July 2016 d5c95

July 2016 Harvard IT Summit 2016

July 2016 Harvard IT Summit 2016

- Keynote by Isaac Kohane, Chair of Dept of Bioinformatics at HMS
- Older Examples of drugs causing heart attacks that weren't caught because lack of data
- Newer example can catch domestic abuse via bioinformatics 2 years before diagnosis
- But …

o When not properly understood, could be misapplied

o Example of men having a better than 50% chance of dying w/in 3 years if they get a white blood count test between 12am and 8am

o No causality blood tests in the middle of the night are always done for someone who is really sick and having an emergency

- Goal get medical diagnosis as good and predictive as Netflix
- Billing codes are not accurate data points on diagnosis. It's about billing and figuring out payment. Lots of deliberately incorrect data there. Instead, they're doing natural language processing on the medical records getting better info on health/illness trends
- Recent story of young researchers able to use Kohane's data to test a theory (and it was true) to identify causal link between cardiac angiogenic imbalance and peripartum cardiomyopathy due to the data being available in a secure manner
- Trend of great medical research and solutions emerging from data mining and passion to solve a problem great work even being done by people who don't have medical backgrounds
- Should be moving more bioinformatics compute to the cloud to increase security. On-prem health systems too antiquated, legacy. Should get more professional management.
- HMS and hospitals charged w/ moving several level 4 / HIPAA-compliant systems to the cloud

o Dedicated instances on AWS

o 1 account w/ multiple VPC's

o Encrypt everything

o Audit everything

o / HTTPS://grdr.hms.harvard.edu/

o undiagnosed diseases network building on their success and expanding it through NIH. We're hosting these other sites because we've proven we can do it.

- he monitors his 90 year old mother's weight via Fitbit. recently made a diagnosis re: her diarrhea based on Fitbit data that saved her from an ER visit
- Anecdote about EPIC being really expensive over time, complex, running on antiquated code, transformative but also creates lots of new problems
- Why can't healthcare IT be more like Minecraft?~

10:50 Creative Pedagogy: MOOCs - Diane Moore from Harvard Divinity School, Sever Room 103

- Experiences w/ MOOC and EdX on "World Religions through Their Scriptures"
- Started out w/ concern that it is still interactive, not just barfing out content
- Also wanted to bring in variety of people from around the world, various perspectives and faiths, into a constructive dialogue
- Metrics for course

o 330k total enrolled

o 31k currently enrolled

o About 10k - 15k in individual courses in the series

- multiple courses in a series Islam, Hinduism, Judaism, Religious Literary, Christianity. Each course runs about a month.
- Moving beyond information-driven delivery (MOOC's grew out of STEM courses - lots of data, info, multiple choice)
- One of the reasons that Harvard helped establish EdX to make MOOC's more useful for humanities
- Anecdote: Harvard also has a competing initiative on "reverse classrooms" with HILT where it's more focused on student interaction/involvement rather than real-time lecture
- Think creatively about increasing student engagement
- 3 rules for this course:

o DON'T LECTURE - videos would be 2-4 minutes in length

o Create a constructive, respectful classroom environment

- EdX platform is incredibly sophisticated and powerful. Discussion and collaboration were weaker.

o Had to use Facebook for a while to provide a better discussion experience

- MOOC opportunities are profound, but need to continue to focus on engagement and collaboration
- They've also been using MIT's UnHangout customized Google Hangouts for realtime collaboration for breakout rooms and RT discussions
- Another realization aesthetics matter! Great web interface, the quality of the videos and animations are high and has an impact
- Something that didn't work very well annotation w/ close text reading. It was overwhelming and not very useful.
- Using maps for visualization also didn't work that well. Mapping tools for creators rather than programmers.

12:15 InfoSec 2015 "Summer of our Discontent" Incident Review by Nathan Hall, HUIT InfoSec, Emerson Room 105

- APT as a term was originally coined by Air Force trying to find a way to say "China" without actually saying China
- APT Lifecycle

o Initial recon

o Compromise

o Establish foothold

o Escalate privileges

o Internal recon

o Move laterally

o Maintain presence

o Repeat

o Complete mission often data exfiltration

- Apr 2015

o Vulnerable Wordpress server

o Remote access tool (RAT) was installed

- PlugX
- Command and control to a ./ ddns.net/ domain

o Credential dumping tool downloaded

o Cached domain admin credentials captured

- Hashed via NTLM but you can also just copy the hash w/out breaking it

o RAT installed on 4 other servers

- May/June 2015

o FAS/Central

o Hacked a cold fusion web server

o Dumped cached credentials for FAS domain admin and local admin

o Installed more RAT's and back doors

o Got access to some FAS domain controllers and installed some PlugX

o Were able to laterally move to University AD via a popped account and installed RAT and C&C

o Were doing this all via net login

o Couldn't access the boxes via RDP since they were blocked

o They popped a linux host via shell shock. Installed a proxy and began tunneling traffic for RDP to domain controllers

- August / HKS

o Email scan from a Xerox multifunction printer

o Installs malware on systems

o Dumped credentials

o Got local admin

o Move laterally

o Installed back doors via SeaDuke

o Get domain admin account

o Used compromised credentials to access VPN - HKS tunnel

o Whack-a-Mole

o Domain admin activity noticed - Mid August

o Compromised VPN accounts de-activated

o Then they activated back doors

o Additional activities

- Connect to domain controllers, run power shell scripts (lots of these)

o big remediation project

- Password changes
- Privilege separation
- LAPS
- Crowdstrike

o Return to the scene in Sept thru Nov

o Connect to VPN via other popped accounts

o Found a domain admin account that wasn't updated

o Dumped entire SAM database

o Popped other servers

o Got email administrator password

- Were looking at admin chatter too on response to their activities
- Accessed emails for people of interest
- HLS

o Initial compromise in Apri 2015

o Room book application (EMS)

o Upload attachment to an event

o Uploaded a web shell and other tools

o Went dormant for a month

o Eventually logged onto 4 servers and installed a RAT on a domain controller

o Got caught in late June remediation. Popped domain controllers taken off line

o Domain admin passwords changed

o Didn't catch everything

- Service on DC still there

- Room book vulnerability re-used
- Ran power shell scripts
- Key Trends and lessons learned

o Unmatched servers/services

o Web servers in AD = tragically bad

o Password re-use = bad

o Insufficient privilege separation and domain admin use

o Insufficient protection for DC's

o Unusual activity from privileged accounts

1pm DevOps by Mark Boudreau HUIT Cloud, Emerson, Room 305

- Term DevOps getting overused and misapplied
- Core conflict between development_promoting change and operations_promoting stability
- DevOps tools conferences teams missions etc have all emerged to magically solve the problem
- In 2007-2008, Patrick Debois and Andrew Shafer trying to apply agile methodologies to infrastructure
- In 2008, flicker blog post 67 deploys of over 400 changes in 1 week.

o 10 deploys a day

- What were they doing as a company to move at that kind of speed?
- Started a huge shift in the conversation
- In 2009, Twitter hashtag created DevOps as a term for a conference
- In 2010 CALMS concept

o Culture

o Automation

o Lean manufacturing principles

o Measurement

o Sharing

- Phoenix Project in 2013
- 3 principles to DevOps in Phoenix Project

o Flow - Systems thinking

- Examine entire flow of manufacturing process

♣ What works well

♣ What are the slow downs or bottlenecks

- way to address more automation
- Way to address keep batch size of changes small (rather than huge deployments of lots of changes)
- Defects passing down stream - bad. Testing changes should be part of workflow from the beginning

o Amplify Feedback loops

- Continuous integration tools like Jenkin
- Get instant feedback
- Run automated testing and get results back rapidly
- Should do the same thing for the team and processes
- If it moves, measure it

o Continual learning and experimentation

- Continual improvement

♣ Understand the direction

♣ Grasp current condition

♣ Establish next target condition

♣ Iterate towards the target condition

- don't be afraid to take risks and make mistakes, just be committed to learning from those mistakes
- What does this mean for Higher Ed?

o Good = higher Ed has lots of money

o Bad = higher Ed has had money for a long time. lots of technical debt

o The 3 principles above don't just apply to the sexy new cloud stuff, can apply to all aspects of IT even the old stuff

o It's not about the tools, it's about the culture

o Gene Kim the way you organize yourself can pre-ordain failure

o Need to foster the basic principles and culture

- Amazon now doing deployments every 11 seconds
- High performing IT organizations experience 60 times fewer failures and recover from failure 168 times faster than their lower performing peers

2:20pm Infrastructure Poker - RC, Sever 103

- NEWS - secured $1.6m to expand MGHPCC to add 2 new pods
- Old infrastructure - big chillers, physical plant
- New infrastructure credit cards to rent cycles at cloud providers
- New SIeM microscopes
- 1 cubic millimeter of brain = 1 petabyte
- 3TB every hour
- 1 Sanger institute per hour
- Trends in RC

o Clouds

o Facilitation

o “Long tail (Comet, JetStream, Bridges) < NSF

o Containerization

o Algorithmic complexity

o Novel devices - FGPA, GPGPU, ASIC

o Storage and data retention

o Talent pool & training (ACIREF, software carpentry)

3:30pm Keynote Bryson Koehler, VP IBM, CITO, The Weather Company

- At Weather, he is both CIO and CTO
- Debated with himself re: flexibility_speed_agility vs. stability/reliability
- How to change the culture to take more risks?
- Culture is the way you think, act, and interact
- Increasing commoditization of enterprise IT tools we used to spend lots of money/ time running
- These days most of these systems are replaced w/ commodity/cloud-based services

o Google Apps, Salesforce, Google Hangout, AWS, etc.

- To be fluid w/ business, we had to change our engineering principles:

o Aligned w/ business

o No science projects

o Be agile

o Improve quality

o Be financially disciplined

o Foster an engineering culture of trust and accountability

o Have an engineering discipline that scalable, robust, can be relied on

o Ensure collaboration and learning

o Easy discovery, re-use, and extension of artifacts, assets, services

o Minimize technical debt

o Improve availability SLA

o Rationalize/simplify and cloud ifs

o Be vendor/technology agnostic as much as possible

- Technology Goal incorporate more IoT data into weather data aggregation. Many sensors

o Not a weather platform but a data platform

- Collecting data from planes, personal weather stations, info from thermostats, weather/vehicle data from cars, user devices (the weather app on phones), engines
- On a 3 day basis, they're about 70%-ish accurate
- When they get it wrong, it's because they have the wrong data to begin with
- 100tb worth of data every day

o Over 530m personal weather station reports

o Over 9m webcam uploads each day

- weather company has 96 surface observations in Bay Area versus US weather only have 14
- They aggregate 170 unique forecast model runs each day
- To create forecasts on demand for 2.2b precise locations
- Updated every 15 minutes
- Maintaining big run books aren't sufficiently agile to keep up w/ 6 changes a day

- Focus on measurement

o Measuring server performance doesn't tell the right story

o Measure based on end user performance/experience

- CIO's were constantly having to fix their budget regardless of demand, lowering service levels to meet budget
- Had to shift to a unit cost basis - not a flat budget

o Maps to revenue more cleanly

- "Safe is risky"

o Older, slower processes that focus on reliability versus speed/time to market are risky to the success of the business

o Need to be more comfortable taking calculated risks

- Commit

o Change what gets measured

o Remove barriers

o Single person accountability

o Rapid decision making

o Know your customers

o Play to your strengths

o Supplement your weakness

o Have the courage to decide

o Be the chief disorganizer

#learning/conferences