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

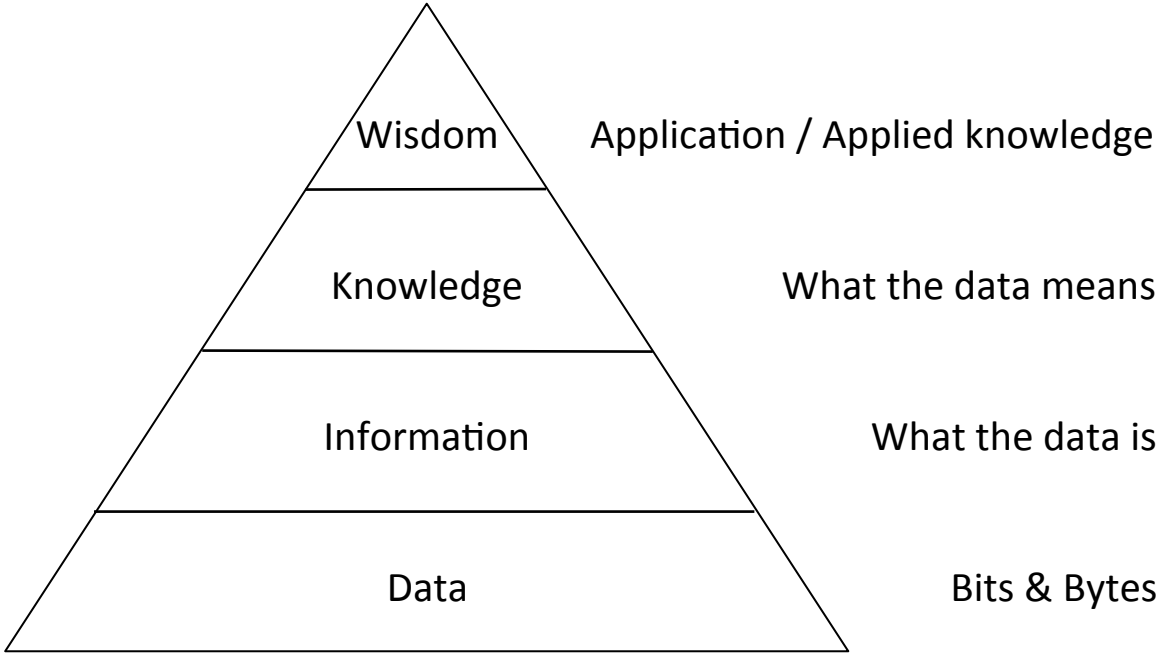
- 4 yr Splunk User
- ArcSight admin for 3 yrs
- Worked in InfoSec for 10+ yrs
- 2015 SplunkTrust Member

➢ Getting data into Splunk isn't the end game!

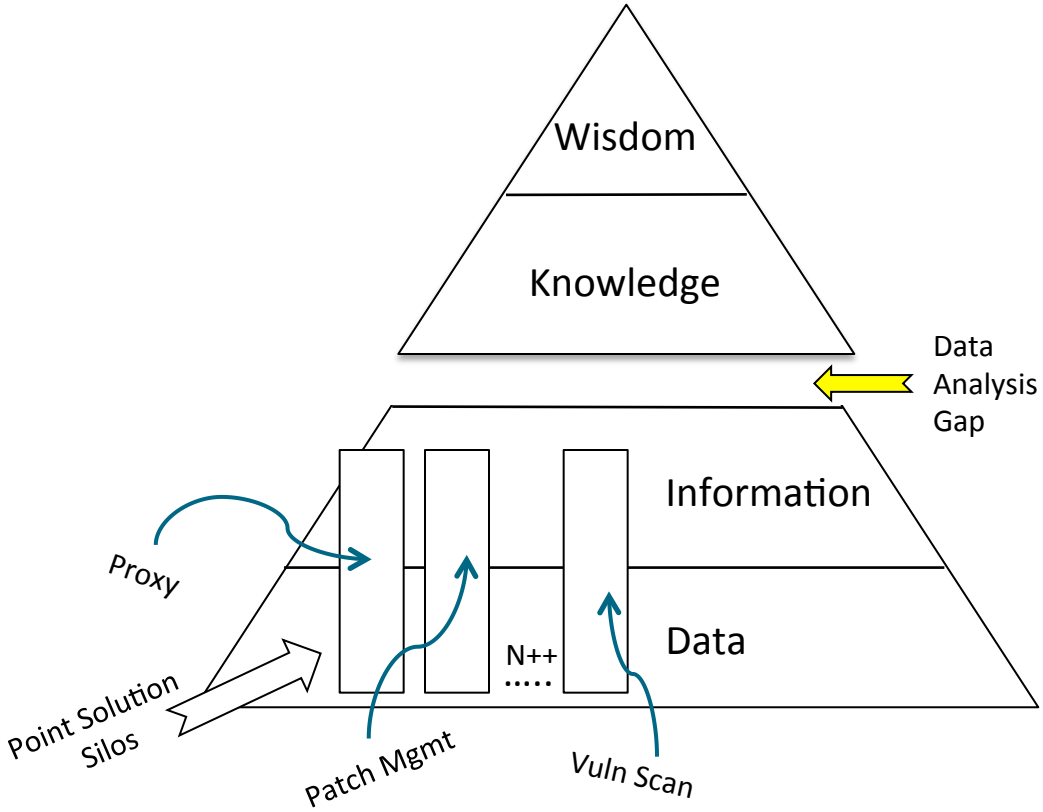
Outcomes

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

DIKW Pyramid



Typical Business



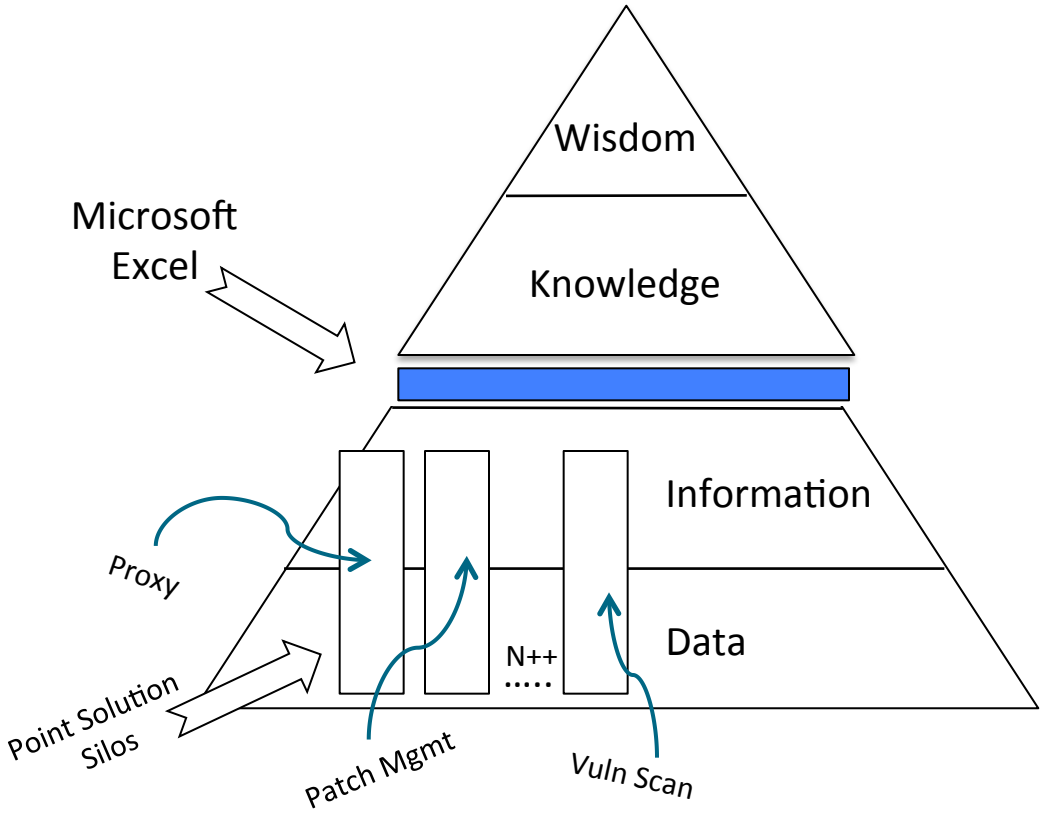
Management

Conceptual Views
Lines of Business
Service Health

System Admins

System Centric Views
Component Health
Discreet SMEs

Typical Business



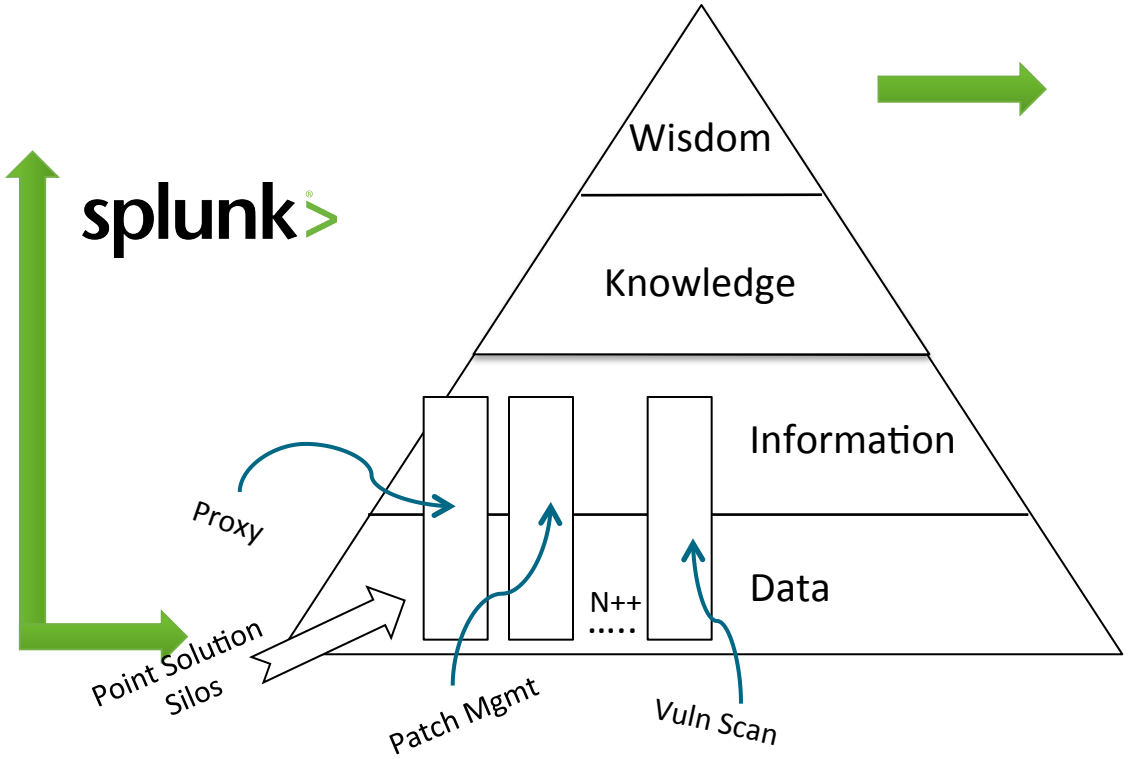
Management

Conceptual Views
Lines of Business
Service Health

System Admins

System Centric Views
Component Health
Discreet SMEs

What Splunk Brings

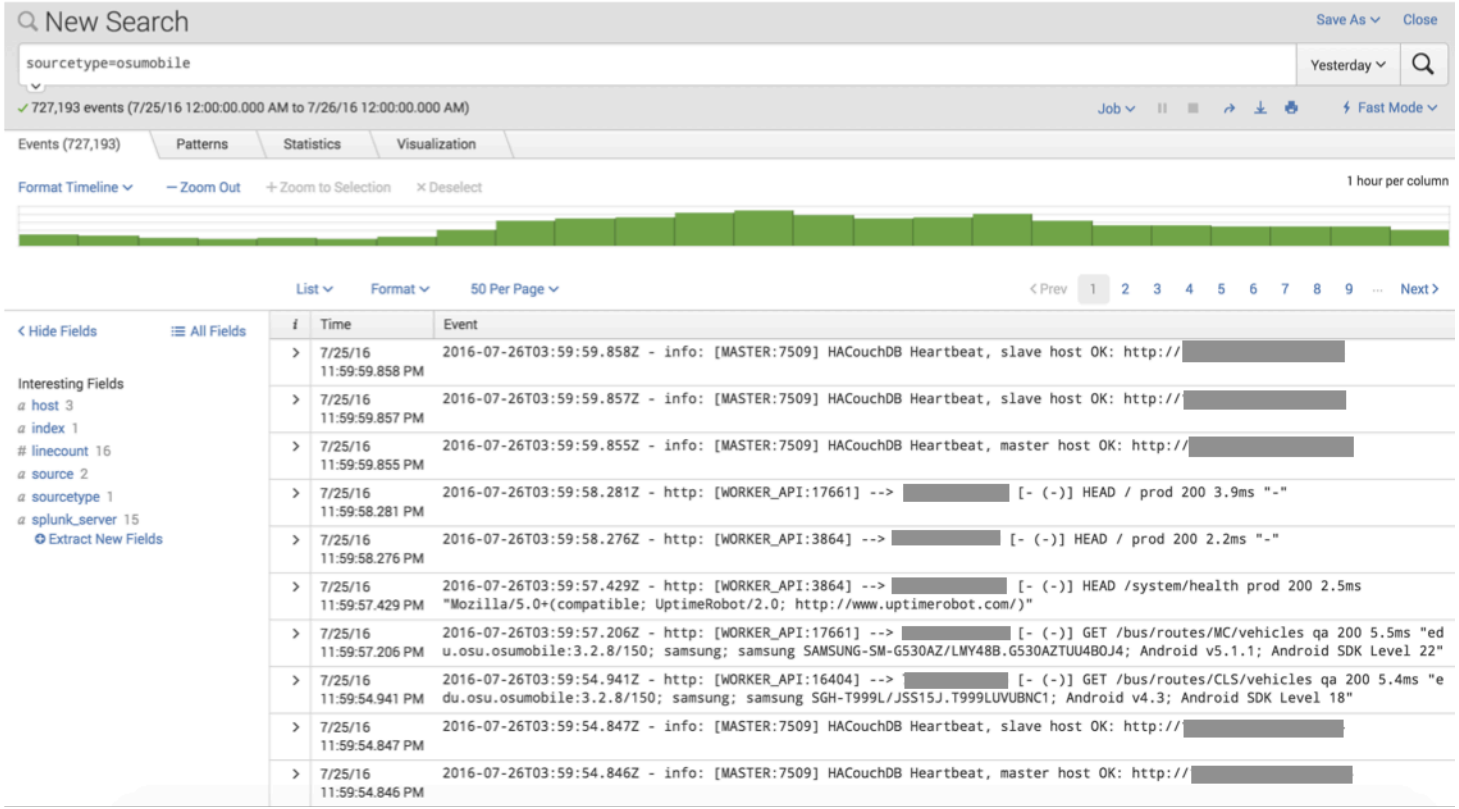


Business insight from operationally enriched data

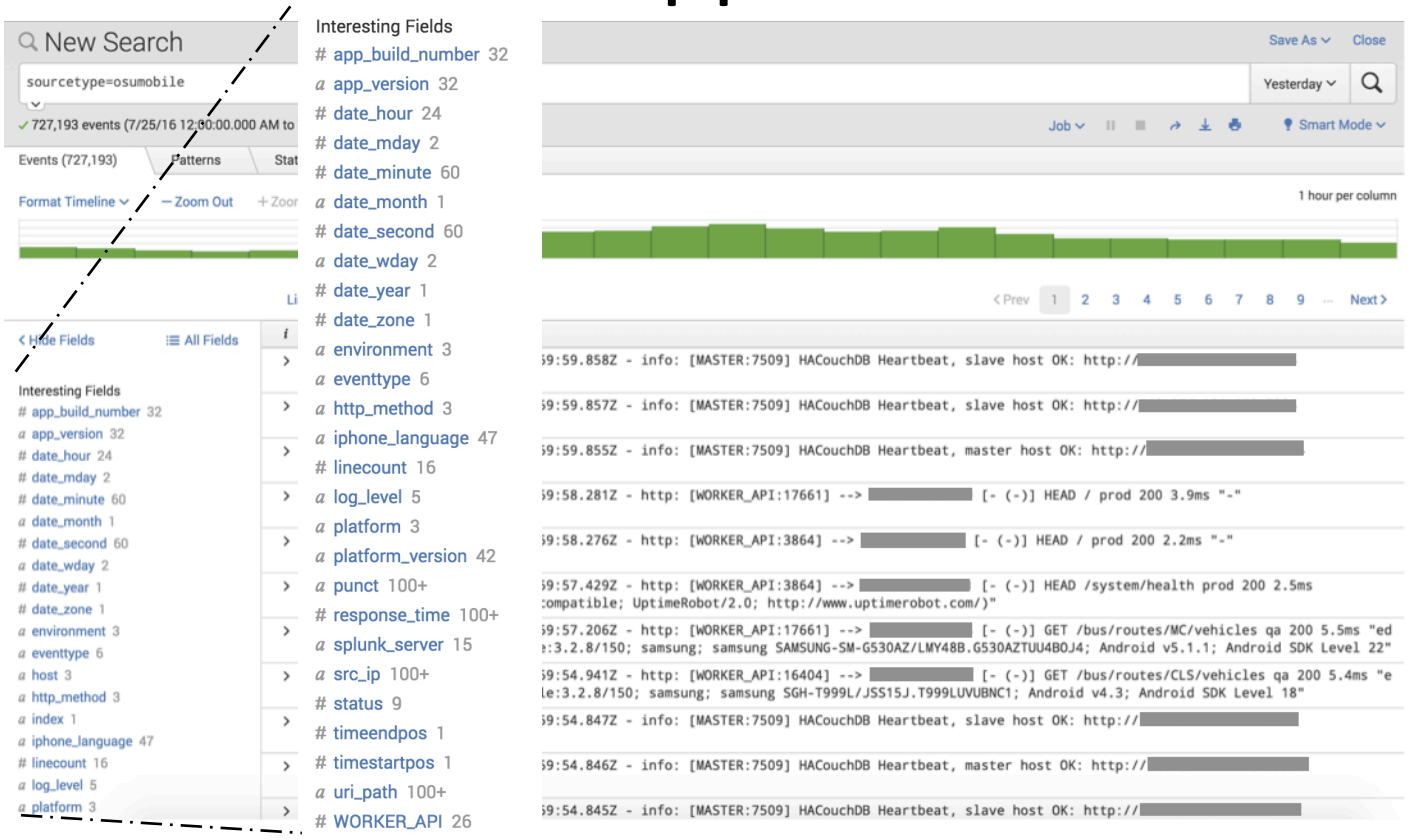
- Enrich data with business context
- Powerful analytic platform
- Correlate data across silos
- Dynamic query

Splunk Maturity Model

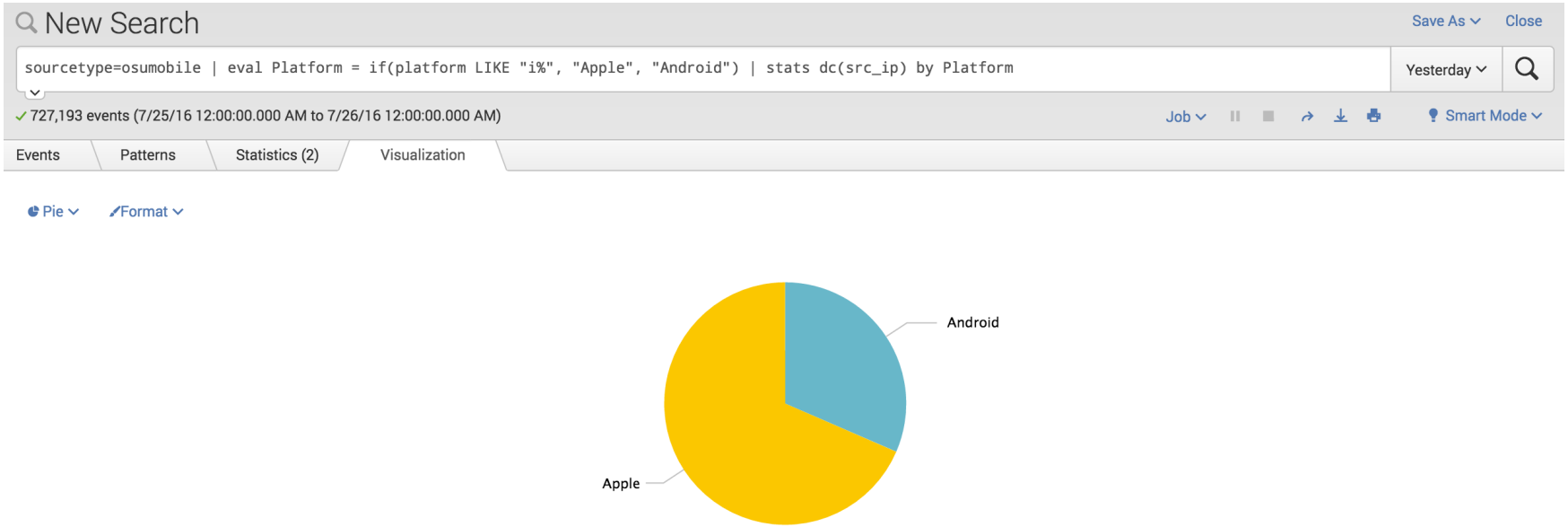
OSU Mobile App - Data



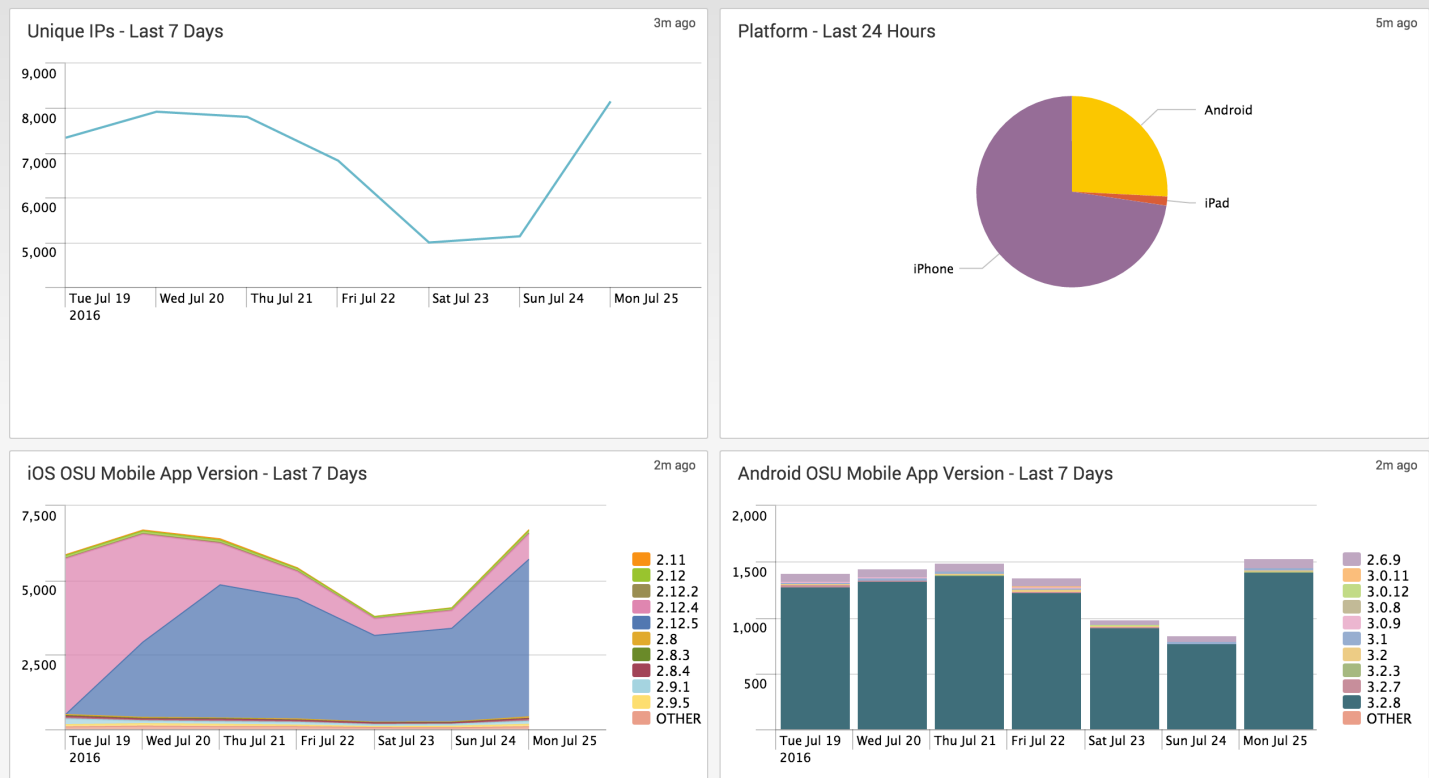
OSU Mobile App - Information



OSU Mobile App - Knowledge

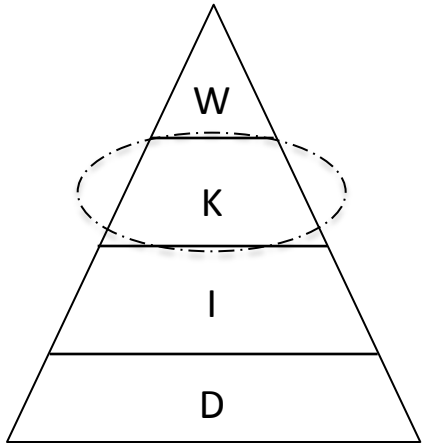


OSU Mobile App - Wisdom



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)

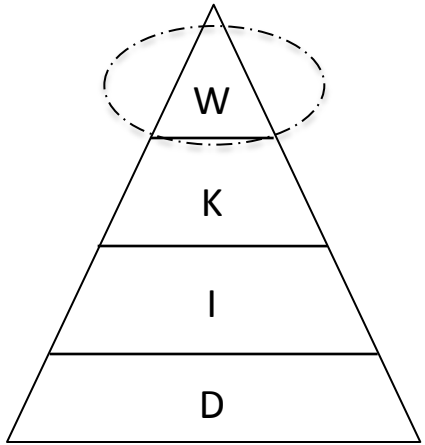


Final Thoughts

- 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

splunk>