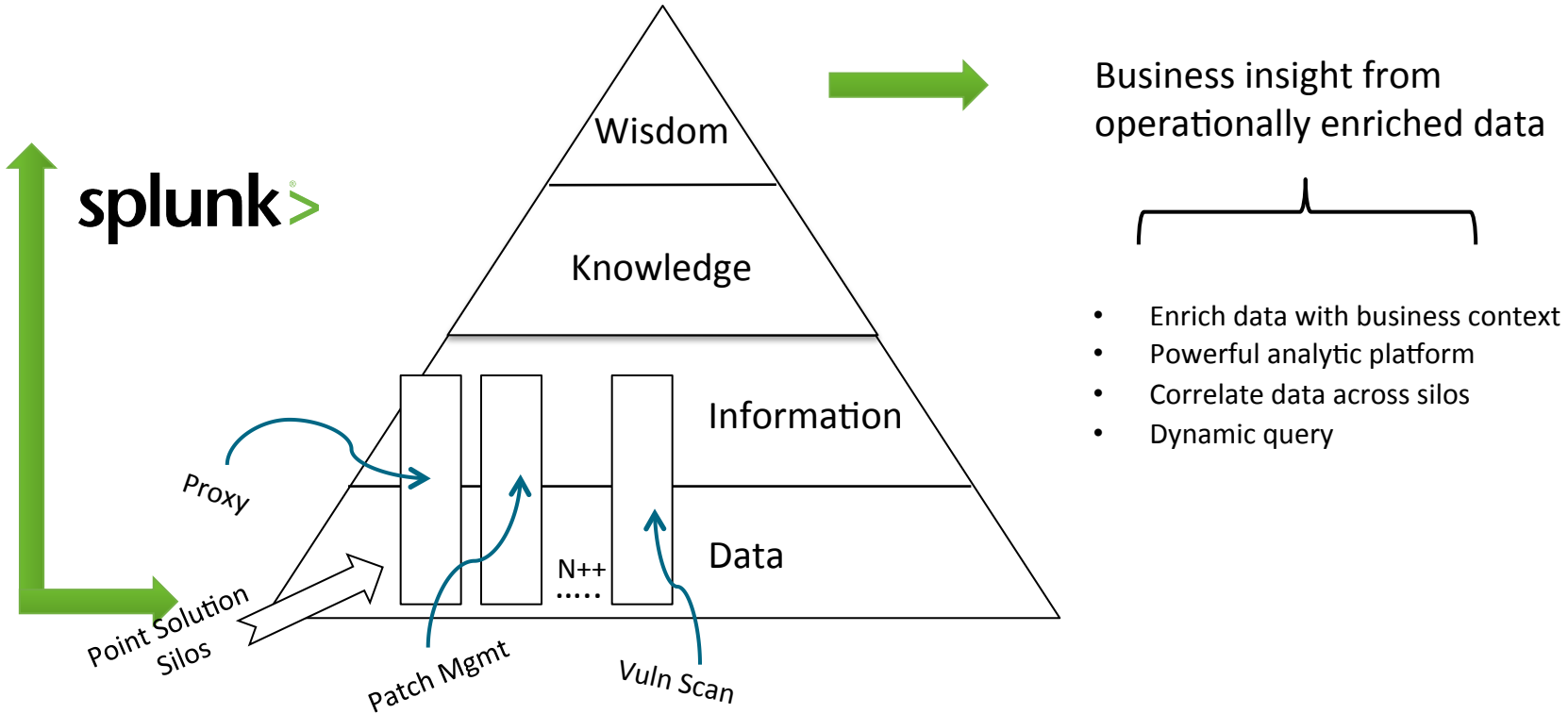
## System Admins

System Centric Views  
Component Health  
Discreet SMEs

# Typical Business

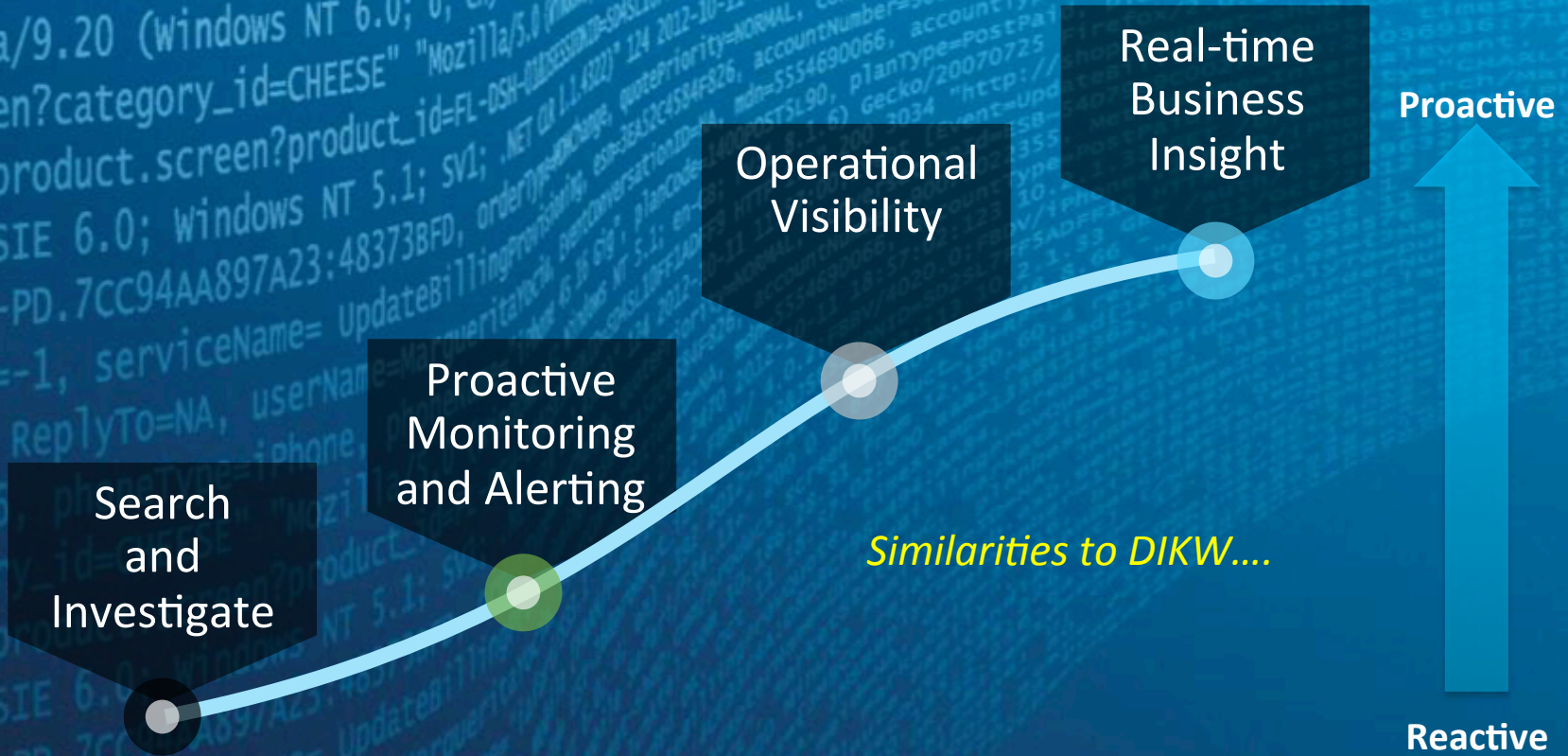


# What Splunk Brings





# Splunk Maturity Model



# OSU Mobile App - Data

New Search Save As Close

sourcetype=osumobile Yesterday Q

✓ 727,193 events (7/25/16 12:00:00.000 AM to 7/26/16 12:00:00.000 AM) Job Fast Mode

Events (727,193) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 50 Per Page Prev 1 2 3 4 5 6 7 8 9 Next

Hide Fields All Fields

Interesting Fields

- host 3
- index 1
- linecount 16
- source 2
- sourcetype 1
- splunk\_server 15

Extract New Fields

#	Time	Event
>	7/25/16 11:59:59.858 PM	2016-07-26T03:59:59.858Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://[REDACTED]
>	7/25/16 11:59:59.857 PM	2016-07-26T03:59:59.857Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://[REDACTED]
>	7/25/16 11:59:59.855 PM	2016-07-26T03:59:59.855Z - info: [MASTER:7509] HACouchDB Heartbeat, master host OK: http://[REDACTED]
>	7/25/16 11:59:58.281 PM	2016-07-26T03:59:58.281Z - http: [WORKER_API:17661] --> [REDACTED] [- (-)] HEAD / prod 200 3.9ms "-"
>	7/25/16 11:59:58.276 PM	2016-07-26T03:59:58.276Z - http: [WORKER_API:3864] --> [REDACTED] [- (-)] HEAD / prod 200 2.2ms "-"
>	7/25/16 11:59:57.429 PM	2016-07-26T03:59:57.429Z - http: [WORKER_API:3864] --> [REDACTED] [- (-)] HEAD /system/health prod 200 2.5ms "Mozilla/5.0+(compatible; UptimeRobot/2.0; http://www.uptimerobot.com/)"
>	7/25/16 11:59:57.206 PM	2016-07-26T03:59:57.206Z - http: [WORKER_API:17661] --> [REDACTED] [- (-)] GET /bus/routes/MC/vehicles qa 200 5.5ms "ed u.osu.osumobile:3.2.8/150; samsung; samsung SAMSUNG-SM-G530AZ/LMY48B.G530AZTU4B0J4; Android v5.1.1; Android SDK Level 22"
>	7/25/16 11:59:54.941 PM	2016-07-26T03:59:54.941Z - http: [WORKER_API:16404] --> [REDACTED] [- (-)] GET /bus/routes/CLS/vehicles qa 200 5.4ms "e du.osu.osumobile:3.2.8/150; samsung; samsung SGH-T999L/JSS15J.T999LUVUBNC1; Android v4.3; Android SDK Level 18"
>	7/25/16 11:59:54.847 PM	2016-07-26T03:59:54.847Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://[REDACTED]
>	7/25/16 11:59:54.846 PM	2016-07-26T03:59:54.846Z - info: [MASTER:7509] HACouchDB Heartbeat, master host OK: http://[REDACTED]

# OSU Mobile App - Information

New Search

sourcetype=osumobile

727,193 events (7/25/16 12:00:00.000 AM to

Events (727,193) Patterns Stat

Format Timeline Zoom Out Zoom In

Interesting Fields

- # app\_build\_number 32
- a app\_version 32
- # date\_hour 24
- # date\_mday 2
- # date\_minute 60
- a date\_month 1
- # date\_second 60
- a date\_wday 2
- # date\_year 1
- # date\_zone 1
- a environment 3
- a eventtype 6
- a http\_method 3
- a iphone\_language 47
- # linecount 16
- a log\_level 5
- a platform 3
- a platform\_version 42
- a punct 100+
- # response\_time 100+
- a splunk\_server 15
- a src\_ip 100+
- # status 9
- # timeendpos 1
- # timestartpos 1
- a uri\_path 100+
- # WORKER\_API 26

Save As Close

Yesterday

Job Smart Mode

1 hour per column

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

9:59.858Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://

9:59.857Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://

9:59.855Z - info: [MASTER:7509] HACouchDB Heartbeat, master host OK: http://

9:58.281Z - http: [WORKER\_API:17661] --> [- (-)] HEAD / prod 200 3.9ms "-"

9:58.276Z - http: [WORKER\_API:3864] --> [- (-)] HEAD / prod 200 2.2ms "-"

9:57.429Z - http: [WORKER\_API:3864] --> [- (-)] HEAD /system/health prod 200 2.5ms compatible; UptimeRobot/2.0; http://www.uptimerobot.com/)

9:57.206Z - http: [WORKER\_API:17661] --> [- (-)] GET /bus/routes/MC/vehicles qa 200 5.5ms "ed :3.2.8/150; samsung; samsung SAMSUNG-SM-G530AZ/LMY48B.G530AZTU4BOJ4; Android v5.1.1; Android SDK Level 22"

9:54.941Z - http: [WORKER\_API:16404] --> [- (-)] GET /bus/routes/CLS/vehicles qa 200 5.4ms "e le:3.2.8/150; samsung; samsung SGH-T999L/JSS15J.T999LUVUBNC1; Android v4.3; Android SDK Level 18"

9:54.847Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://

9:54.846Z - info: [MASTER:7509] HACouchDB Heartbeat, master host OK: http://

9:54.845Z - info: [MASTER:7509] HACouchDB Heartbeat, slave host OK: http://

# OSU Mobile App - Knowledge

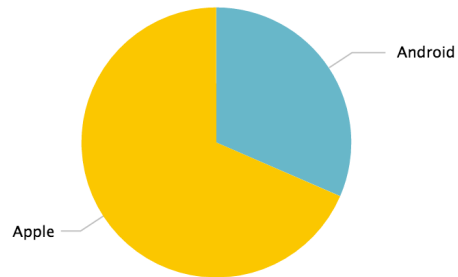
New Search Save As Close

```
sourcetype=osumobile | eval Platform = if(platform LIKE "i%", "Apple", "Android") | stats dc(src_ip) by Platform
```

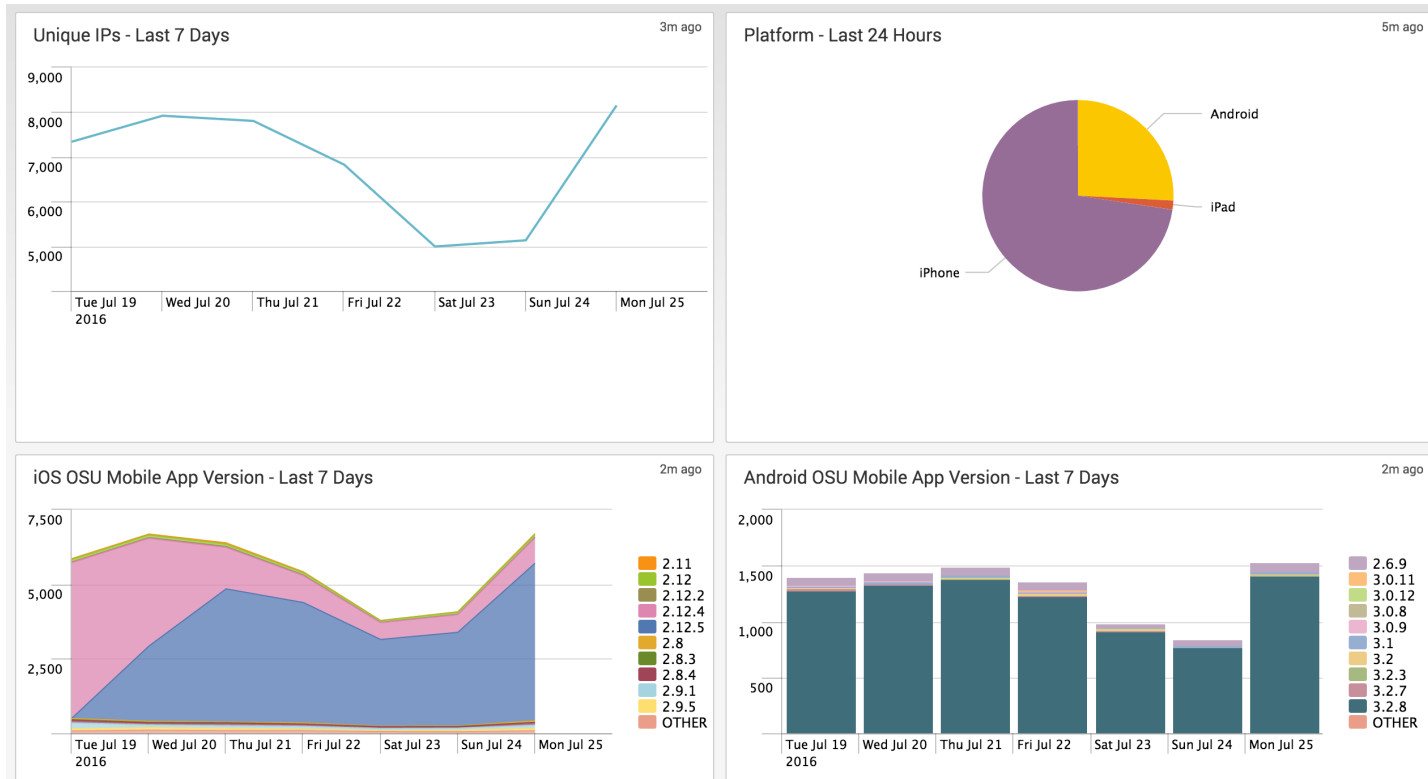
727,193 events (7/25/16 12:00:00.000 AM to 7/26/16 12:00:00.000 AM) Job || ■ → ↓ + Smart Mode

Events Patterns Statistics (2) Visualization

Pie Format

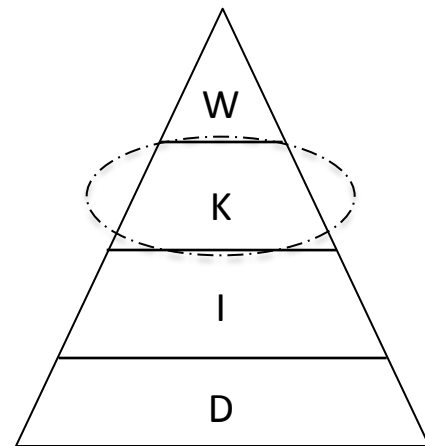


# OSU Mobile App - Wisdom



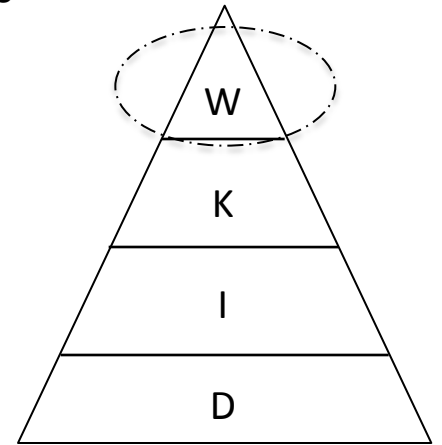
# Other Thoughts

- Leverage the Splunk Common Information Model (CIM)  
Common 'language' across data types
- Use Knowledge Objects to bridge systems to services  
lookups, tags, eventtypes
- Make alerts more actionable – not just What happened  
Incorporate recipient's 'next' question (ie where, who)



# Final Thoughts

- Understand the difference between Measurements and Metrics  
Metric = combination of 2 or more measurements
- Administer Splunk with end state in mind
  - What are your use cases?
  - What pain points are you trying to address?
- Help bridge the Information and Knowledge analytic gap
  - Key step in leveraging Splunk toward 'Wisdom' ends



# THANK YOU

.conf2016