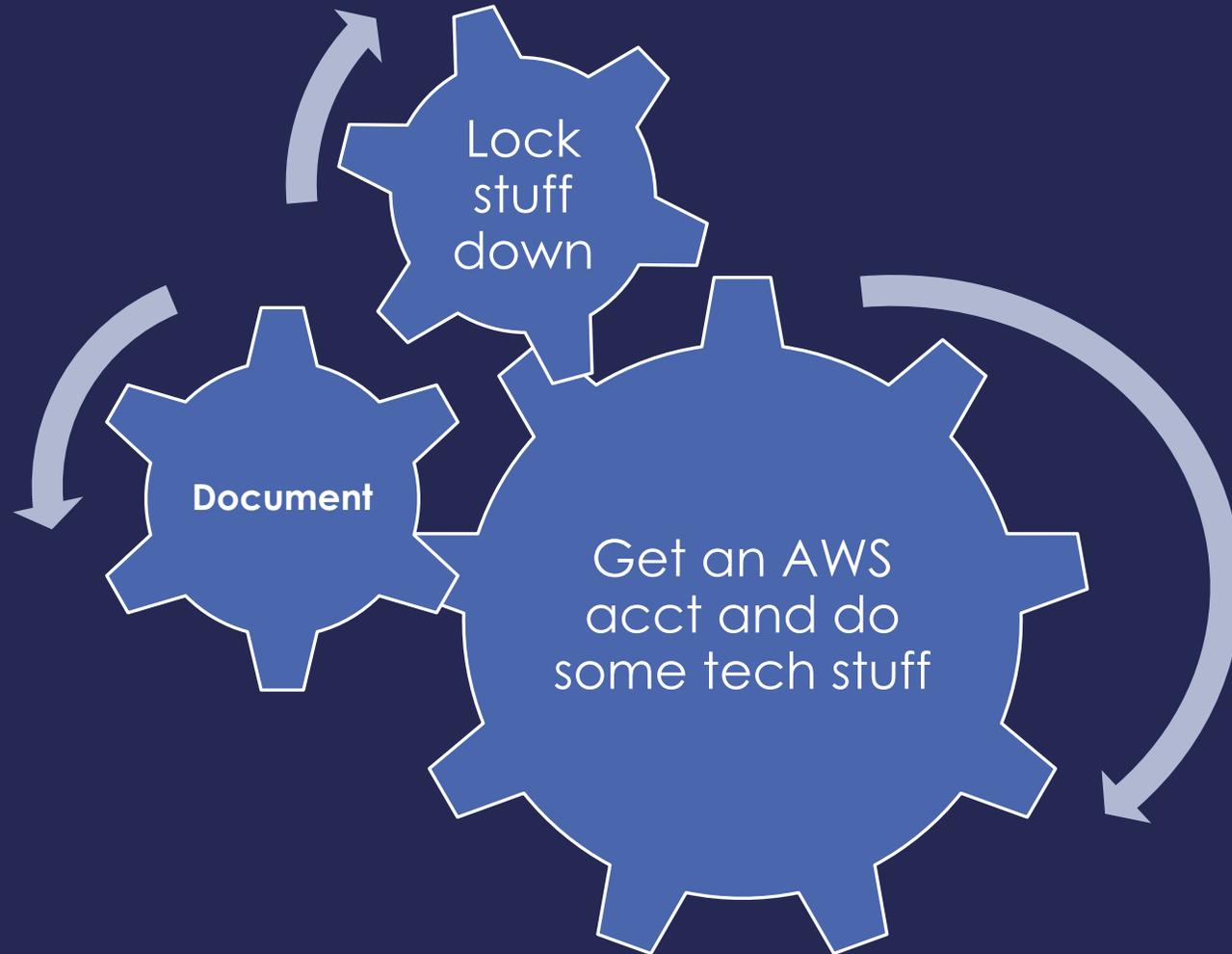


Securing the Cloud for Research: A Collaborative Effort

Claire Mizumoto

UCCSC 2018

Originally this is what we thought



Instead this is what it really looks like



Technical engagement

Compliance Docs

Technical Engagement, take 2

Enter UC San Diego Health

Technical Process

What's Next

December 2016

Assumed it was mostly a technical problem that we needed to solve

March 2017

First pilot participants with ***de-identified, open data***

April 2017

We began to dig deep on the HIPAA certification docs

Wait...this was mostly a compliance issue

So we rebooted.....

We stepped up the pace to create:

- Systems Design Document
- System Security Plan
- Backup and Recovery Policy
- Configuration Management Document
- Contingency Plan
- IAM Policy
- IDS Document
- Incident Reporting Plan
- Production Support Document



May 2017

First official meetings with:
Campus IT Security
UC San Diego Health



Already engaged a specialist – HIPAA/FISMA with
the technical knowledge to put them together

And the glue that binds Health and Campus
together: Health engaged the same consultant

Leverage Native Services

AWS Core Cloud Infrastructure Services

- Compute
- Storage & Content Delivery
- Database
- Networking
- Administration & Security

AWS Cloud Platform Services

- Analytics
- Application Services
- Development & Management
- Mobile & Devices

AWS Global Infrastructure

- Availability Zones
- Regions
- Edge Locations

Application Services

- CloudSearch, CloudSearch IDP Metadata, Elastic Transcoder, Email, SES, SNS, SNS Email Notification, SNS HTTP Notification, SNS Topic, SQS, SQS Message, SQS Queue, S3, SWF Decider, SWF Worker

Compute and Networking

- Auto Scaling, AWS Direct Connect, EC2, EC2 AMI, EC2 CloudWatch, EC2 On Instance, EC2 Elastic IP, EC2 Instance, EC2 Instances, Elastic Load Balancing, Elastic Network Interface, EMR
- EMR Cluster, EMR HDFS Cluster, Route 53, Route 53 Hosted Zone, Route 53 Route Table, VPC, VPC Customer Gateway, VPC Internet Gateway, VPC Router, VPC VPN Connection, VPC VPN Gateway

Database

- DynamoDB, DynamoDB Attribute, DynamoDB Attribute, DynamoDB Item, DynamoDB Table, ElastiCache, ElastiCache Node, RDS, RDS DB Instance, RDS Read Replica, RDS Instance Snapshot, RDS MySQL Instance, RDS MySQL DB Instance, RDS Oracle DB Instance, Redshift, SimpleDB, SimpleDB Domain

On-Demand Workforce

- Mechanical Turk Workers, Mechanical Turk, Mechanical Turk Requester, Mechanical Turk Assignment Task, Mechanical Turk Human Intelligence Tasks

Deployment and Management

- CloudFormation, CloudFormation Stack, CloudFormation Template, CloudWatch, CloudWatch Alarm, Data Pipeline, Elastic Beanstalk, Elastic Beanstalk Application, Elastic Beanstalk Deployment, IAM, IAM Add-on, IAM STS, OpsWorks

So many services, so little time!

Eliminate management overhead!
Not all managed service will meet your exact needs.
Examples:

- CloudFormation – Create your infrastructure in a reproducible, re-useable, and code-based method
- EC2 Fleet
- RDS and/or Serverless Aurora
- Elastic Beanstalk (for applications elasticity)
- DynamoDB

EC2 Fleet target capacity: 15

Launch template
 Instance type: c3.large

On-Demand capacity: 10	Launch template overrides
	c4.large Weighted capacity: 1
Spot capacity: 5	c5.large Weighted capacity: 2

UC San Diego Health: AWS Cloud Strategy

Phase I core infrastructure (Complete)

System Security Plan and Design document provisionally approved by security

Pending organizational decisions on Logging, IDS/IPS (firewall-type)

Phase II focusing on customer defined service needs

Storage with S3

Role transfer account -> S3

Customer buckets (filegateway endpoint as a NFS mount)

Filegateway Virtual tape library

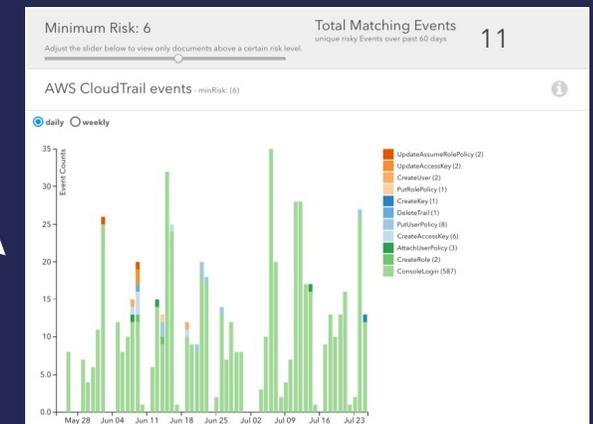
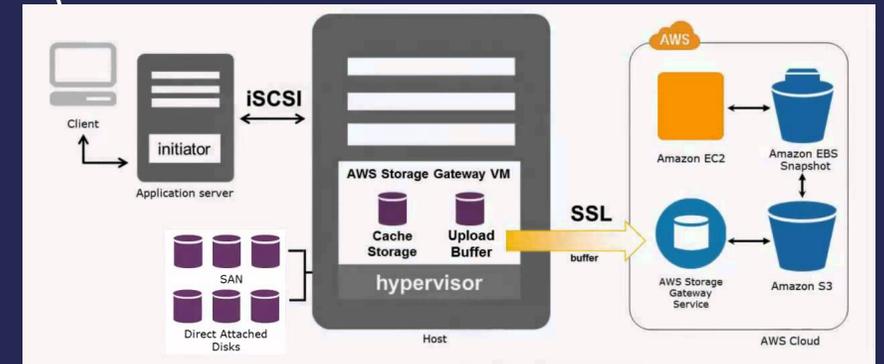
StorageGateway application mounts (an iscsi) and S3

***AWS Macie** - DLP and Bucket analytics service: *evaluating*

AD and MFA authentication, Duo MFA delete verification

AWS WorkSpaces VDI environment

Proof of Concept in progress



So, Instead of Being Competitive, We Collaborated

On the Health side,

- S3
- Access control
- Boundary security
- VPC/EC2 within an account
- Logging infrastructure
- Vulnerability/Compliance scanning

UC San Diego Health

Collaboration, cont'd

On the Research IT side,

- Evident.io
- OpenVPN / Campus VPN / Campus IP space
- DUO MFA
- 2 more research project pilot participants
- User documents
- And more....

What's Next

- Continue to collaborate
- Compliance and Privacy Review
- Proof of Concept project to evaluate cost of outsourcing the maintenance of the environment
- “Packaging” compliance docs and code-sharing
- Handing off the Research IT side



In Summary

Collaboration



Questions?