

The logo features the word ".conf2015" in white, sans-serif font inside a red speech bubble shape. The year "2015" is also present in the background network visualization.

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

Mathew Benwell
Information Security Specialist,
The University of Adelaide

The Splunk logo consists of the word "splunk" in a lowercase, bold, sans-serif font, followed by a registered trademark symbol (®) and a large, stylized, upward-pointing arrow.

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 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



.conf2015

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

splunk > App: UofA Security >

Mathew Benwell > Messages > Settings > Activity > Help > Find

Search Incident Response > Security Reporting > Antivirus > IDS > Network Traffic > Sinkhole > URL Filtering > Vulnerability Scan > Pivot Reports Alerts Dashboards UofA Security

IDS Reporting

during Sun, Feb 8, 2015

Total IDS Incidents 1m ago Total PAN IDS Incidents 1m ago Total SRX IDS Incidents 1m ago

24893 **19728** **5165**

IDS Incidents by Country

IDS Incidents by Severity

| severity | count |
|----------|---------|
| CRITICAL | ~500 |
| HIGH | ~17,500 |
| INFO | ~0 |
| MEDIUM | ~4,500 |

Security Uses – Anti-malware

Antivirus Reporting

during Mon, Mar 9, 2015

Total Malware Incidents <1m ago 316

Total McAfee Malware Incidents <1m ago 132

Total SCEP Malware Incidents <1m ago 24

Total PAN Malware Incidents <1m ago 160

Daily Virus Count by Source AV System <1m ago

The chart displays the daily count of viruses detected by three different antivirus systems. The x-axis represents time from 12:00 AM to 8:00 PM on Monday, March 9, 2015. The y-axis represents the count of viruses, ranging from 0 to 60. The legend indicates three sources: mcafee (blue), pan_logs (yellow), and sccm (red). The data shows a significant peak at 12:00 PM, with a total of approximately 50 viruses detected.

| Time | mcafee | pan_logs | sccm | Total |
|----------|--------|----------|------|-------|
| 12:00 AM | 2 | 1 | 0 | 3 |
| 4:00 AM | 10 | 0 | 1 | 11 |
| 8:00 AM | 12 | 0 | 2 | 14 |
| 12:00 PM | 10 | 40 | 2 | 52 |
| 4:00 PM | 10 | 5 | 0 | 15 |
| 8:00 PM | 10 | 10 | 0 | 20 |

McAfee Antivirus <1m ago

Top 10 by Malware Name

| Threat Name | count |
|----------------------|-------|
| JS/Downloader-BMA | 124 |
| Java/Adwind | 4 |
| Artemis!FC4953D088BE | 3 |

Microsoft System Centre End... <1m ago

Top 10 by Malware Name

| Threat Name | count |
|-------------------------------------|-------|
| TrojanDownloader.JS/Nemucod.F | 3 |
| Adware:Win32/SaverExtension | 2 |
| BrowserModifier:Win32/KipodToolsCby | 2 |

PAN Antivirus <1m ago

Top 10 by Malware Name

| Threat Name | count |
|-------------------------------------|-------|
| Virus/Win32.WGeneric.earot(2745008) | 66 |
| Virus/Win32.WGeneric.eaogs(2459134) | 17 |
| Virus/Win32.WGeneric.cwuuw(2003768) | 12 |

PAN Wildfire <1m ago

Top 10 by Malware Name

| Threat Name | count |
|-------------------------------------|-------|
| Virus/Win32.WGeneric.estcw(3010211) | 6 |
| Virus/Win32.WGeneric.estro(3084575) | 5 |
| Virus/Win32.WGeneric.esgfm(3065716) | 2 |

Security Uses: Looking For Bad Things

The screenshot shows the PhishTank homepage. At the top, it says "PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!" Below the header, there's a navigation bar with links for Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. The main content area features a section titled "Join the fight against phishing" with instructions to "Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API." It includes a search bar with placeholder text "Found a phishing site? Get started now — see if it's in the Tank:" and a button labeled "Is it a phish?". Below this is a table titled "Recent Submissions" showing 14 rows of data. The columns are ID, URL, and Submitted by. Most URLs are identical (http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap...), and they were all submitted by "cyscon". One row is submitted by "phishReporter".

| ID | URL | Submitted by |
|-------------------------|---|---------------|
| 2369934 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369933 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369932 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369931 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369930 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369929 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369928 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369927 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369926 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |
| 2369925 | http://zahbia.net/pcu/xx.php | phishReporter |
| 2369924 | http://archiwum.zielonewydarzenia.pl/bip/php/dd/Ap... | cyscon |

Security Uses – Incident Response

The screenshot shows a Splunk search interface with two main panels. The left panel displays a table of 'Related Domains' with columns for time, initial_domain, and Hon. Sc. The right panel shows a table of 'Activity' with columns for domain and misc.

| _time | initial_domain | Hon. Sc. |
|---------------------|----------------|----------|
| 2015-05-07 09:05:32 | kengusar.org | |
| 2015-05-07 09:05:07 | kengusar.org | |
| 2015-05-07 08:45:39 | kengusar.org | |
| 2015-05-07 08:45:33 | kengusar.org | |
| 2015-05-07 08:41:31 | kengusar.org | |
| 2015-05-07 08:38:53 | kengusar.org | |
| 2015-05-07 08:16:36 | kengusar.org | |

| domain | misc |
|-----------------------|--|
| kengusar.org | kengusar.org/ |
| spynet2.microsoft.com | spynet2.microsoft.com |
| copy.com | copy.com/ |
| violation-notice.com | violation-notice.com/p id= [1] [4] [1] [4] |
| violation-notice.com | violation-notice.com/k id= [] [] |
| violation-notice.com | violation-notice.com/ix id= [000] [4] |
| violation-notice.com | violation-notice.com/z id= [] [] |

Security Uses – Incident Response

splunk > App: UofA Security

Mathew Benwell > Messages > Settings > Activity > Help > Find

Search Incident Response Security Reporting Antivirus IDS Network Traffic Sinkhole URL Filtering Vulnerability Scan Pivot Reports Alerts Dashboards UofA Security

Related

| Time | User | IP | Action | URL | Time |
|---------------------|---------------|-----------------|---------------|--|---|
| 2015-05-07 08:38:03 | kengusar.org | 195.242.161.151 | web-browsing | art7.kiev.ua/system/logs/9u15b2HilmPjr.php?id= | 1m ago |
| 2015-05-07 08:38:03 | -1 | 46.161.30.201 | web-browsing | violation-notice.com/assets/afp-global-styles-002.css | 1m ago |
| 2015-05-07 08:38:03 | -1 | 46.161.30.201 | web-browsing | violation-notice.com/assets/import.css | 1m ago |
| 2015-05-07 08:38:03 | -1 | 46.161.30.201 | web-browsing | violation-notice.com/ix8sw4g.php?id= | 1m ago |
| 2015-05-07 08:38:03 | -1 | 64.235.151.46 | ssl | copy.com/ | |
| 2015-05-07 08:38:03 | -1 | kengusar.org | 0.250000 | 1 0 1 | 2 46.161.30.201 web-browsing violation-notice.com/ix8sw4g.php?id= |
| 2015-05-07 08:38:03 | -1 | kengusar.org | 0.250000 | 1 0 1 | 2 46.161.30.201 web-browsing violation-notice.com/ix8sw4g.php?id= |
| 2015-05-07 08:38:03 | 185.42.15.147 | ssl | kengusar.org/ | 1.30.201 web-browsing violation-notice.com/ix8sw4g.php?id= | |
| 2015-05-07 08:38:09 | | | | 5.151.46 ssl copy.com/ | |



.conf2015

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

Splunk > App: Internet Usage

Mathew Benwell > Messages > Settings > Activity > Help > Find

Internet Usage

Search Today's Offnet Usage Weekly Offnet Usage Annual Offnet Trends Annual Offnet Traffic Comparison Pivot Rate Limiting Reports Detailed Usage

Today's Offnet Usage

Total Offnet Usage (GB) 7m ago

Inbound Offnet Usage (GB) 7m ago

Outbound Offnet Usage (GB) 7m ago

Edit More Info  

535.212 522.678 10.034

Users Rate Limited Today 37m ago

| _time | Name | User | policy | Gigabytes | Status |
|---------------------|------|---------|------------------------|-----------|---------|
| 2015-09-07 14:00:00 | F | uofa\al | RateLimitAllUsage | 18.91 | success |
| 2015-09-07 14:00:00 | H | uofa\al | RateLimitAllUsage | 15.95 | success |
| 2015-09-07 14:00:00 | M | uofa\al | RateLimitAllUsage | 9.60 | success |
| 2015-09-07 14:00:00 | J | uofa\al | RateLimitAllUsage | 8.49 | success |
| 2015-09-07 14:00:00 | Z | uofa\al | RateLimitAllUsage | 7.88 | success |
| 2015-09-07 14:00:00 | K | uofa\al | RateLimitHighUsage | 5.48 | success |
| 2015-09-07 14:00:00 | C | uofa\al | RateLimitHighUsage | 4.19 | success |
| 2015-09-07 13:00:00 | Z | uofa\al | RateLimitHighUsage | 4.12 | success |
| 2015-09-07 14:00:00 | J | uofa\al | RateLimitModerateUsage | 3.54 | success |
| 2015-09-07 10:00:00 | K | uofa\al | RateLimitModerateUsage | 3.42 | success |

« prev 1 2 next »

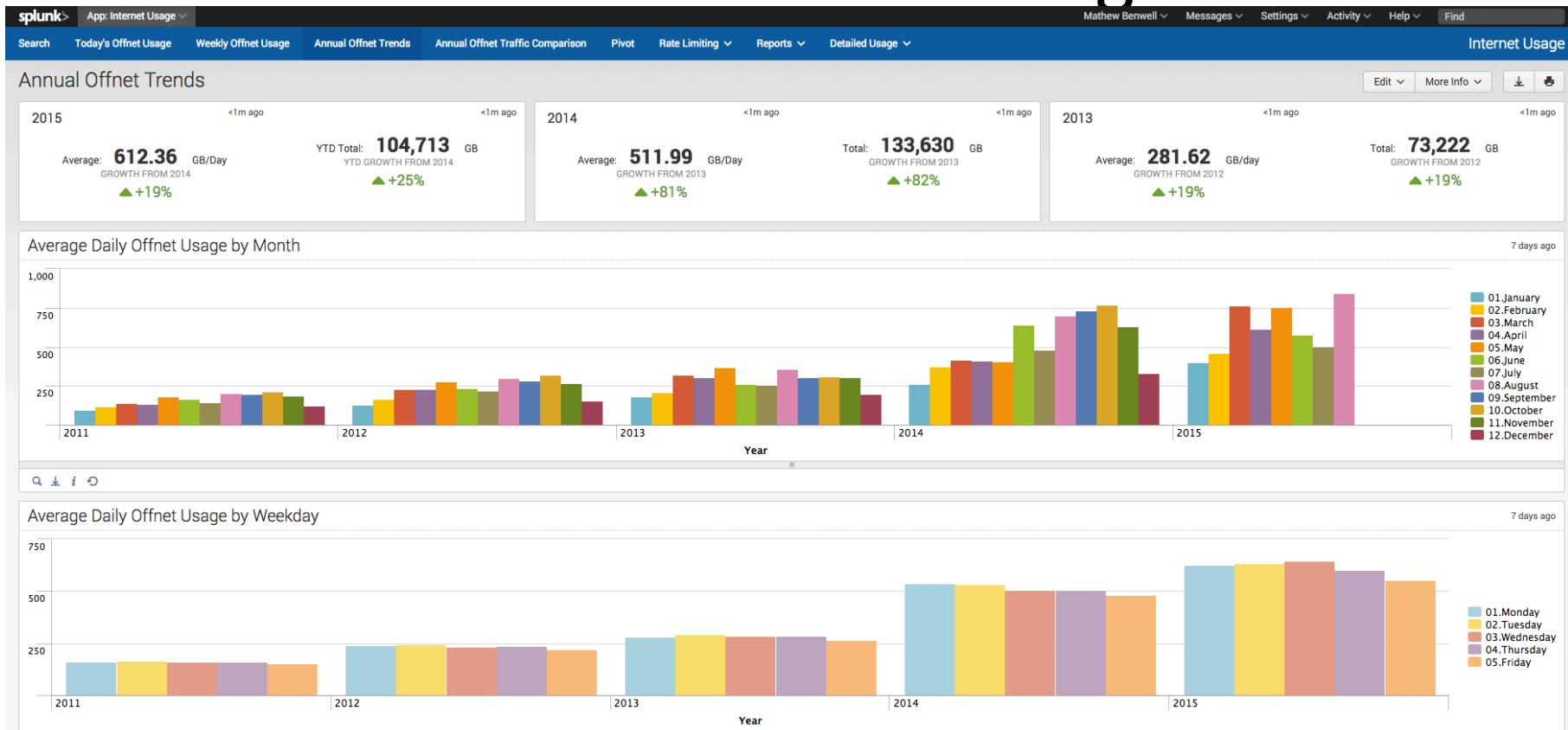
Top 10 Applications 7m ago

| Application | Download |
|--------------|----------|
| web-browsing | 183.43 |
| ssl | 80.95 |
| dropbox | 62.22 |
| httpsvideo | 60.05 |

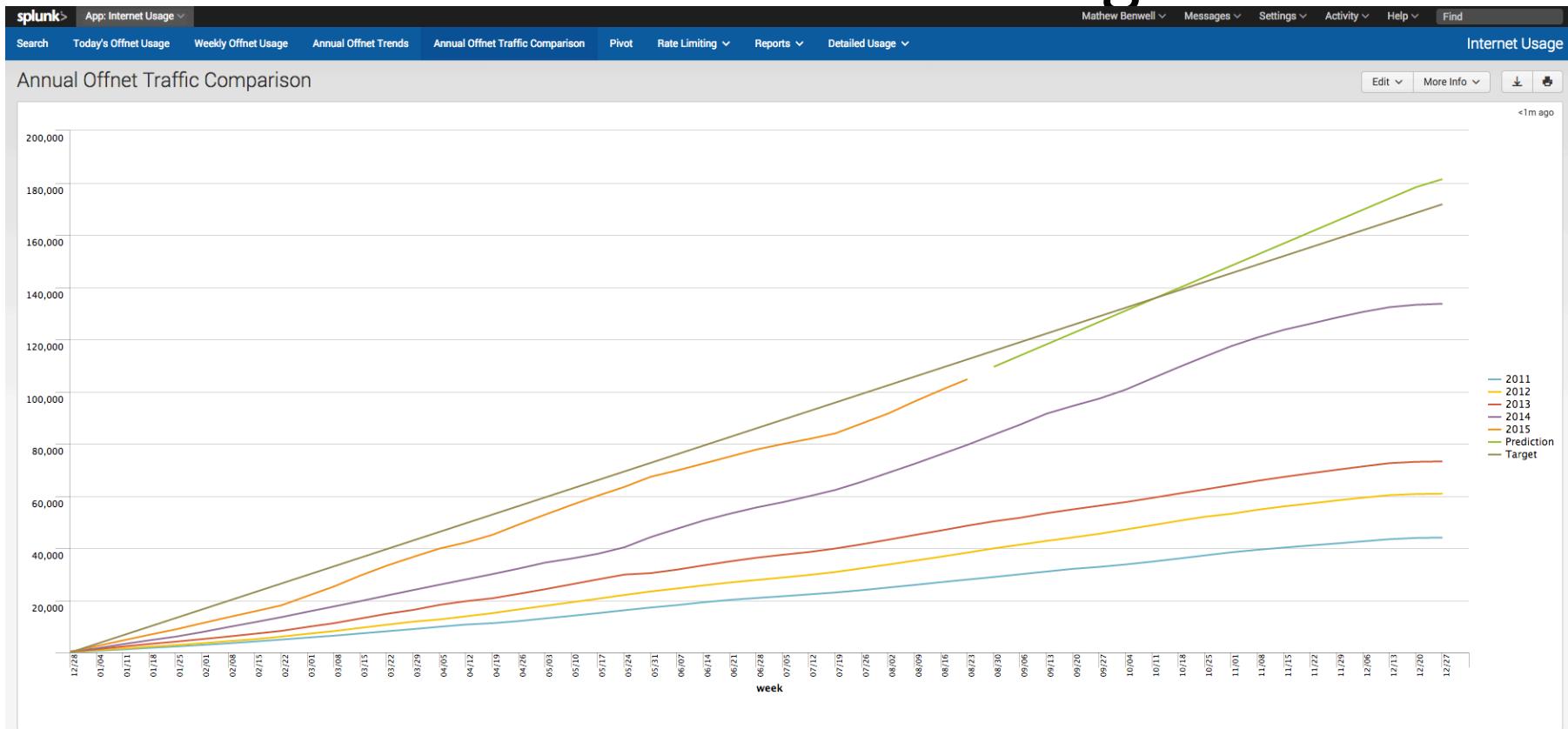
Top 10 Known Users <1m ago

| User | mail | eduPersonAffiliation | Download |
|------|-------------|---------------------------------|----------|
| a1 | n...@...au | Student | 18.91 |
| a1 | hi...@du.au | Student PGCW Masters Student | 15.95 |
| a1 | cl... | Staff | 10.06 |

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

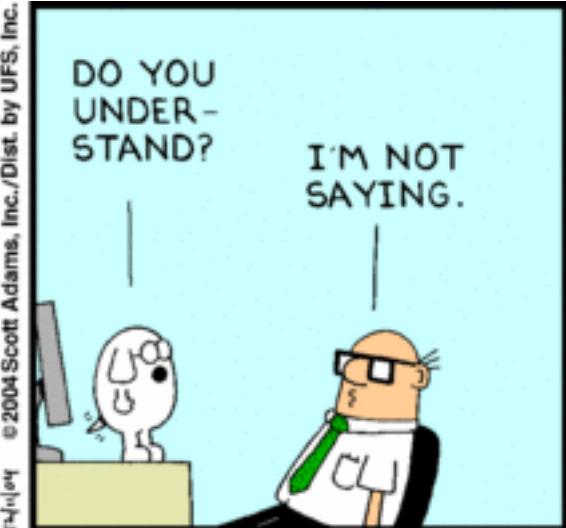
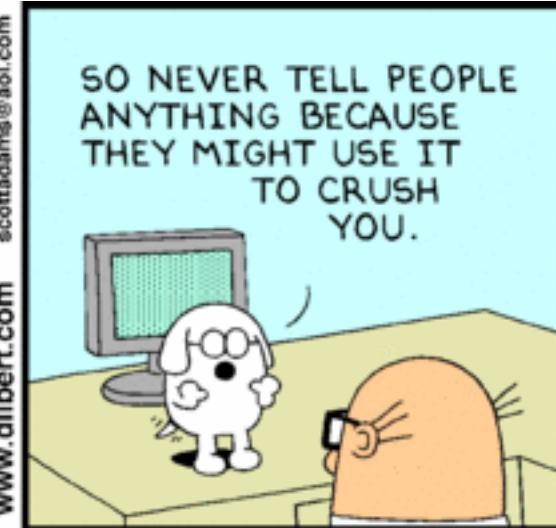
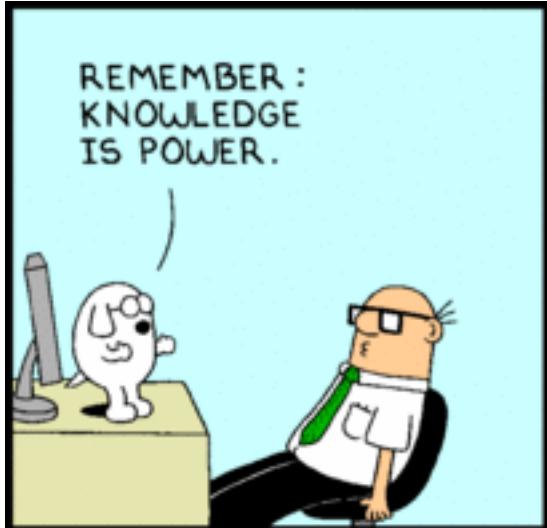


- We are helping to control cost

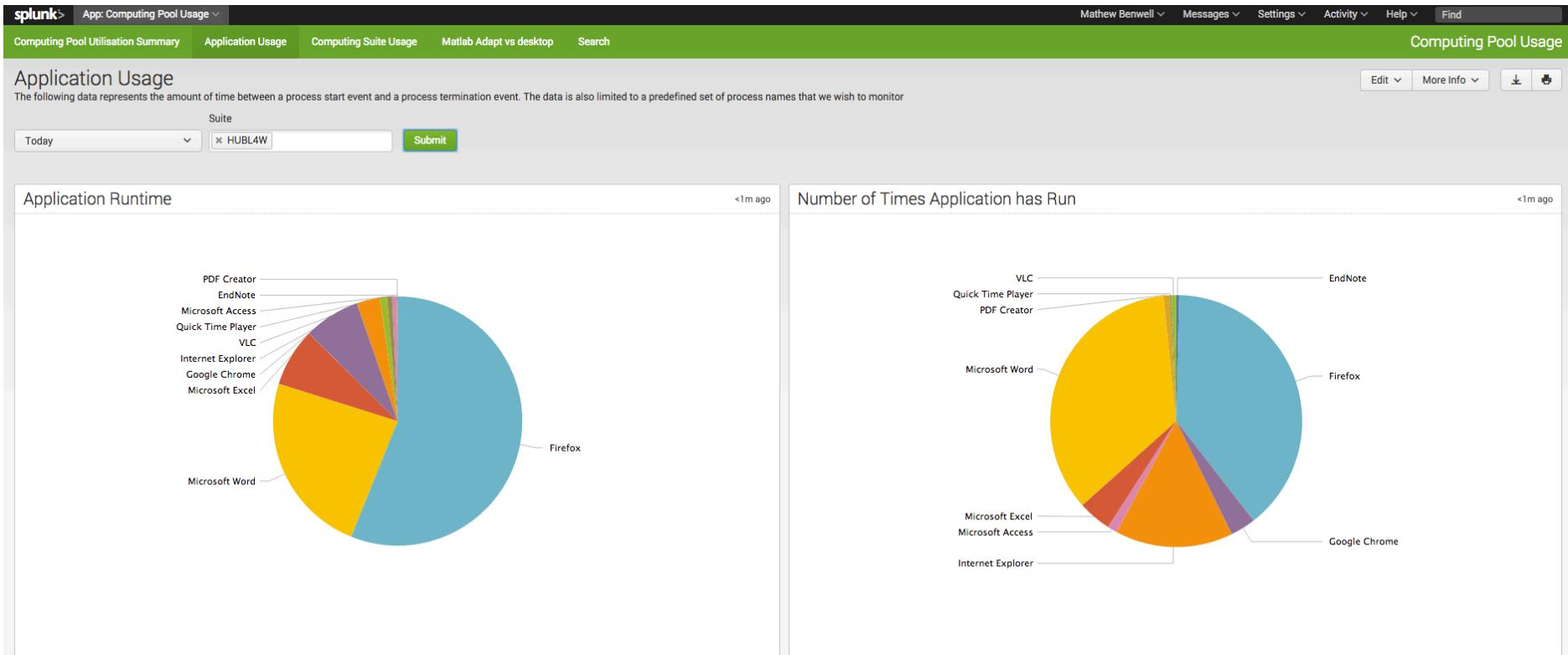


- No cost, we already have the data for Security

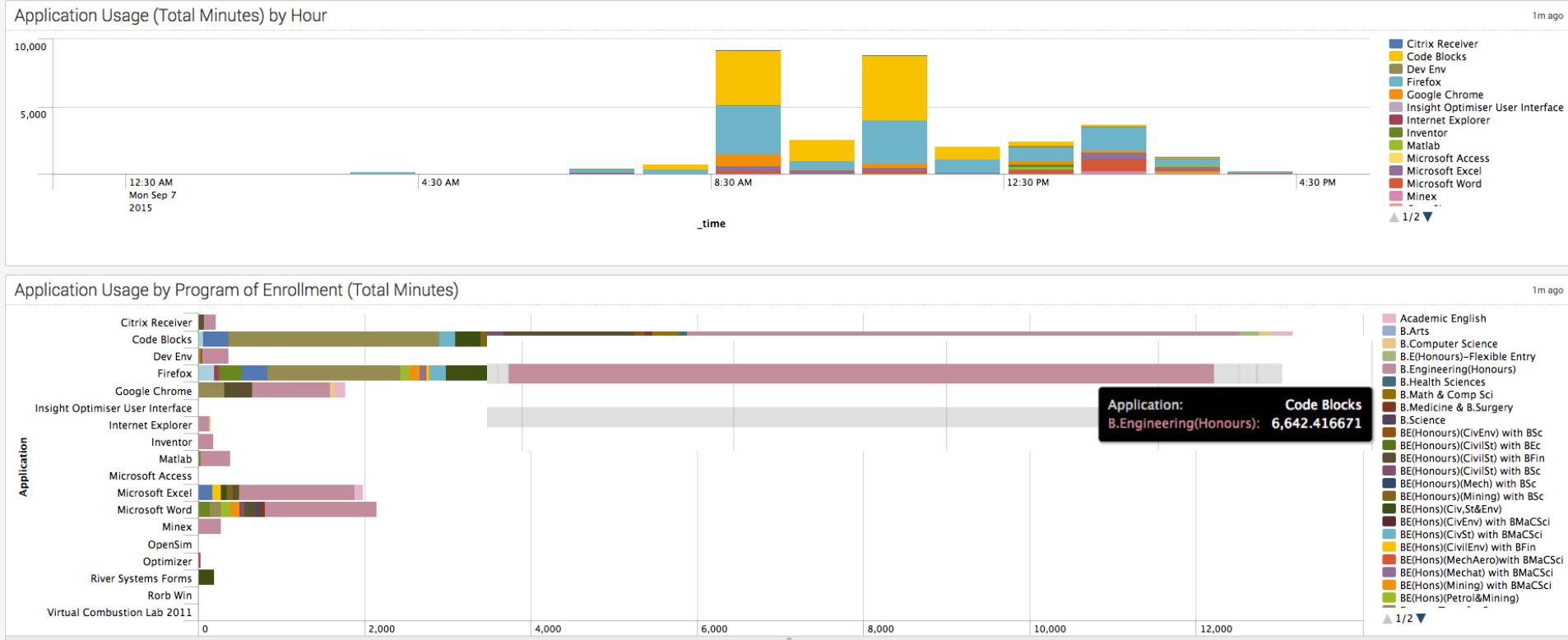
Computing Suite Utilization



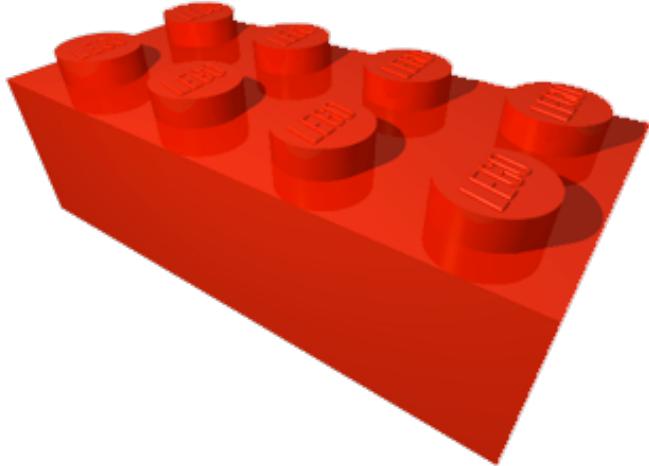
Computing Suite Utilization



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)



.conf2015

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)

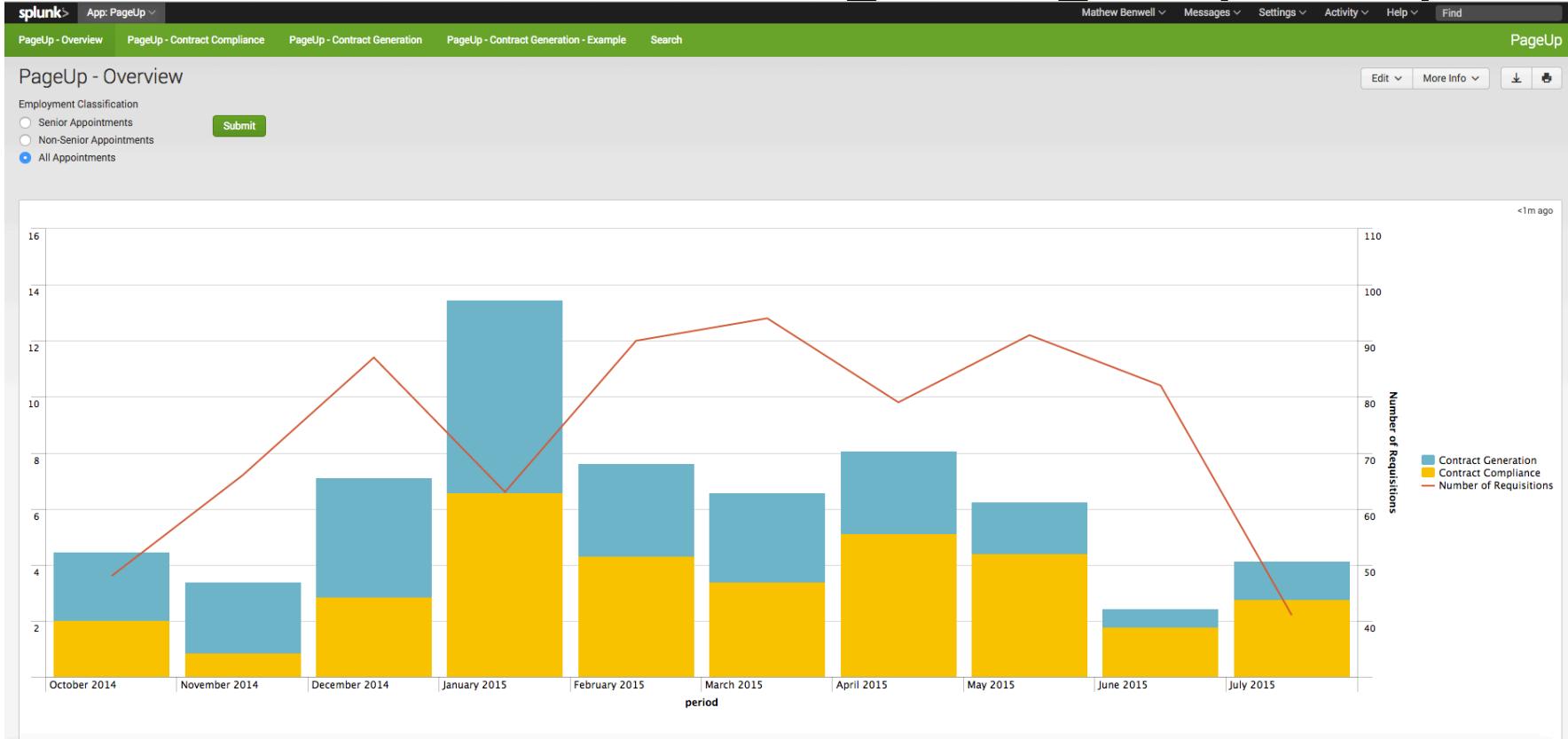


HR Contract Processing— Before Splunk

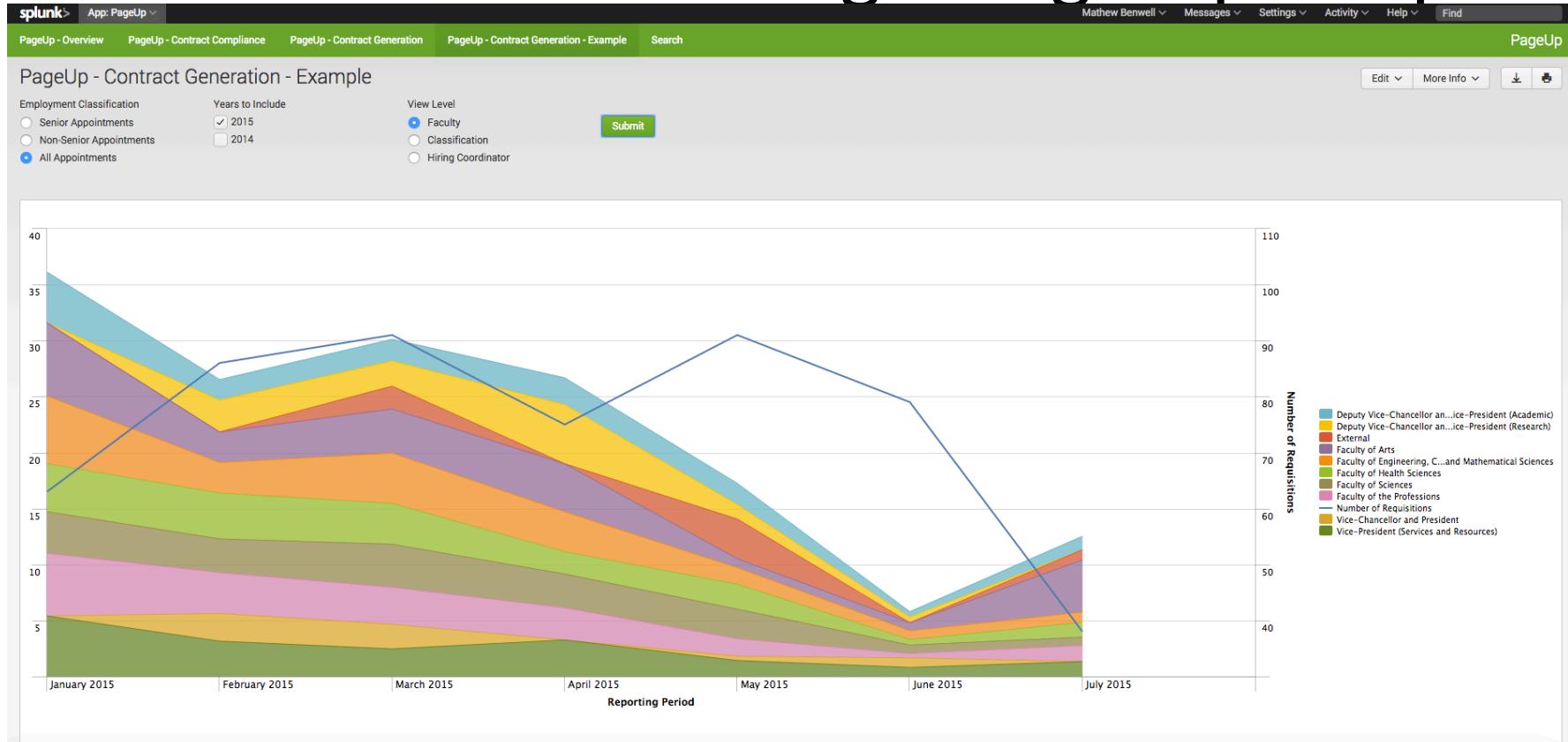
- Manual report extracted from PageUp
- Data massaged using Microsoft Excel
- Charting performed in Excel



HR Contract Processing – Page Up People



HR Contract Processing – Page Up People



HR Contract Processing - Outcome



- Report generation is automated

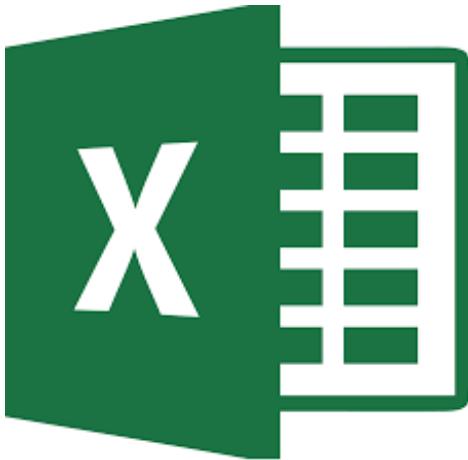


- Human Resources manual processes can be reduced, saving time and effort



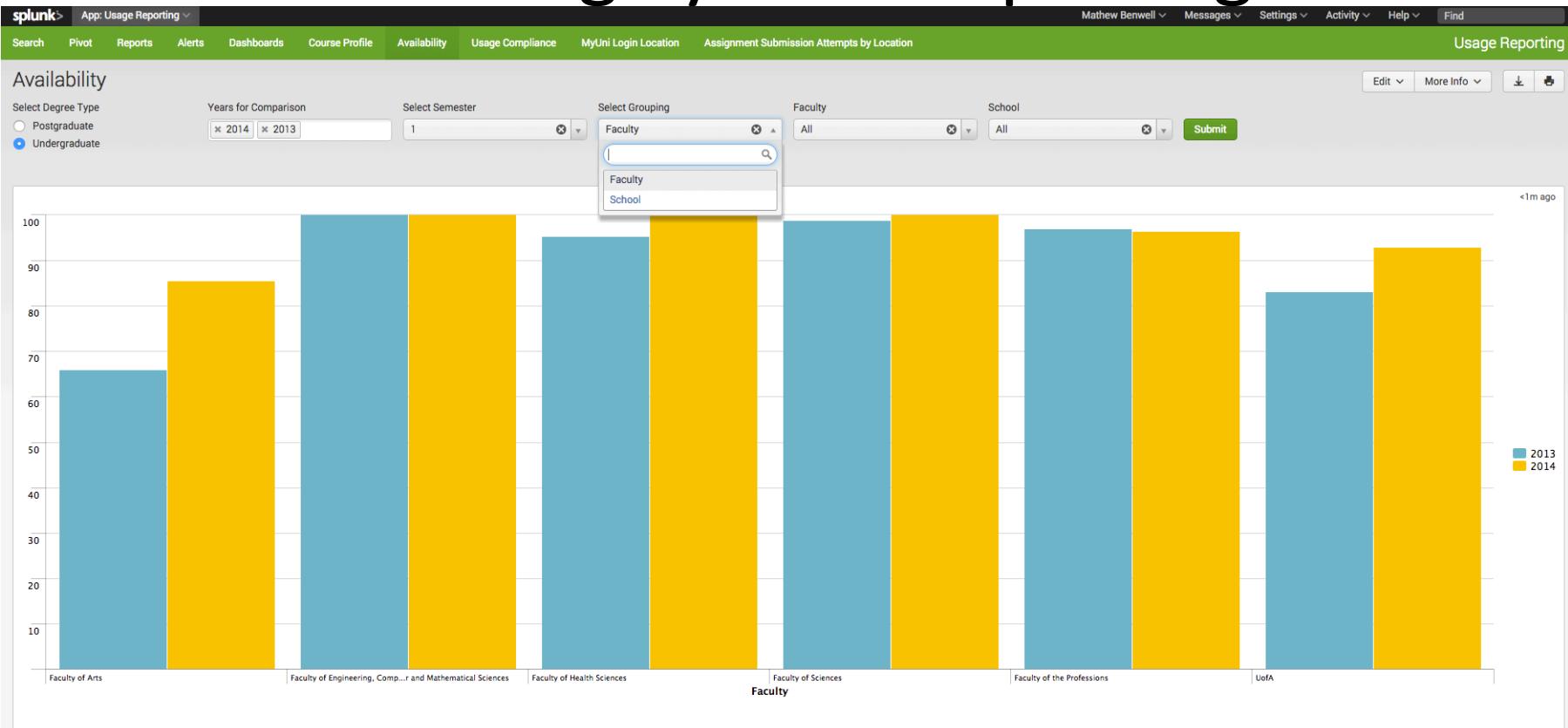
- Virtually no cost

Learning System Reporting – Before Splunk

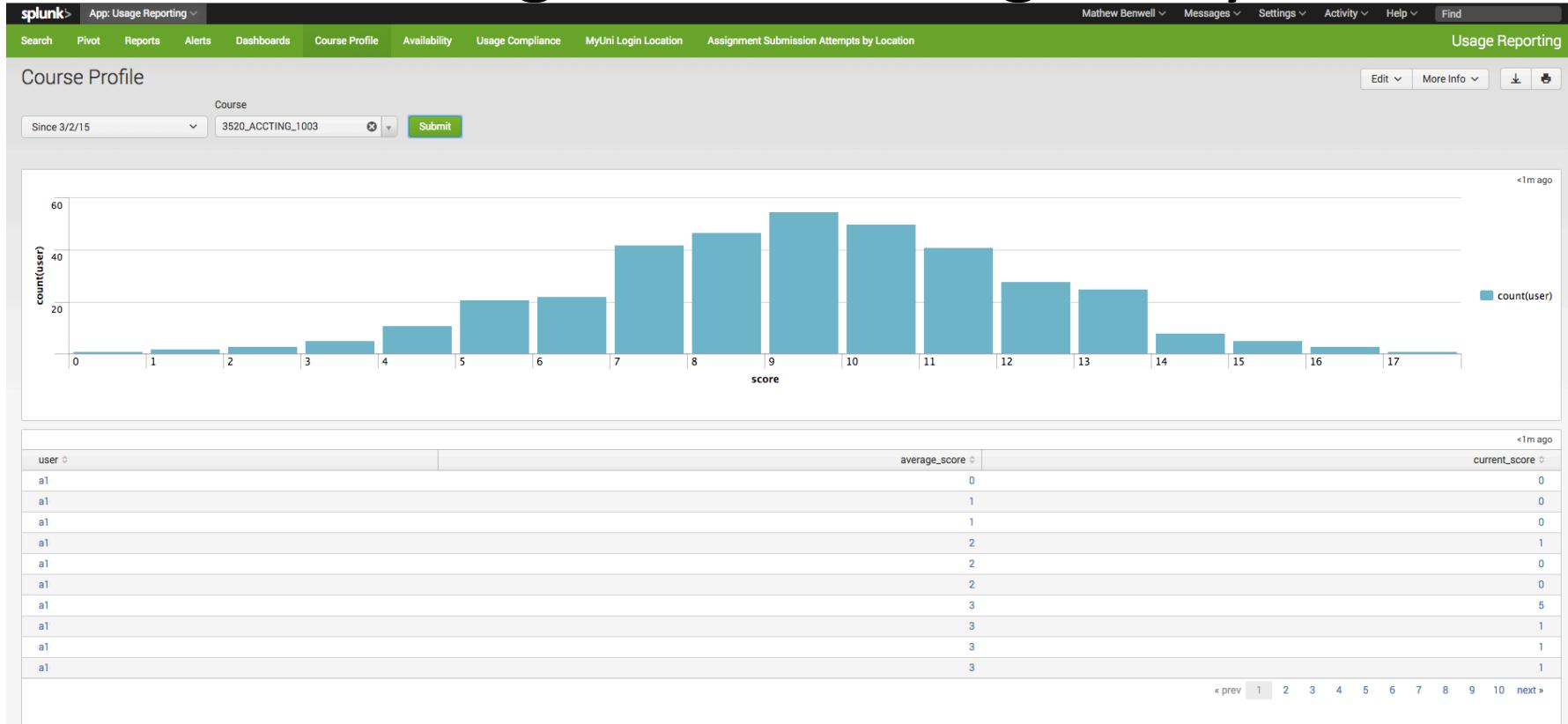


- Basic content reporting
- Team extract data from Oracle database
- Data is massaged into a usable form using Microsoft Excel
- Excel charts are copied into a Word report

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

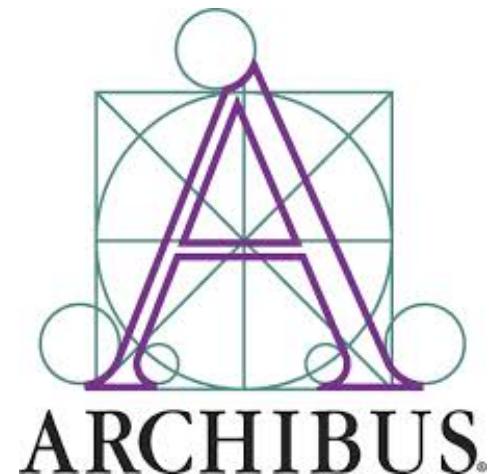
Space Reporting – Before Splunk



- 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

splunk>
POWERED



UniSpace Smarter Space Decisions

UniSpace UFA ▾ Search Pivot Logout

Space By Condition

Edit ▾ More Info ▾

New Drill

All Campuses

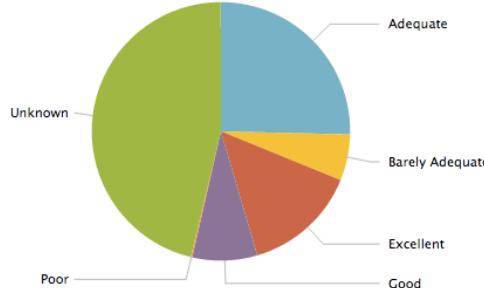
All Faculties

All Schools

All Buildings

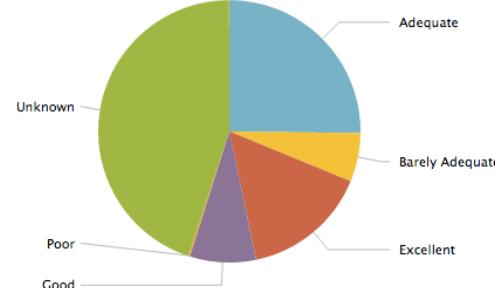
Census: 1st January 2015

<1m ago



Today

<1m ago



UniSpace Dashboards

UniSpace Smarter Space Decisions



UniSpace UFA Search Pivot Logout

Space By Location

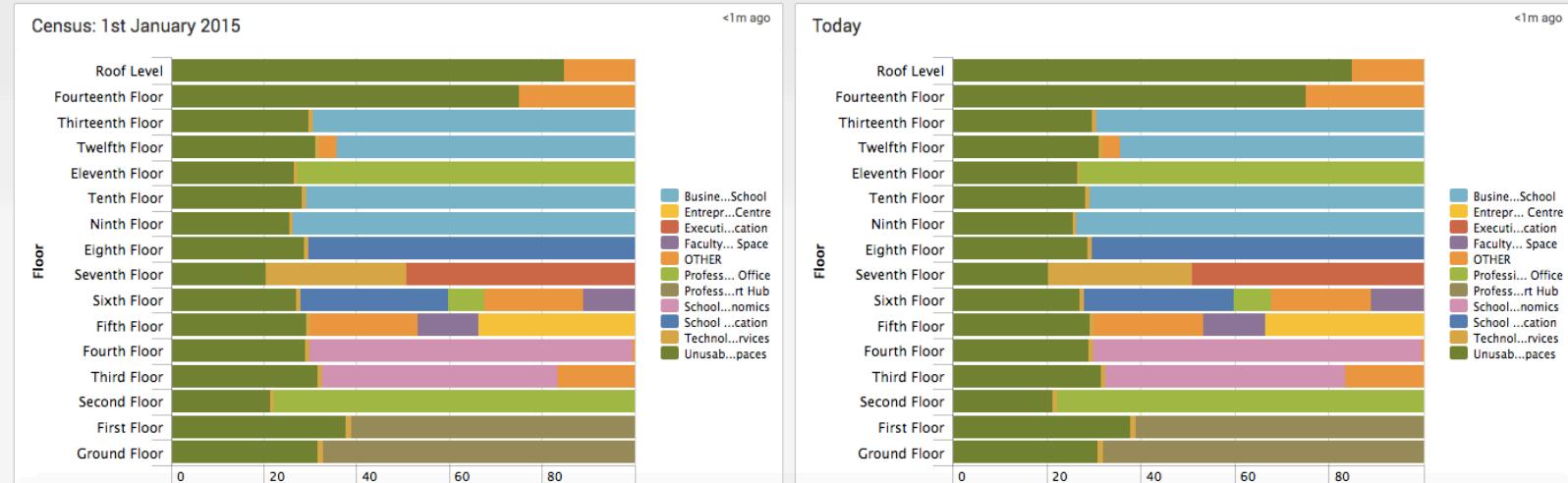
Please select a building

New Drill

All Campuses

10 Pulteney Street - Nexus 10 To...

Edit More Info





.conf2015

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

.conf2015

THANK YOU

splunk®