Release Management in a Compliant Cloud

Anthony Boyd
Sherlock
San Diego Supercomputer Center @ UC San Diego
WHO ARE WE?

SDSC is a division within SDSC, which is an organized research unit at UC San Diego.
Sherlock's Evolution

2008–Present

FISMA Platform

2013

Sherlock HIPAA Cloud
Hosted by SDSC for the last 6 years; built to NIST 800-53 specification

2016

Sherlock Cloud for Protected Data (HIPAA, CUI)
Multi-tenant, Private Cloud for academia & research organizations with varying compliance needs

2017–19

Hybrid Cloud for Protected Data
Multi-tenant, Hybrid Cloud (SDSC-AWS) for Academia, Government & Industry

2019–20

Innovation Accelerator Platforms
Fit-for-Use, turnkey platforms for big data management, analytics, data science, machine learning
OUR ROOTS ARE IN COMPLIANCE & CYBERSECURITY

- HIPAA
- FISMA COMPLIANCE
- NIST
  National Institute of Standards and Technology
  U.S. Department of Commerce
- Controlled Unclassified Information
- SHERLOCK SECURE CLOUD SOLUTIONS
- Privacy
- AUDIT
BUT WE ARE EVOLVING TOWARDS PROVIDING VALUE ADDED CAPABILITY
What is CI/CD?
Sherlock’s approach to supporting CI/CD

• Turnkey Solutions
  • Automated build-outs for CI/CD workflows

• Ease of Use
  • We want developers to use the tools they’re used to

• Customization
  • We can create a CI/CD framework that meets your needs

• Limiting Costs
  • Pay per use, utilize cloud services

• Make the cloud easier for customers so they can focus on their work
Challenges Meeting Compliance

• Overhead of managing infrastructure and security
  • Administrating systems, implementing security controls, maintaining compliance

• Detecting security issues before they become a problem
  • Patch management, software upgrades, monitoring threats

• A lack of integrated security tools

• Security testing slowing down processes
How Sherlock Handles these Challenges

• Automation
  • Build-outs, patch management, management tasks

• Leveraging RedLock’s signatures for compliance
  • Scans cloud platforms against HIPAA, NIST 800-53 Rev4, SOC 2, and other signatures

• CIS compliant AMIs
  • Custom built compute images with security tools included

• SIEM with Splunk
  • Logging the entire platform to catch threats

• Perimeter UTM with WAF IPS
  • Control and gain insight into what’s coming in or going out
CI/CD Tools and Stages

Orchestration and Automation
AWS CodePipeline

Versioned Source
GitHub
AWS CodeCommit

Build and Test
AWS CodeBuild

Deployment
AWS CodeDeploy

Environments

Some of the other interoperable tools:
Jenkins
maven
Bitbucket
Approvals

Approve or reject the revision

Comments

Looks good.

Cancel

Approve

Reject
CodePipeline orchestrates the build, test, and deployment based on a defined process.

GitHub

AWS CodeBuild
Compiles source code, runs tests, and produces build artifacts

AWS CodePipeline

Amazon S3 bucket
Stores source artifacts and build artifacts

AWS CodeDeploy
Automated deployment service that installs your code onto your hosts

Elastic Load Balancer

Firewall

EC2 Hosts

VPC
Thank you!

Anthony Boyd
Sherlock
San Diego Supercomputer Center @ UC San Diego