Splunking IT Data Is Great, Splunking Non-IT Data Is Awesome

Mathew Benwell

Information Security Specialist,

The University of Adelaide

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.

About the University of Adelaide

THE UNIVERSITY of ADELAIDE

The University of Adelaide is one of Australia's leading research-intensive universities and is consistently ranked among the top 1% of universities in the world. Established in 1874, it is Australia's third oldest university with a strong reputation for research and teaching excellence, and producing graduates that make an impact on the world.

About Mathew

- Information Security Specialist at the University of Adelaide
- Information Security for 8 years, IT for 14
- Resident Splunk Guy

Agenda

- Why Splunk at the University?
- Cool Stuff For IT Teams
- Awesome Stuff Not For IT

THE UNIVERSITY of ADELAIDE

But First… Where is Adelaide?

- Here
- ~ 1,100 km (~700 Miles) from Sydney
- 13,505 km (8392 Miles) from here
- 3 Flights, almost 18 hours in the air

Why Splunk?

splunk>

Executive Summary: Before Splunk

Executive Summary: After Splunk

Why We Chose Splunk

- In 2011, attempting to deal with phishing attacks
- Created a Simple Authentication anomaly detection system
  - MySQL database
  - Poorly written ruby script
  - Radius logs

Why We Chose Splunk

- Flexibility
  - Traditional SIEM solutions are not as easy to drill down into the raw event
- Easy to learn
  - Knowledge of Operating System CLI and a bit of SQL
- Most importantly, Splunk met our Use Case requirements

Initial Splunk Use Cases

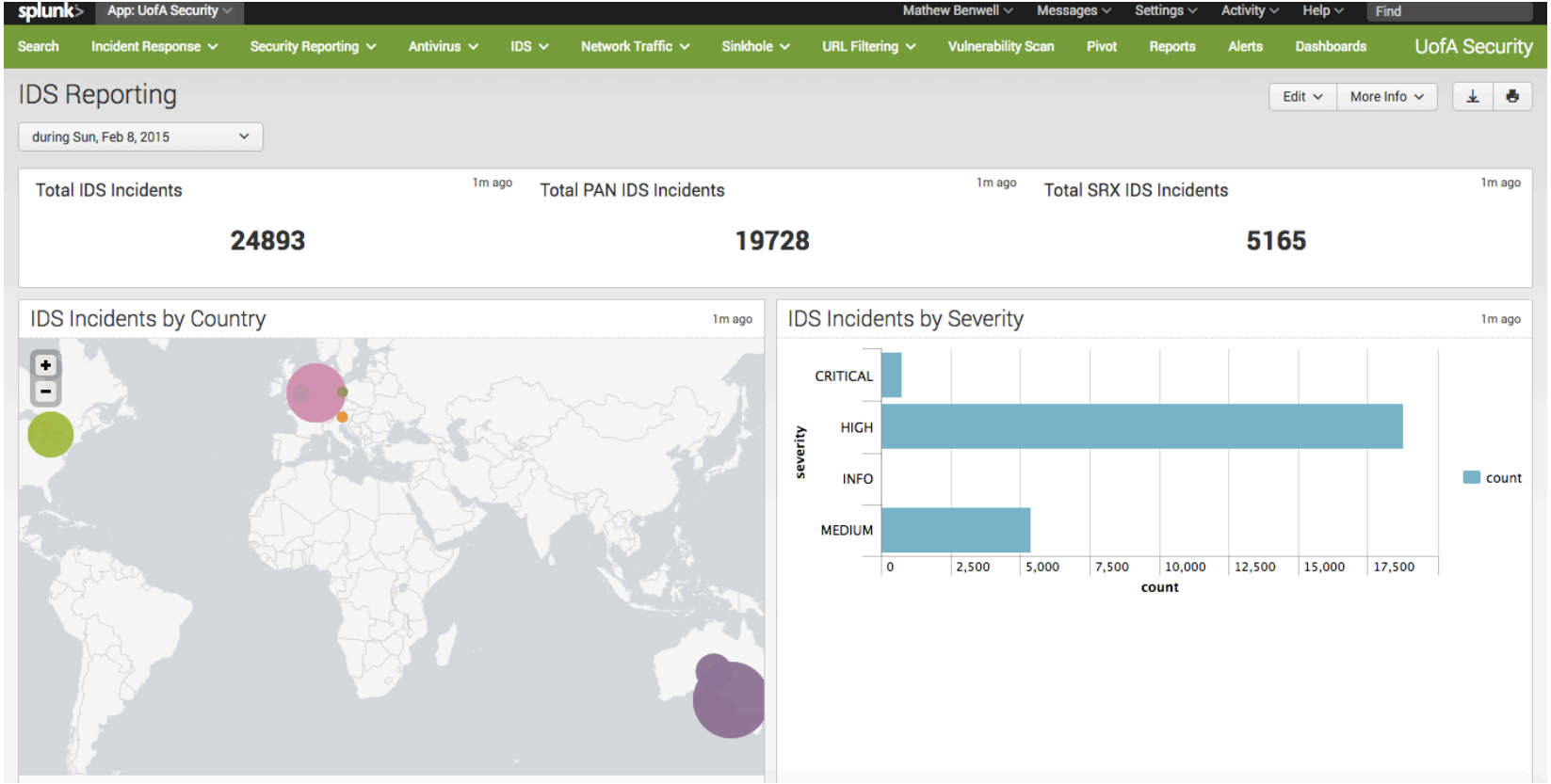
- Anomalies in authentication events
  - Logon within a given time frame for disparate geographic locations
- Phishing email detection
  - Common word list to help identify attacks
- Common account events
  - Failed logon events
    - Single source different account
    - Multiple sources same account
    - Failed logon followed by success
- Large mail volumes

Security Data Sources

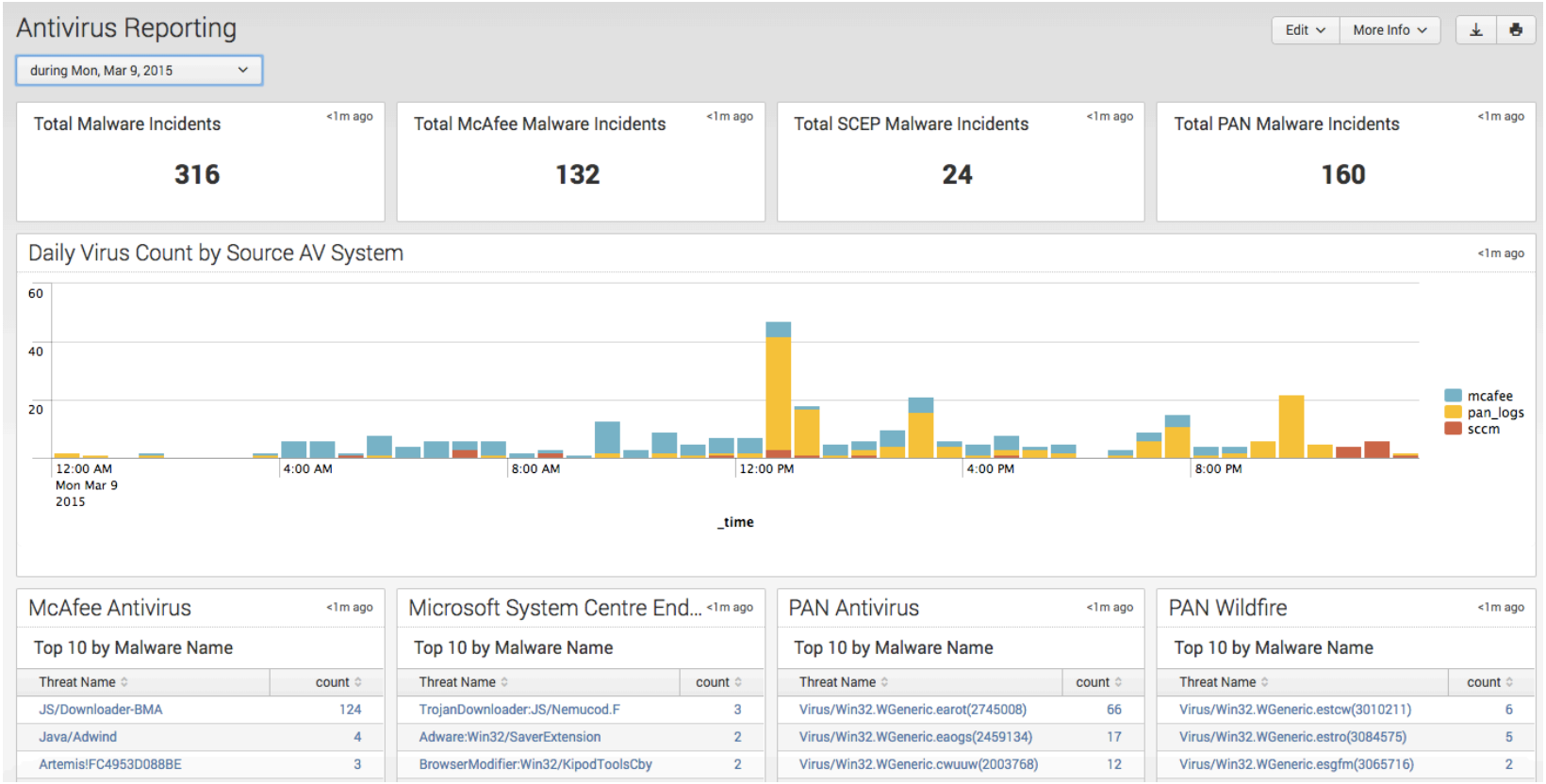
Splunk Common Information Model

- What is the Common Information Model (CIM)?
- Abstraction from raw data
- Standardized knowledge for events (i.e. field names)
- Used by Splunk for Enterprise Security

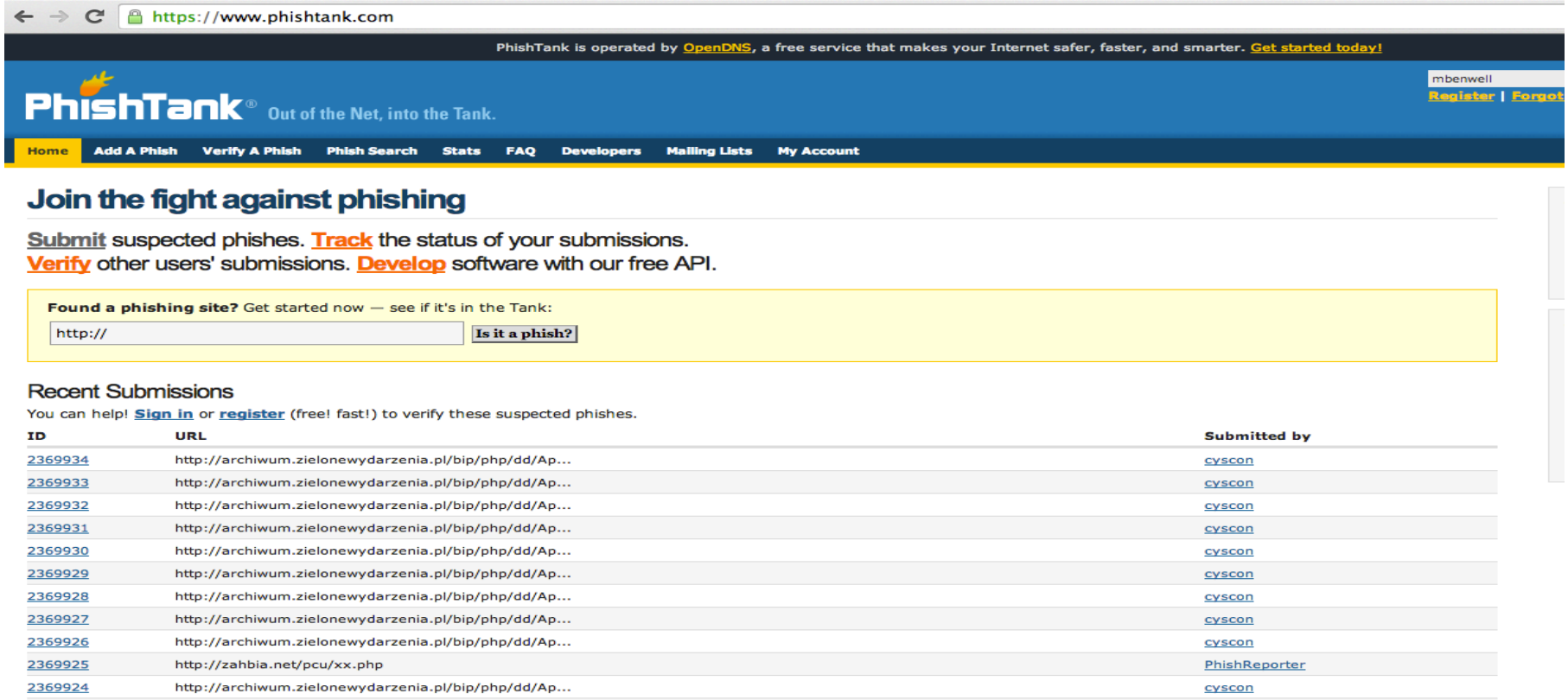
Security Uses – IDS/IPS



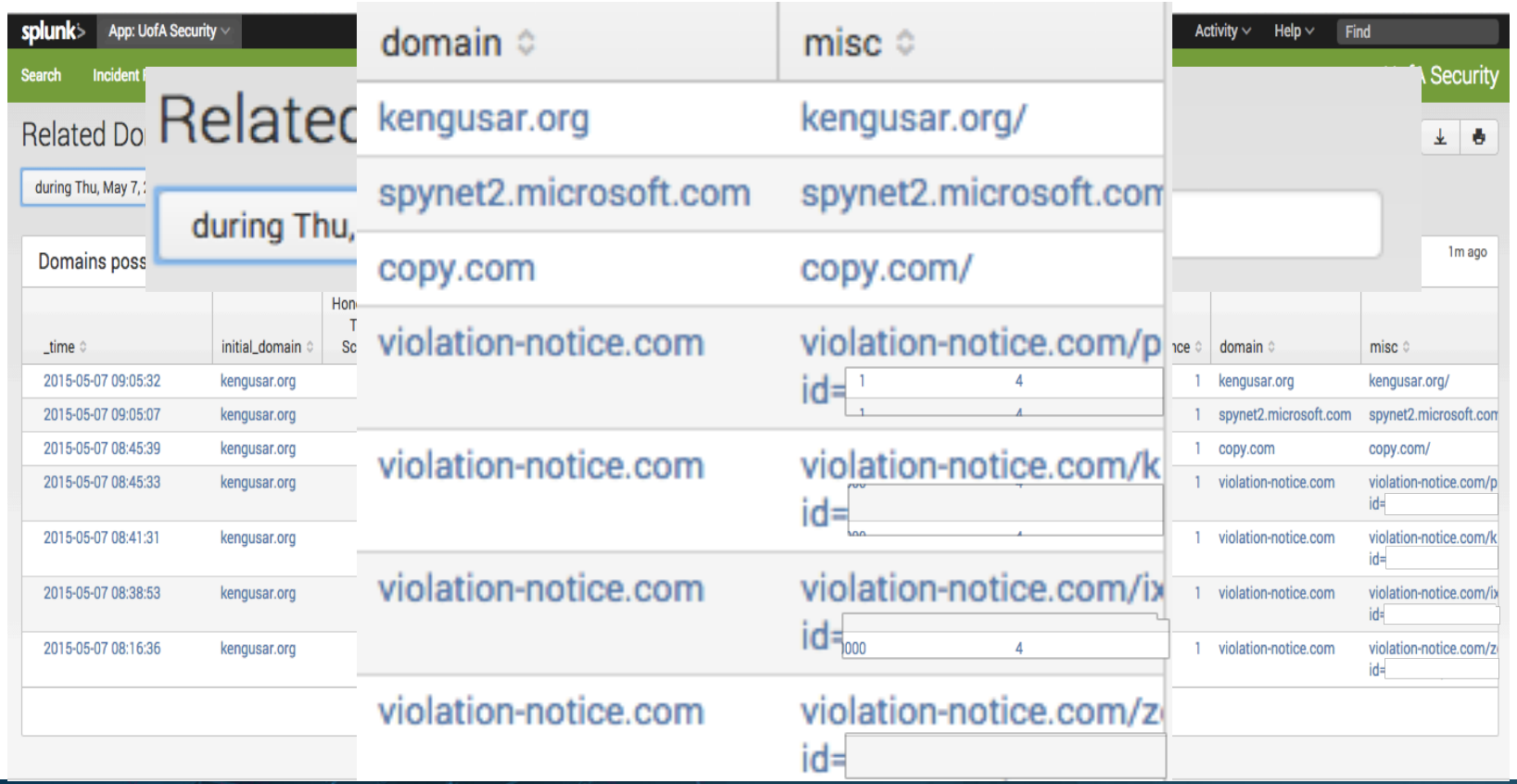
Security Uses – Anti-malware



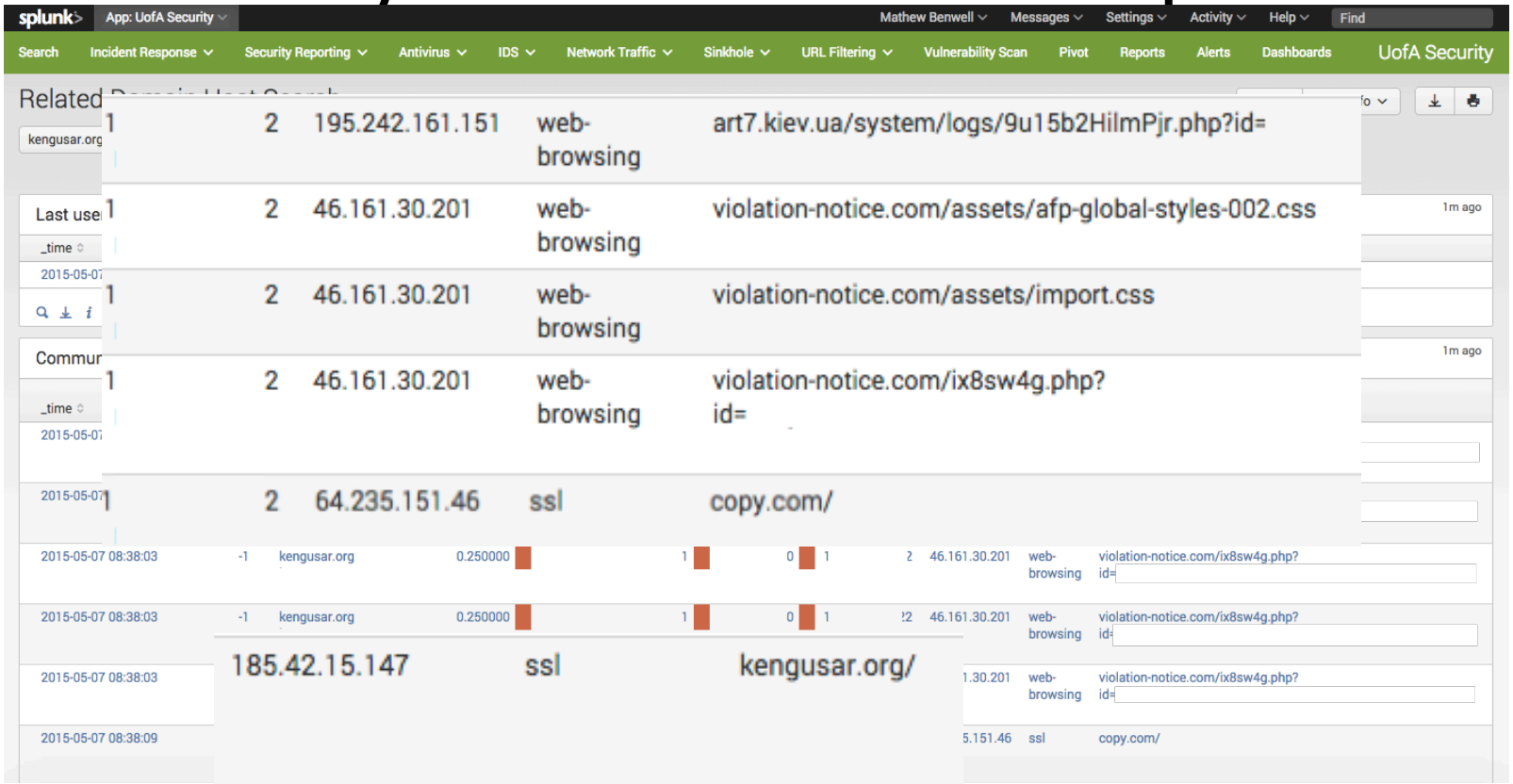
Security Uses: Looking For Bad Things



Security Uses – Incident Response



Security Uses – Incident Response



Great Stuff for IT

splunk>

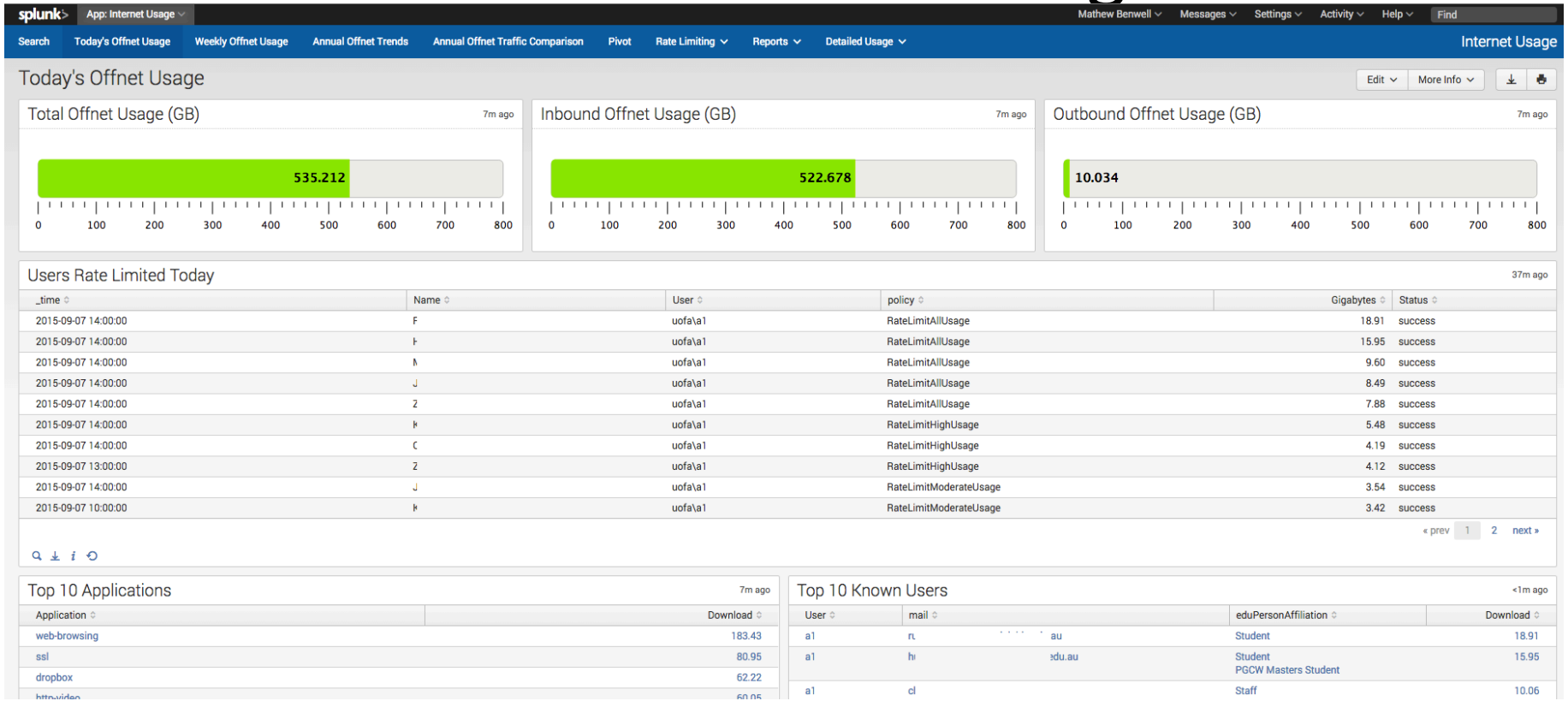
The Great Stuff

- Applications Monitoring
- Citrix Reporting
- Computer Suite Application Usage
- Internet Traffic Accounting
- Print Usage Reporting

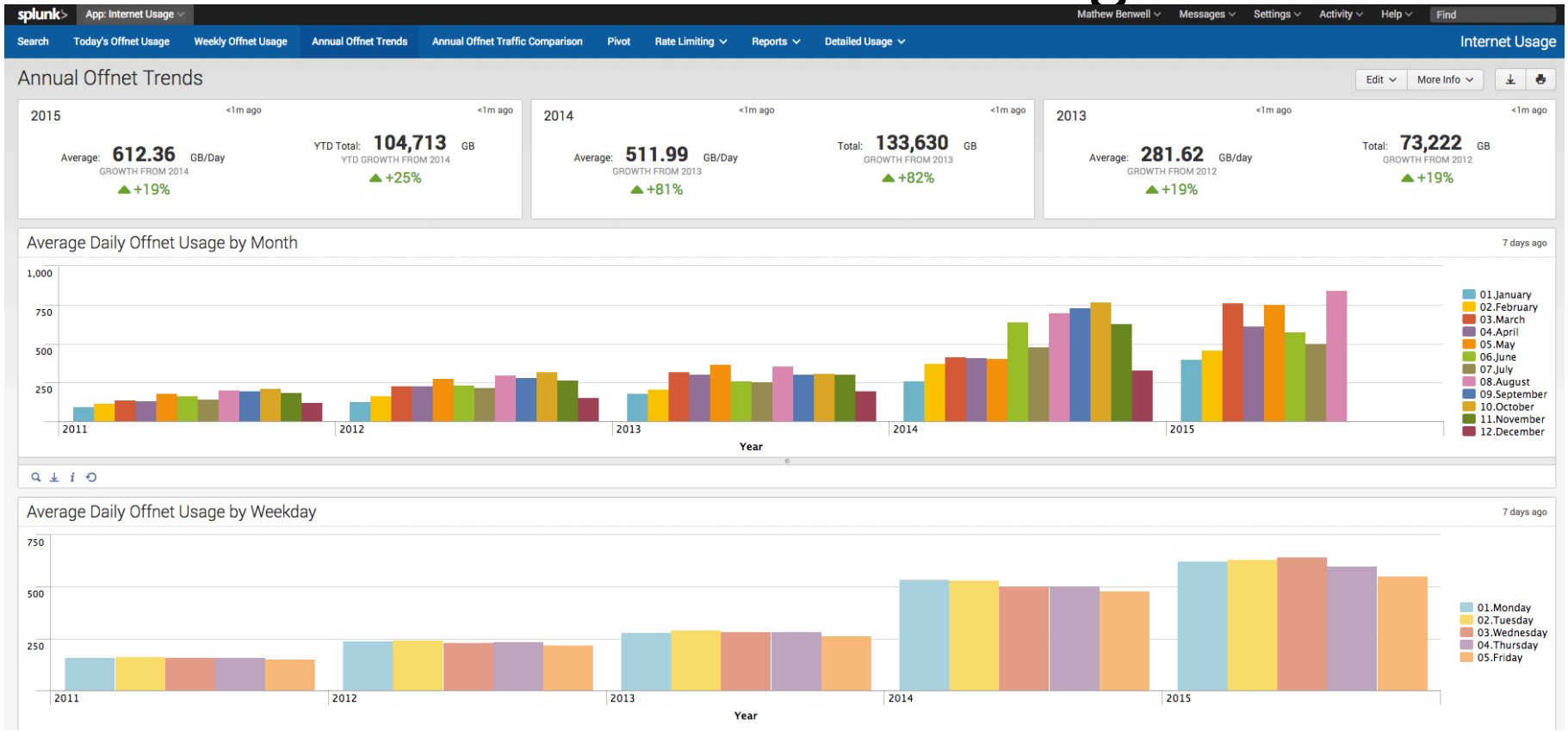
Internet Accounting

- In Australia we are charged for Internet data consumption
- Quota system used previously to control cost
- Quotas removed in 2014
- To help track and control cost we use Splunk

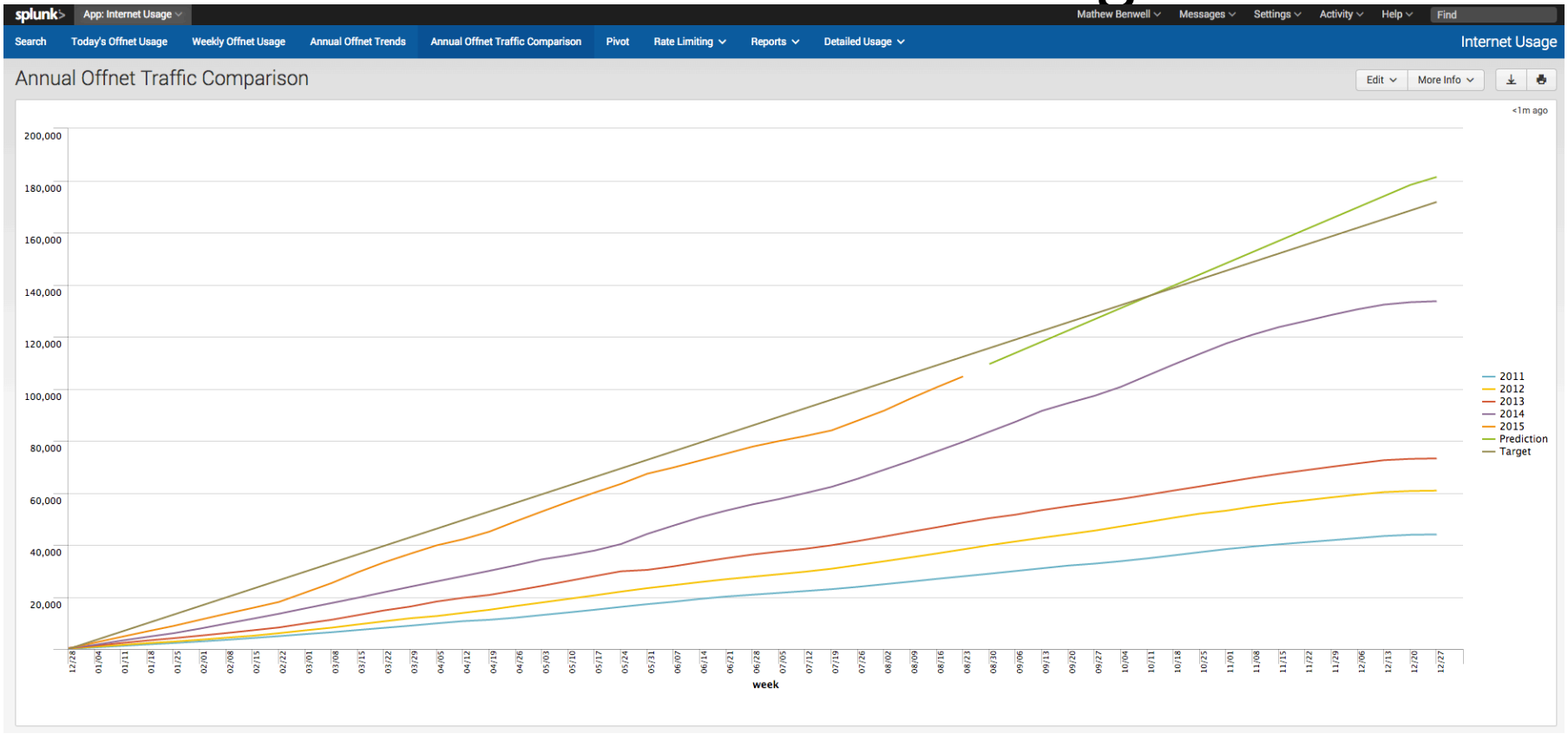
Internet Accounting



Internet Accounting



Internet Accounting



How Did We Build It?

1. Start with the question
   - What did we need to know?

2. Simple use case development

3. Identify supporting data sources
   - Firewall data
   - Unmetered address data

4. Get Splunking
   - Summary indexing used
   - Custom script for metering calculation
   - Extended use of Palo Alto Networks API

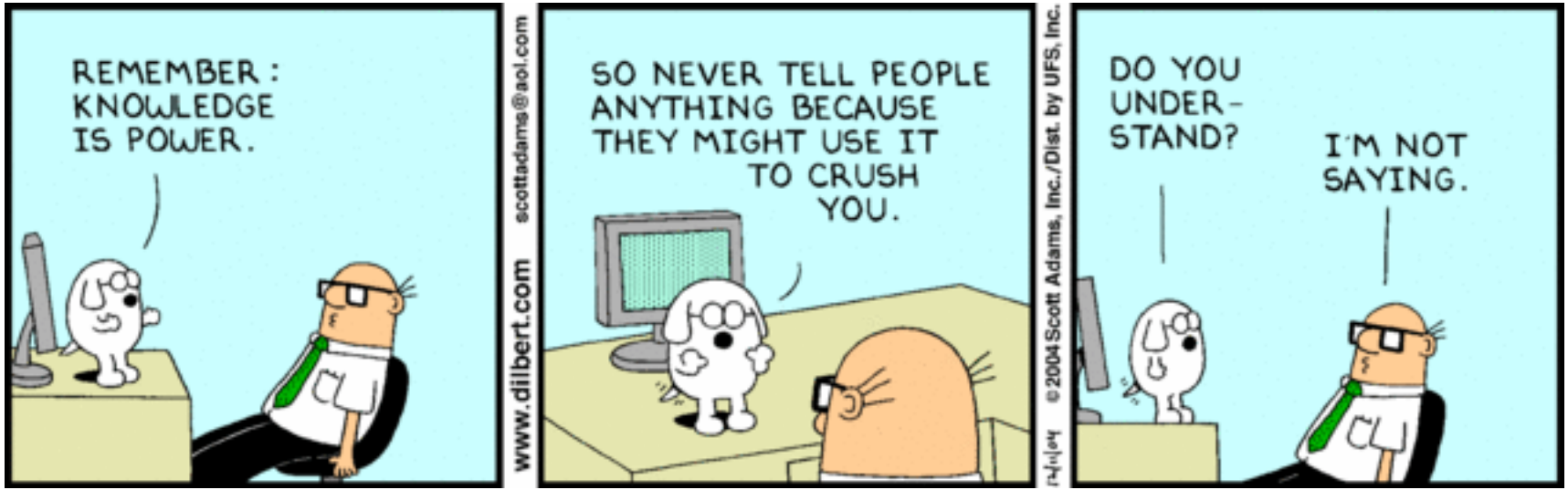
Internet Accounting - Outcome

- We know precisely where we are incurring charges

- We are helping to control cost

- No cost, we already have the data for Security

Computing Suite Utilization



Computing Suite Utilization

splunk> App: Computing Pool Usage | Mathew Benwell | Messages | Settings | Activity | Help | Find

Computing Pool Utilisation Summary | Application Usage | Computing Suite Usage | Matlab Adapt vs desktop | Search | Computing Pool Usage

Application Usage

The following data represents the amount of time between a process start event and a process termination event. The data is also limited to a predefined set of process names that we wish to monitor

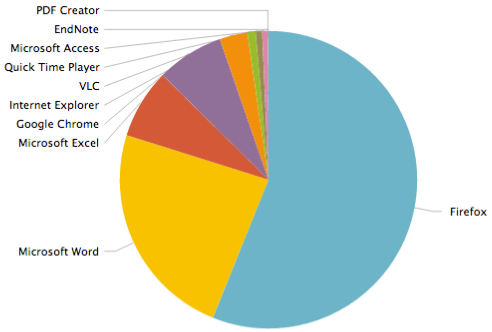
Edit | More Info

Suite

Today | HUBL4W | Submit

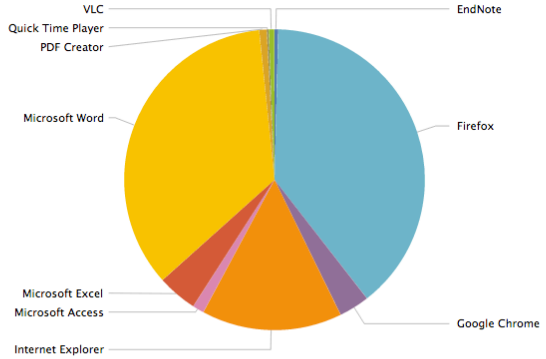
Application Runtime

<1m ago

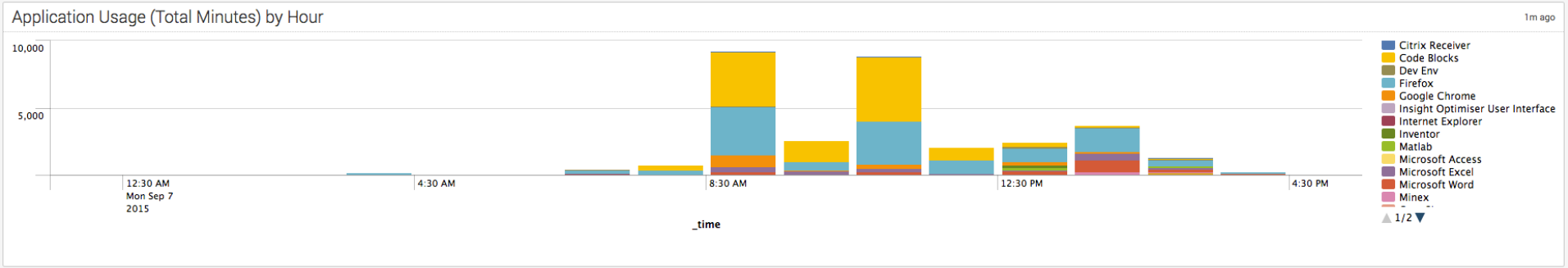


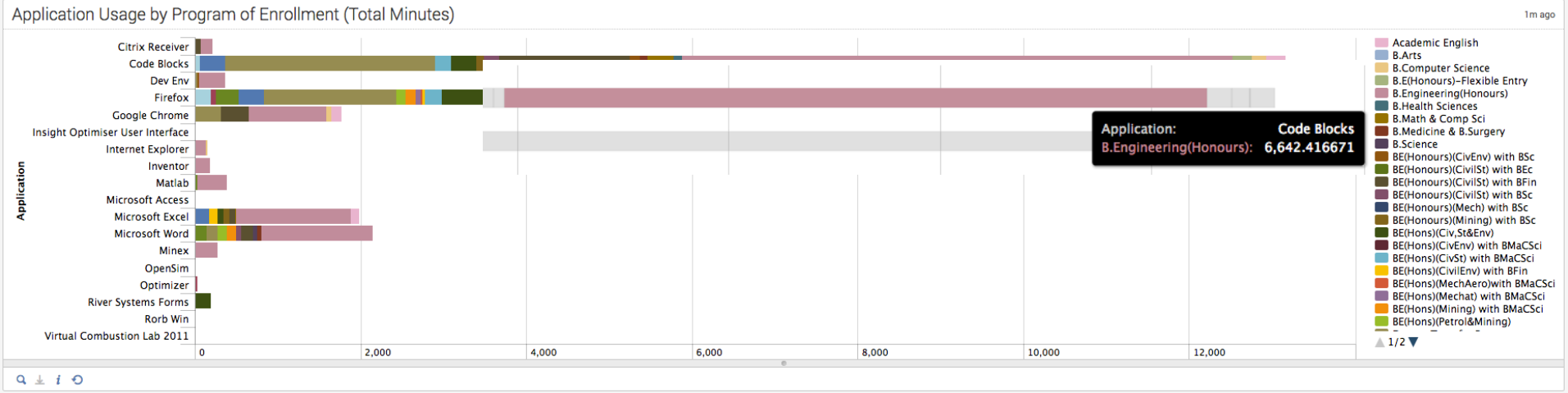
Number of Times Application has Run

<1m ago

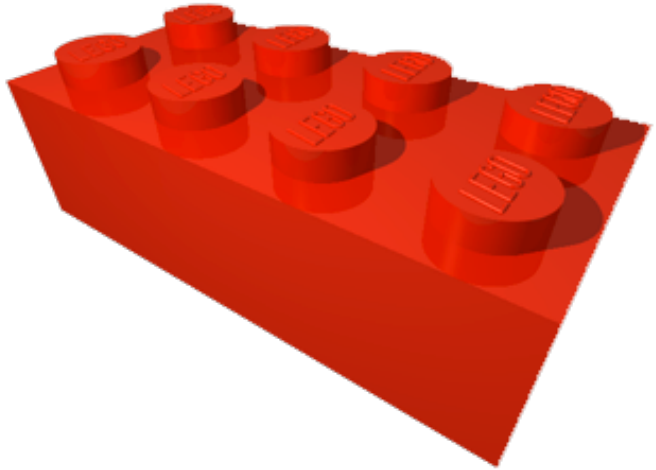


Computing Suite Utilization





How Did We Build It?



1. Start with the question
   - What did we need to know?
2. Simple Use case development
3. Identify supporting data sources
   - Windows process auditing
4. Get Splunking
   - Only tracking processes started by explorer process
   - Windows event log forwarding

Computing Suite Utilization - Outcome

- Team now has visibility to make decisions using real information

- Security team has another useful data source. Think IOC's

- Small cost (5-10gb/day)

Awesome Stuff Not For IT

splunk>

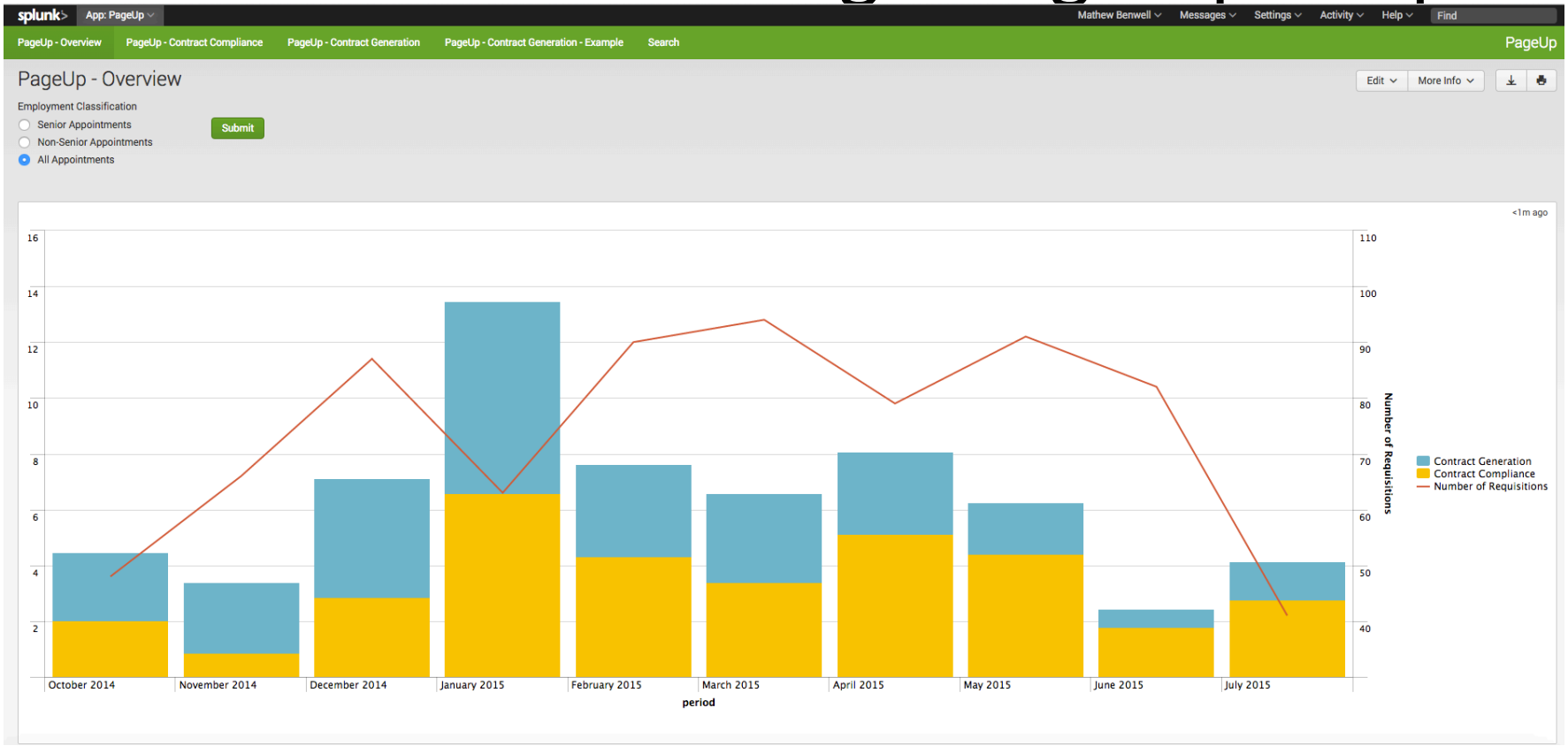
The Awesome Stuff

- Physical space reporting
- Project financial reporting
- Learning management system reporting
- Human Resources contract processing (PageUp People)
- Casual staff timesheet payment system (In house system)

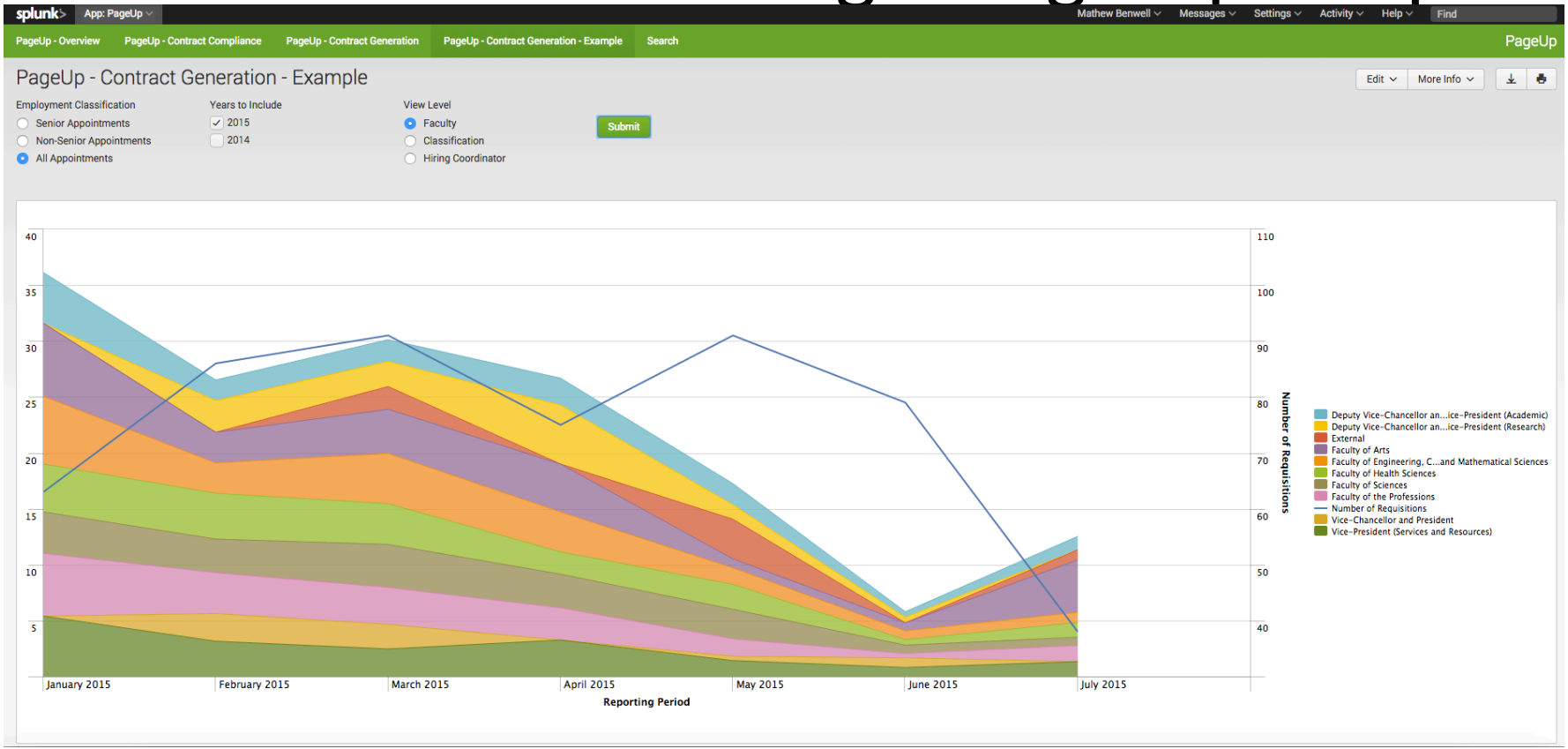
HR Contract Processing– Before Splunk

- Manual report extracted from PageUp
- Data massaged using Microsoft Excel
- Charting performed in Excel

HR Contract Processing – Page Up People



HR Contract Processing – Page Up People



HR Contract Processing - Outcome

- Report generation is automated

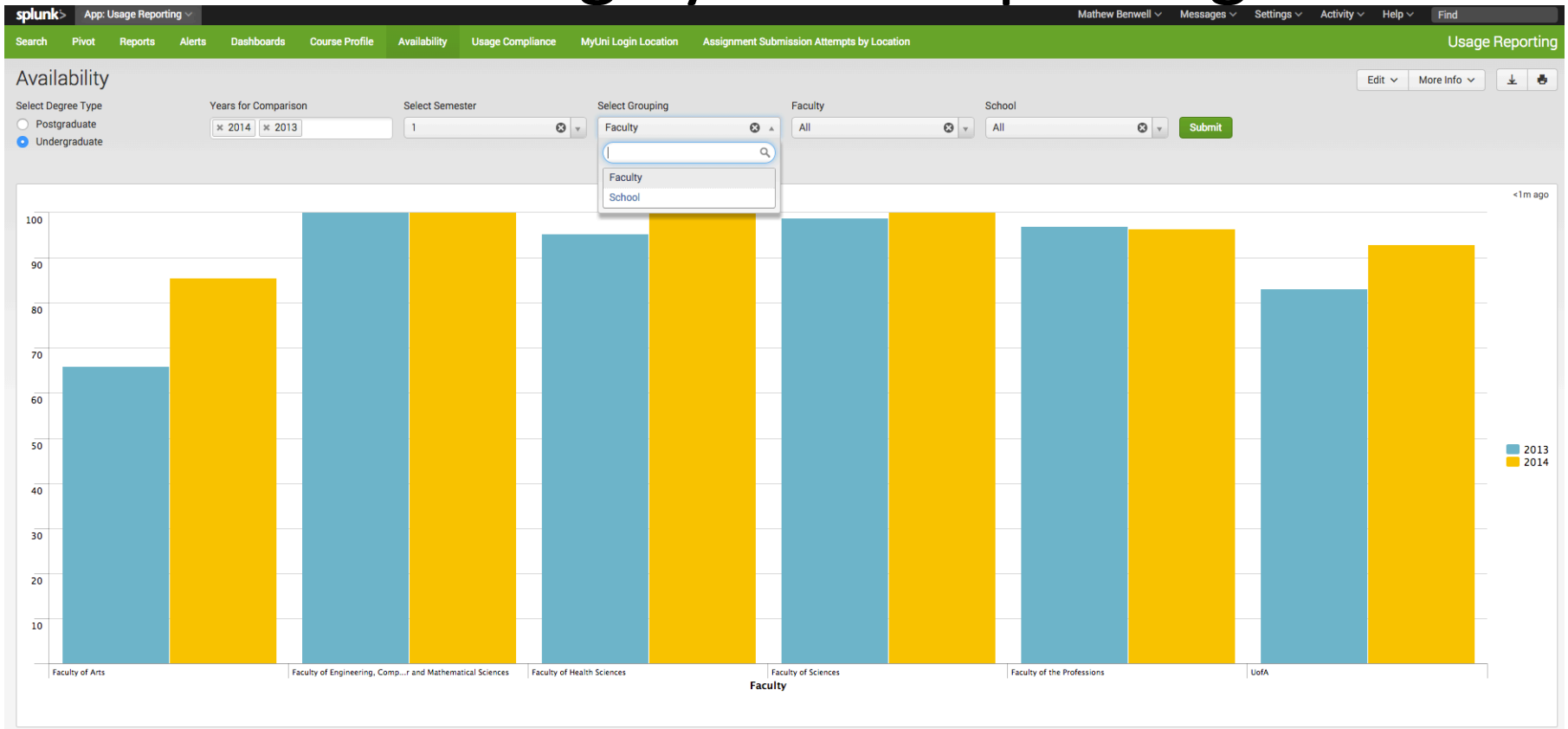
- Human Resources manual processes can be reduced, saving time and effort

- Virtually no cost

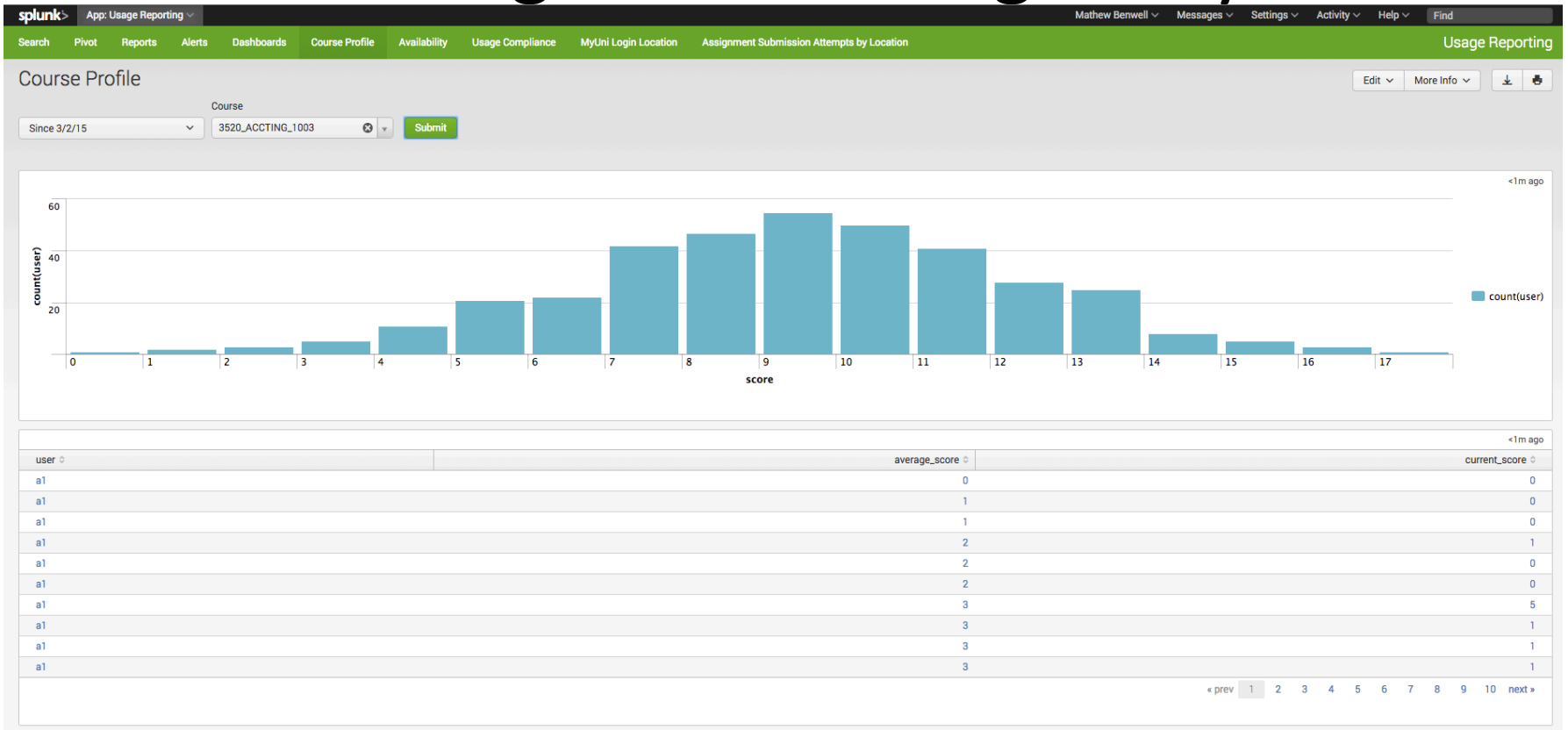
Learning System Reporting – Before Splunk

- Basic content reporting
- Team extract data from Oracle database
- Data is massaged into a usable form using Microsoft Excel
- Excel charts are copied into a Word report

Learning System Reporting



Extending into Learning Analytics



Learning System Reporting - Outcome

- Learning management team are developing their own analytics capability

- Reduce time and effort

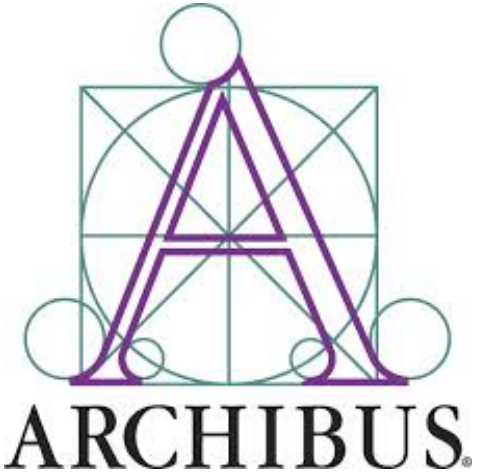
- Virtually no cost

Space Reporting – Before Splunk

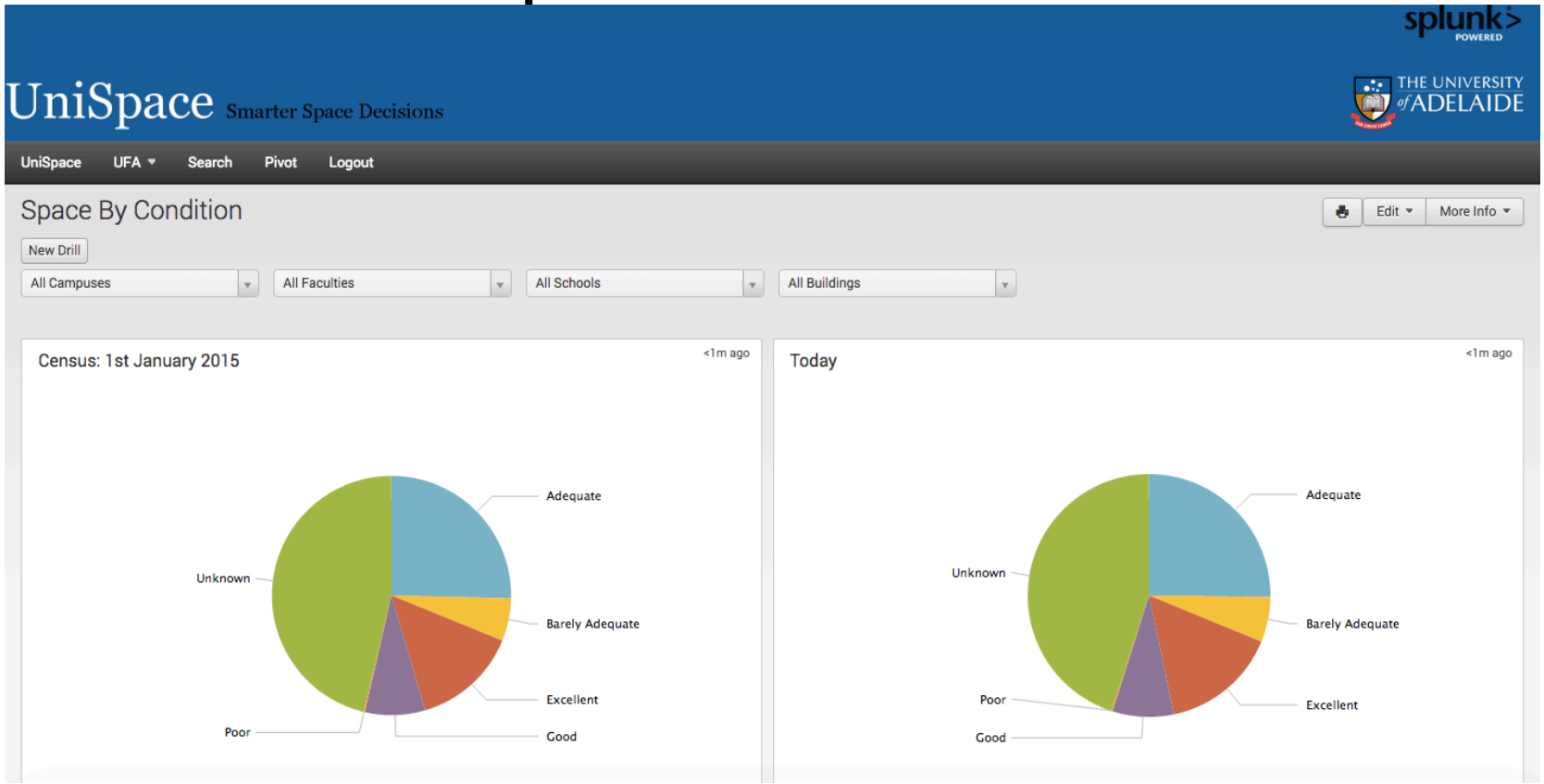
- School/Faculty managers request space allocation report
- Space Planning team extract data into CSV/Excel
- School/Faculty managers generate their own reporting

Space Reporting – Where Does Splunk Fit

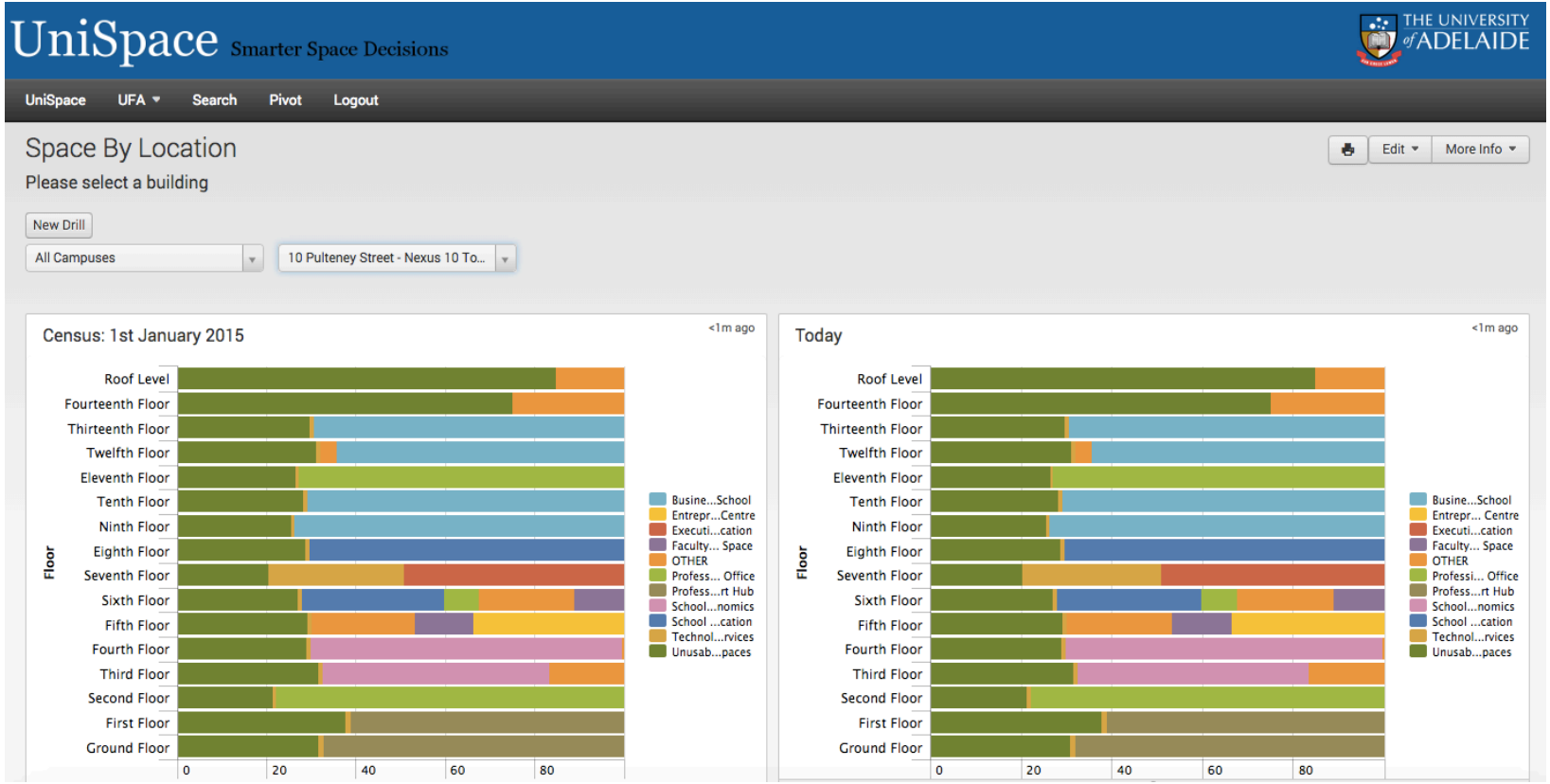
- Archibus Software - Facilities Management
- Splunk DB Connect
  - Nightly data feed from Oracle
- In-house Developed Splunk App
  - Dashboards - In-page Drilldowns
  - Side By Side direct comparison of change over time



UniSpace Dashboards



UniSpace Dashboards



A Quick Demo

splunk>

How Did We Build It?

1. Start with the question
   - What did we need to know?
2. Use case development
   - User flow diagrams (Storyboards)
3. Identify supporting data sources
4. Get Splunking
   - Macros heavily used
   - In-page drilldown script

Space Planning Reporting - Outcome

- School/Faculty managers have on demand access to the latest data
- No time requirement for Space Planning team
- Virtually no cost (25mb/day)

What Does the Future Hold?

- Continue to extend Splunk use
- More advanced Learning Analytics
- Increased space planning capabilities
  - Include fine grained occupancy data
  - Including charging data
  - Including facility capability
- Teaching area utilization (Lecture theatres)

Take-Aways

- Most Importantly: Don't think of Splunk just as an IT tool
- Splunk can be used for a lot of things
- Use a structured approach, starting with the question you want to answer
- Stick to the Splunk Common Information Model (CIM)
- Build a community within your organization

THANK YOU

splunk>