Security Automation and Orchestration

The Foundation of Application Migration and Modernization for Regulated Industry

2018

SESSION OVERVIEW

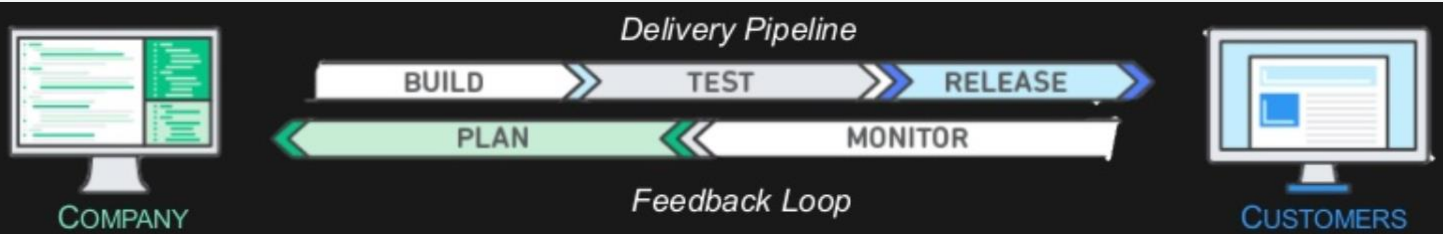
- Security Automation and Orchestration
  - What is Secure DevOps?
  - What happens to our Regulated Customers today, in adopting DevSecOps models?
  - Introduction to Security Automation and Orchestration.

- Stages of Security Automation and Orchestration Adoption
  - Cloud Migrator
  - Cloud Forward
  - Cloud Native

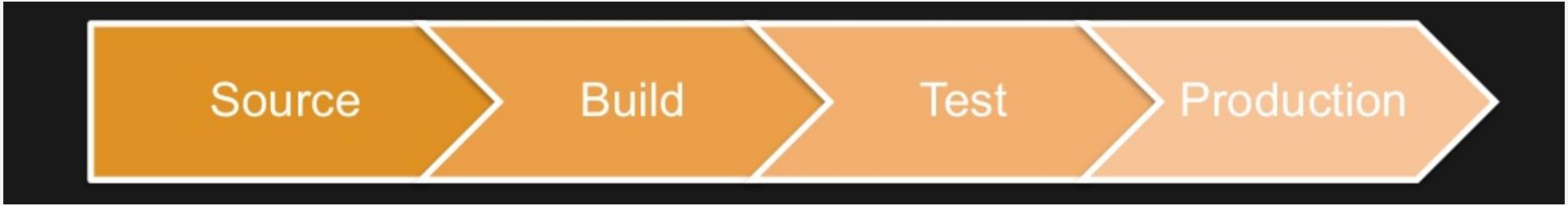
- Collaborative Social Engineering
  - Review of GitHub, and its role in establishing effective security communities.
  - Review of GitHub at the core of Security Automation and Orchestration.
  - Building a continuous accreditation model, across regulated industries.

WHAT IS DEVSECOPS?

- Union of software development and operations
- Migration of Agile continuous development into continuous integration, continuous delivery, and continuous compliance.
- DevSecOps Model
  - No Silos – Puts emphasis on communication, collaboration and cohesion between disciplines
  - Best practices for change, configuration, and deployment automation
  - Deliver apps/services at a faster pace
  - High speed product updates



DEVOPS PROCESSES: 4 MAJOR PHASES



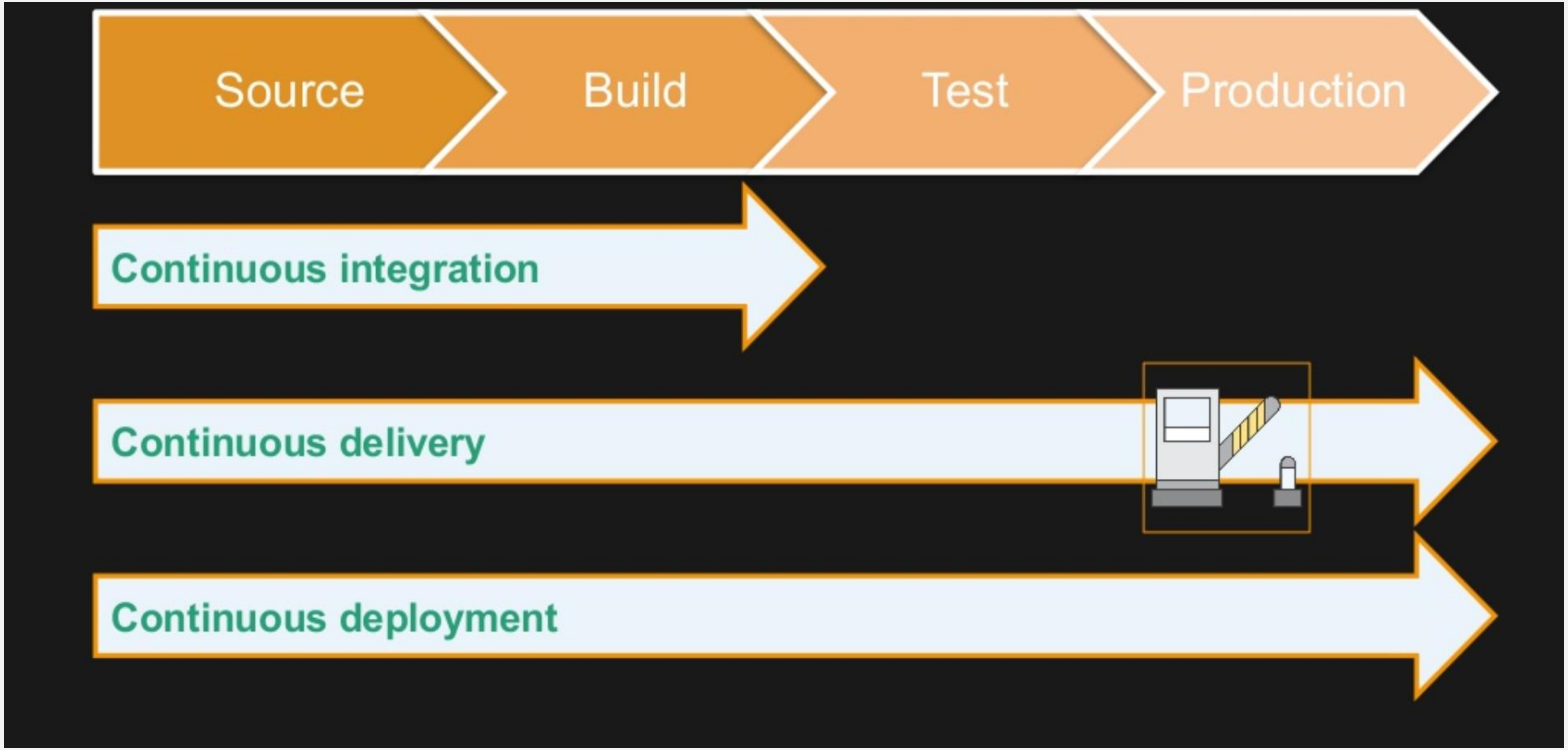
- Check-in source code
- Peer review new code

- Compile code
- Unit tests
- Style checkers
- Code metrics
- Create container images

- Integration tests with other systems
- Load testing
- UI tests
- SecOps Scanning

- Deployment to production environments
- Continuous Monitoring

DEVOPS RELEASE PROCESSES: LEVELS



Problem Statement – Why can’t we be Agile?

Security and risk management leaders continue to labor over **“How”** do they secure current, legacy and cloud resources consistently within their limited constraints.

While cloud services has provided streamlined ways to achieve innovation through the principles of DevOps and Developer Self-Service, regulated customers are still under mandate to follow strict security, governance, and accreditation standards, which are delivered during the production deployment phase.

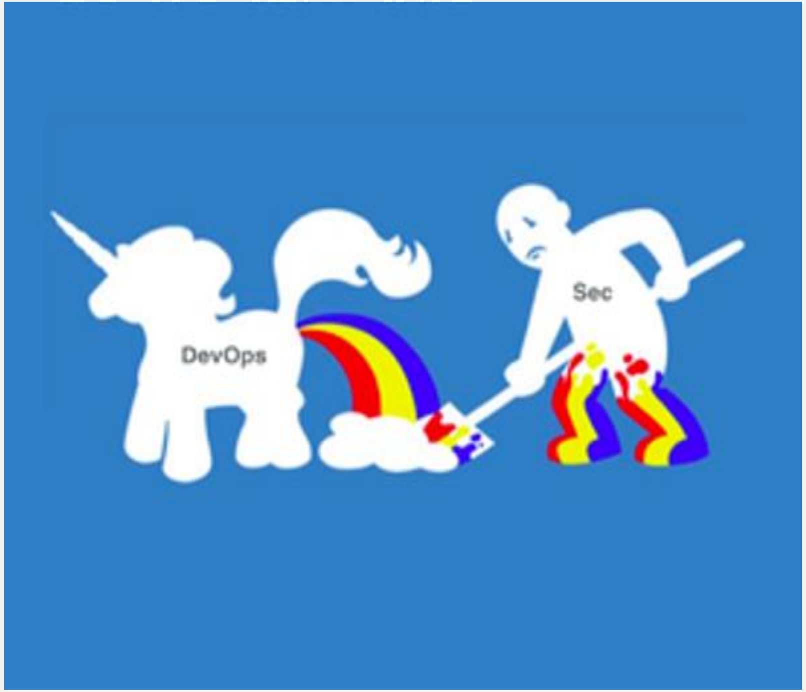
Developer Self-Service – In a Compliance Oriented World

DevOps enables the CI/CD pipeline which is the basis of automation within AWS.

The biggest challenge is breaking out of the traditional security structures and eliminating the divide between developers, operations, and security.

The CI/CD pipeline is the foundation for creating a repeatable, reliable and constantly improving process for taking software from concept to a secure, complaint production solution.

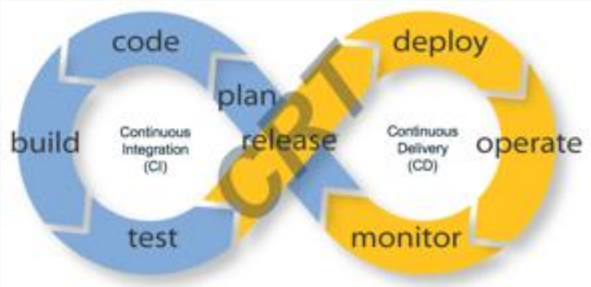
AWSome! But what actually happens in Regulated environments today?



Solution Overview: SAO

Develop an **AWS Security Automation and Orchestration (SAO)** repository for constraining, tracking, publishing continuous security configurations, integration, deployments and treatments which are certified against common security frameworks (e.g. FedRAMP, DoD CC SRG, IRS 1075,CIS, PCI, etc.)

SAO will facilitate the orientation and association of **DevOps** and **Security** practices, changes and coordination of **Continuous Integration (CI)**, **Continuous Delivery (CD)** and **Continuous Risk Treatment (CRT**)* of an AWS customer account and/or multiple accounts.



* CRT is a process and technology approached which is designed to detect, maintain and in *MOST* case correct security, compliance and threats associated with an organization's solution and service deployment within their AWS account. CRT processes monitor security controls in real-time to ensure the risk and/or threat treatment (Control Intent) is working as designed or at least within an intended margin of acceptance base on guard rails, swim lanes and/or rules built into the control to allow for business operations.

Regulatory Standards – What will SAO Satisfy?

1. The Payment Card Industry **Data Security** Standard (**PCI DSS**)
2. Defense Federal Acquisition Regulations Supplement (**DFARS**) NIST SP 800-171
3. Federal Risk and Authorization Management Program (**FedRAMP**) (**Moderate-Impact**)
4. Federal Risk and Authorization Management Program (**FedRAMP**) (**High-Impact**)
5. Department of Defense (*DoD*) Cloud Computing Security Requirements Guide (*SRG*) **Impact Level (*IL) 2***
6. Department of Defense (*DoD*) Cloud Computing Security Requirements Guide (*SRG*) **Impact Level (*IL) 4***
7. Internal Revenue Service (*IRS*) **Publication *1075* Tax Information Security Guidelines**
8. Minimum Acceptable Risk Standards for Exchanges (***MARS-E***) 2.0
9. The Criminal Justice Information Services Division (**CJIS**)
10. The Center for Internet *Security* (CIS)– Critical Security Controls
11. The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679)

SAO Community (to date) - Who's involved?

CIS Center for Internet Security

KRATOS
DEFENSE & SECURITY SOLUTIONS
FROM STRENGTH TO SUCCESS

COALFIRE

Booz | Allen | Hamilton

ANITIAN

GitHub

smartsh p

CloudBees
The Enterprise Jenkins Company

CHEF

redhat.

Cloud Checkr

okta

Barracuda

paloalto NETWORKS

yubico

BLUECAT

splunk>

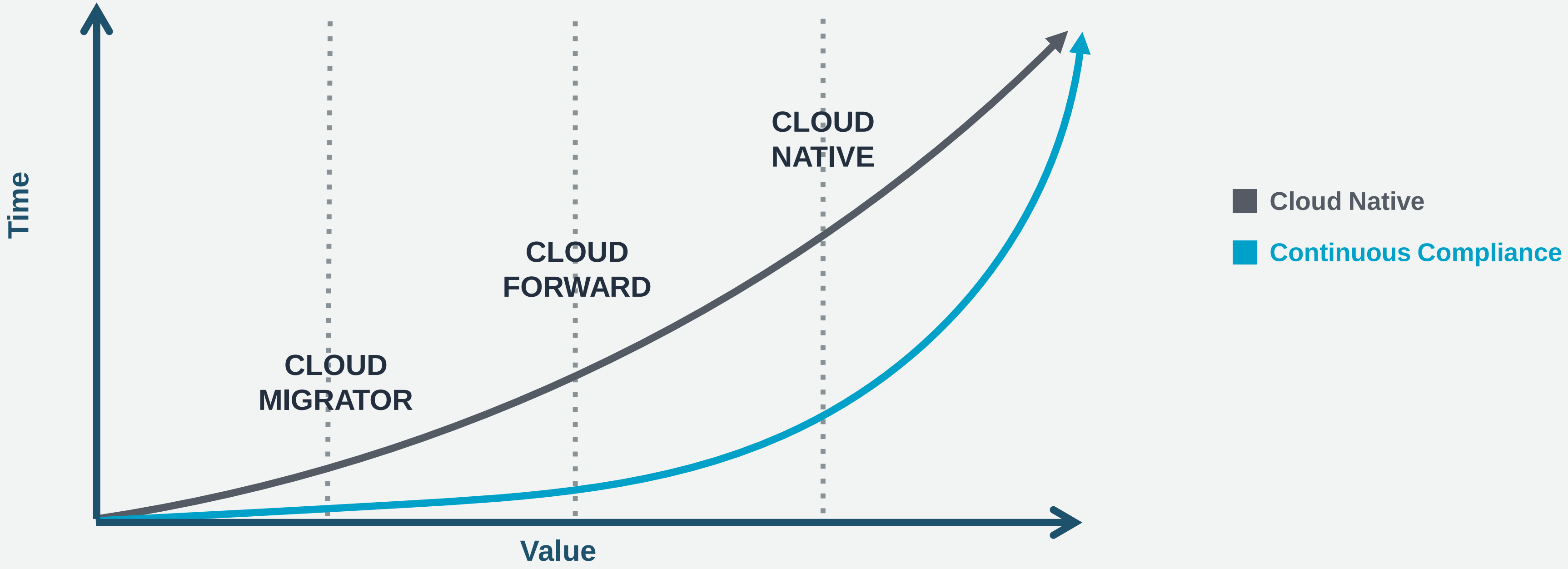
Telos

ALLGRESS

TREND MICRO

aws

Stages of Security Automation and Orchestration



The Result:
“*AWS Trust Boundary In a Box*”

1. Templates, Scripts, Functions and Recipes for securely deploying regulated workloads “Type Accreditation” (Pre-Audited), for all stages of Cloud Service adoption, (Migrator, Forward, Native)

2. Defined operational security and compliance tolerances scripts, functions and treatments (e.g. Guard Rails) for constrained secure operations across the DevOPS CI/CD and CRT through the use of **Governance as Code** (GoC) practices

3. Deployable Continuous Risk Treatments (CRT) resources (e.g. AWS & Partners solutions)

Thank You!

What is GitHub

Version Control

Social Collaboration

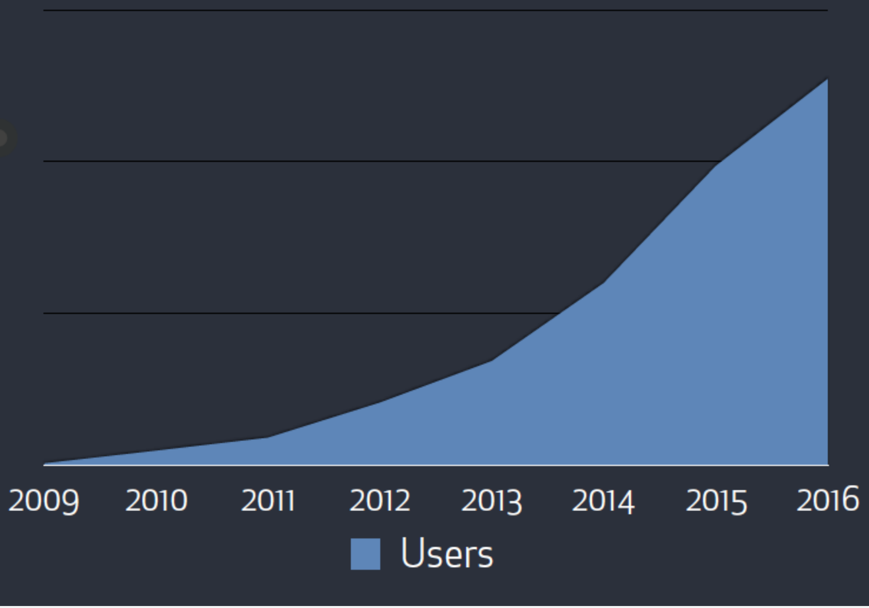
Developer Platform

The collaboration platform where software is made.

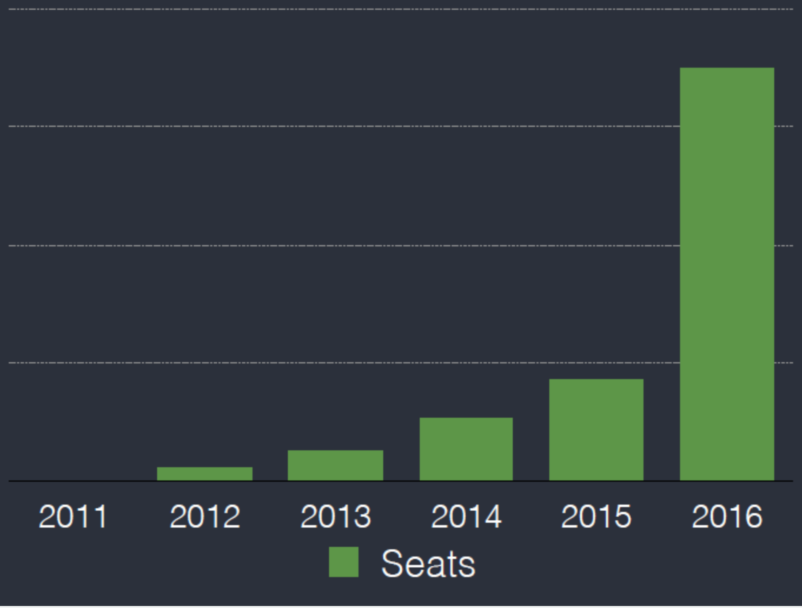
- Largest host of code, globally
- Home base for open source

Government Adoption

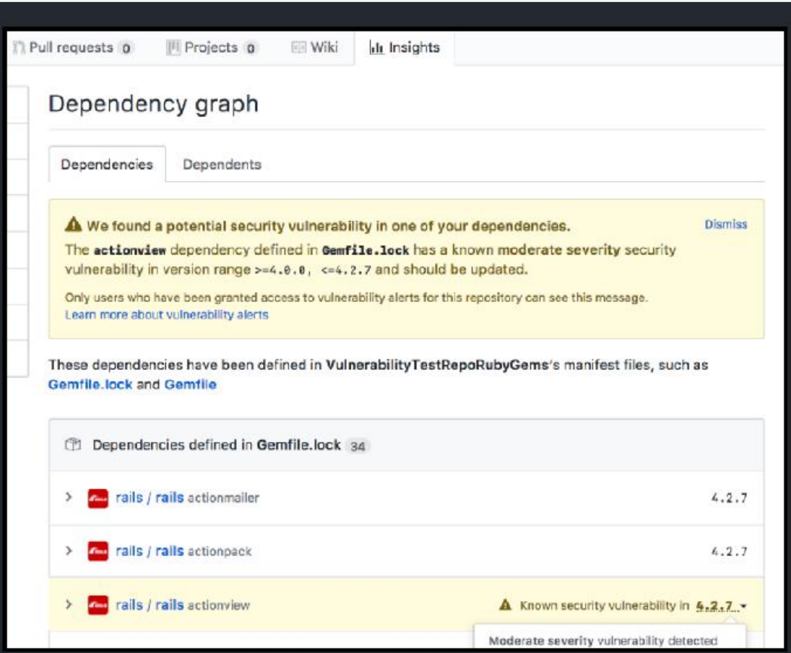
GOVERNMENT
GitHub.com



GOVERNMENT
GitHub Enterprise



Securing your project's **dependencies**



Dependency graph

Dependencies | Dependents

⚠ **We found a potential security vulnerability in one of your dependencies.** Dismiss

The **actionview** dependency defined in **Gemfile.lock** has a known **moderate severity** security vulnerability in version range `>=4.0.0, <=4.2.7` and should be updated.

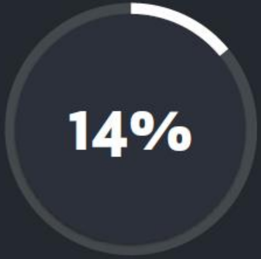
Only users who have been granted access to vulnerability alerts for this repository can see this message.
Learn more about vulnerability alerts

These dependencies have been defined in **VulnerabilityTestRepoRubyGems**'s manifest files, such as **Gemfile.lock** and **Gemfile**

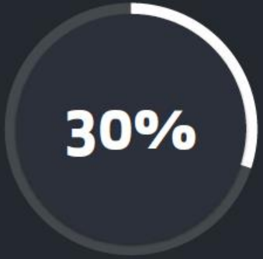
Dependencies defined in **Gemfile.lock** 34

rails / rails actionmailer	4.2.7
rails / rails actionpack	4.2.7
rails / rails actionview	⚠ Known security vulnerability in 4.2.7

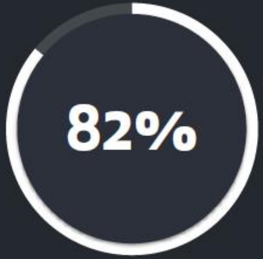
Moderate severity vulnerability detected



OF PACKAGES HAVE **A SECURITY VULNERABILITY**

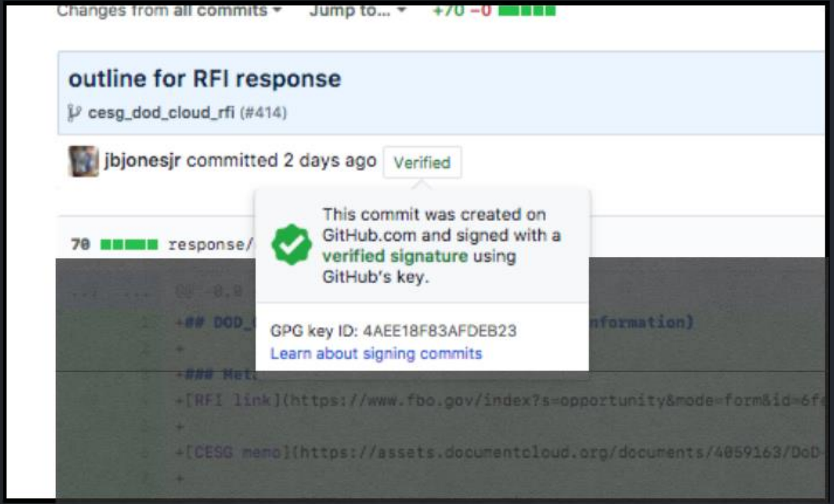


OF COMPANIES **HAVE NO PLAN** FOR ADDRESSING OPEN SOURCE DEPENDENCY VULNERABILITY



OF PUBLIC GITHUB REPOS DO NOT UPDATE THEIR DEPENDENCIES, **EVER**

Validate your **identities**



outline for RFI response

cesg_dod_cloud_rfi (#414)

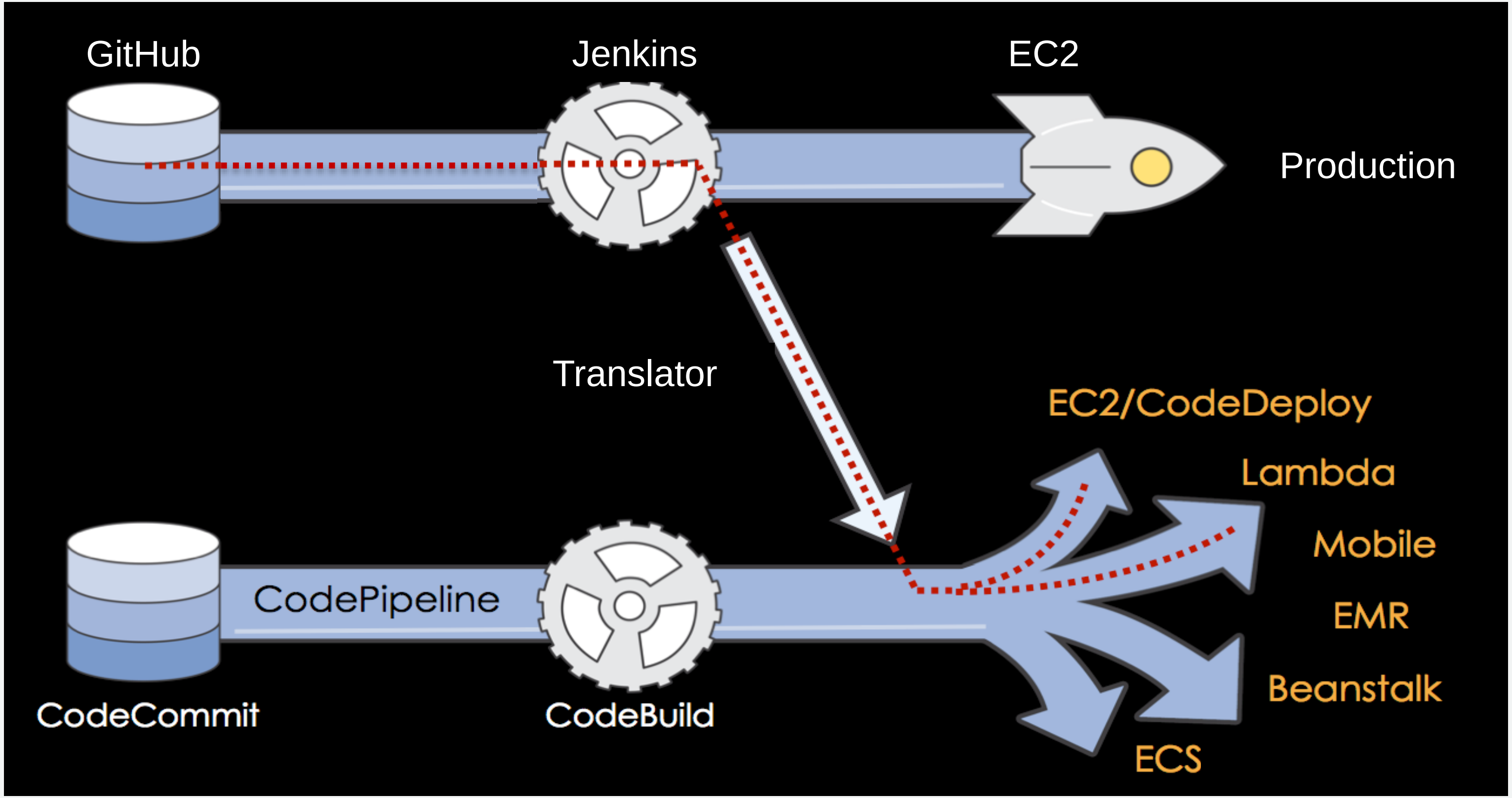
jbjonesjr committed 2 days ago Verified

This commit was created on GitHub.com and signed with a **verified signature** using GitHub's key.

GPG key ID: 4AEE18F83AFDEB23
Learn about signing commits

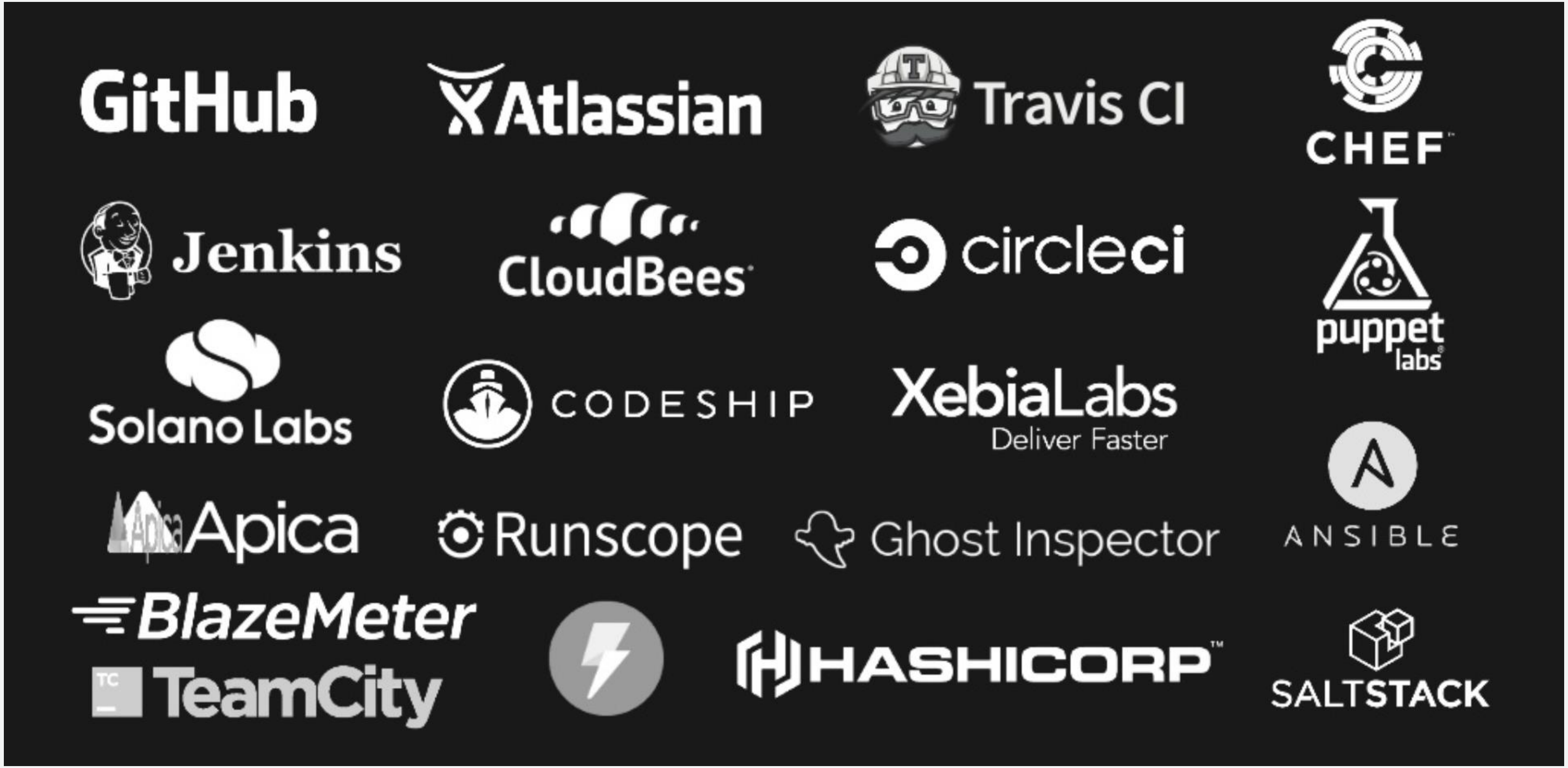
```
70 ■■■■■ response/
@@ -0,0
+## DOD_                                  nformation)
+
+### Met
+[RFI link](https://www.fbo.gov/index?s=opportunity&mode=form&id=6f
+
+[CESG memo](https://assets.documentcloud.org/documents/4059163/DoD-
+
```

MIGRATING YOUR EXISTING PIPELINE



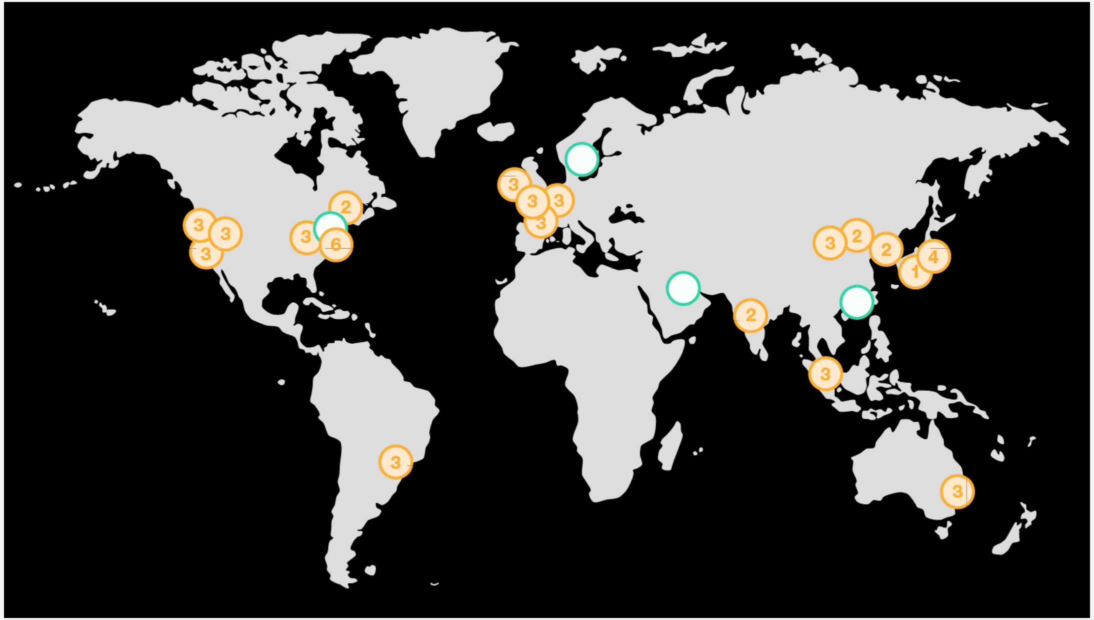
Enabling Value Based Delivery

AWS INTEGRATED PARTNERS – SERVICE TRANSFORMATION



AWS Global Infrastructure

18 Regions – 1 Local Region – 55 Availability Zones – 100+ Edge Locations



Region & Number of Availability Zones

US East
N. Virginia (6),
Ohio (3)

US West
N. California (3),
Oregon (3)

Asia Pacific
Mumbai (2),
Seoul (2),
Singapore (3),
Sydney (3),
Tokyo (4),
Osaka-Local (1)1

New Region (coming soon)

Bahrain

Hong Kong SAR, China

Canada
Central (2)

China
Beijing (2),
Ningxia (3)

Europe
Frankfurt (3),
Ireland (3),
London (3),
Paris (3)

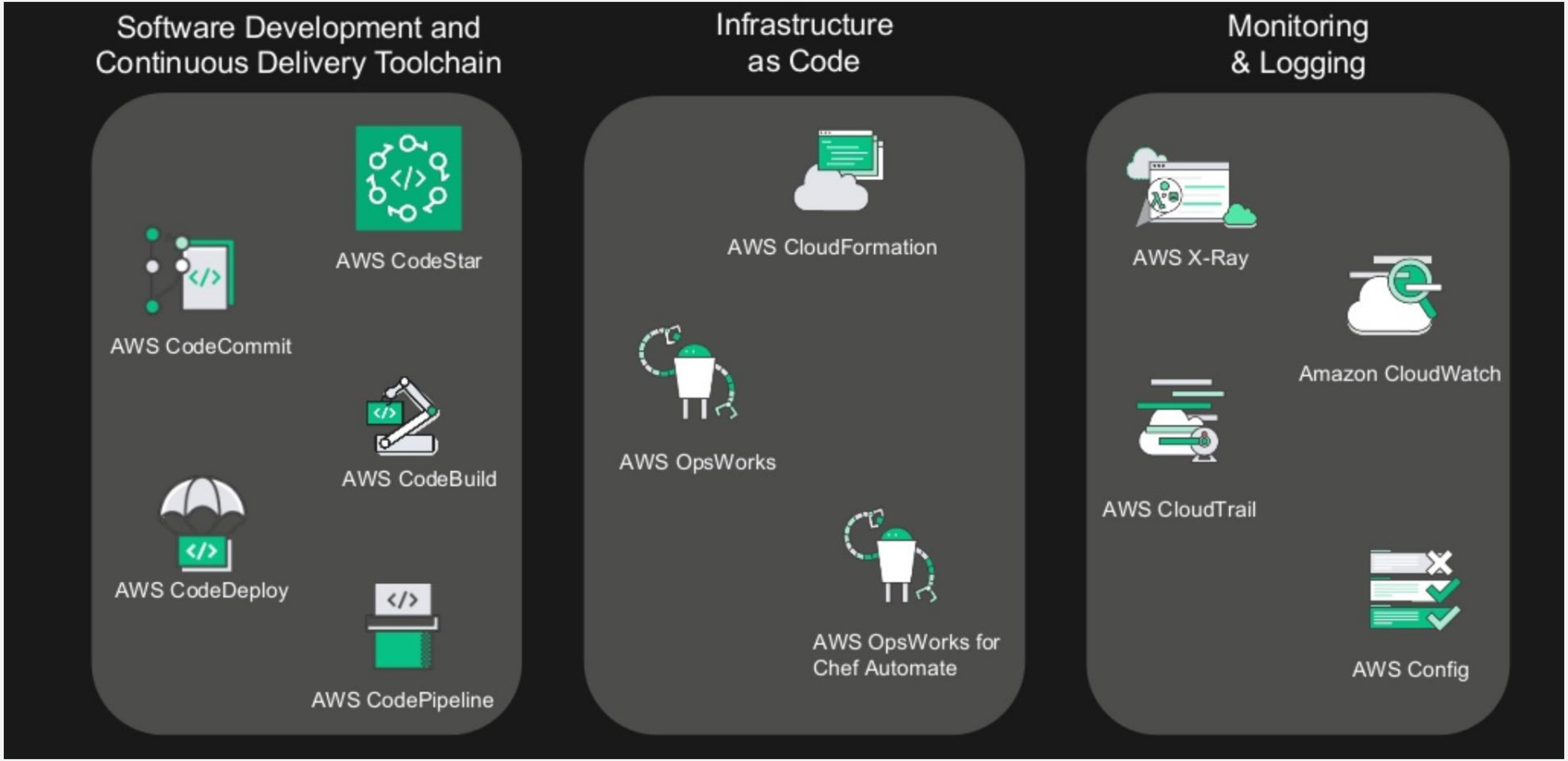
South America
São Paulo (3)

AWS GovCloud (US-West) (3)

Sweden

AWS GovCloud (US-East)

AWS DEVOPS PORTFOLIO



Software Development and Continuous Delivery Toolchain

- AWS CodeCommit
- AWS CodeStar
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Infrastructure as Code

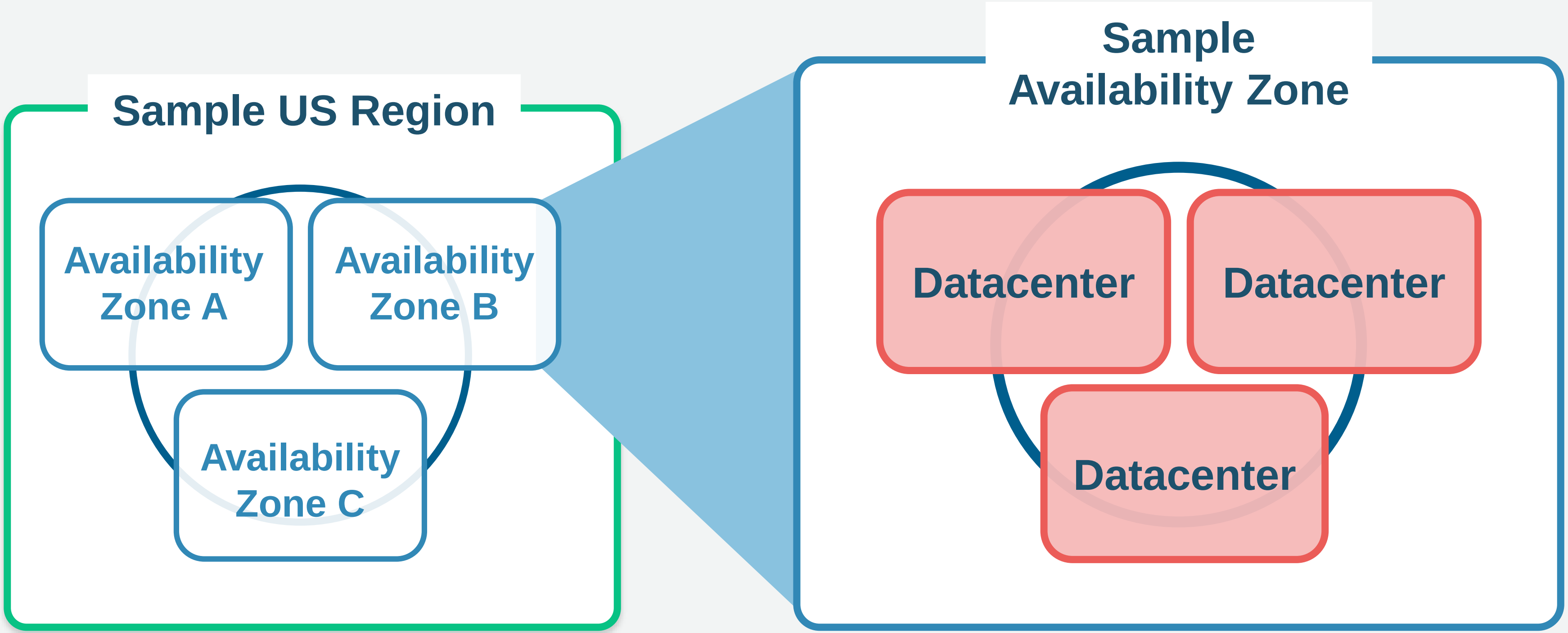
- AWS CloudFormation
- AWS OpsWorks
- AWS OpsWorks for Chef Automate

Monitoring & Logging

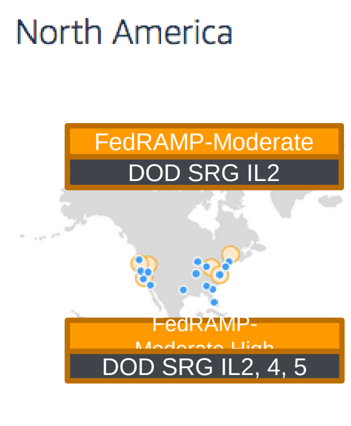
- AWS X-Ray
- Amazon CloudWatch
- AWS CloudTrail
- AWS Config

Zoom In: AWS Region

Zoom In: AWS AZ



US – Regions, AZs and Edge Locations



FedRAMP-Moderate

DOD SRG IL2

FedRAMP-Moderate High

DOD SRG IL2, 4, 5

US East (Northern VA) Region
EC2 Availability Zones: 6
Launched 2006

US West (Oregon) Region
EC2 Availability Zones: 3
Launched 2011

AWS GovCloud (US-West) Region
EC2 Availability Zones: 3
Launched 2011

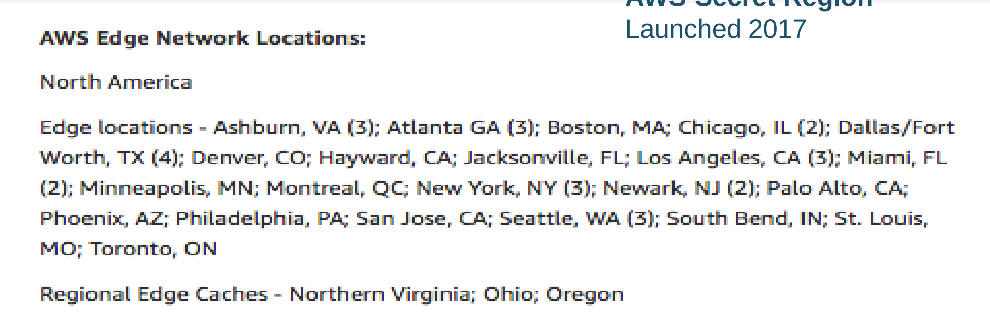
US East (Ohio) Region
EC2 Availability Zones: 3
Launched 2016

US West (Northern CA) Region
EC2 Availability Zones: 3*
Launched 2009

AWS Top Secret (C2S) Region
Launched 2014

DOD SRG IL6

AWS Secret Region
Launched 2017



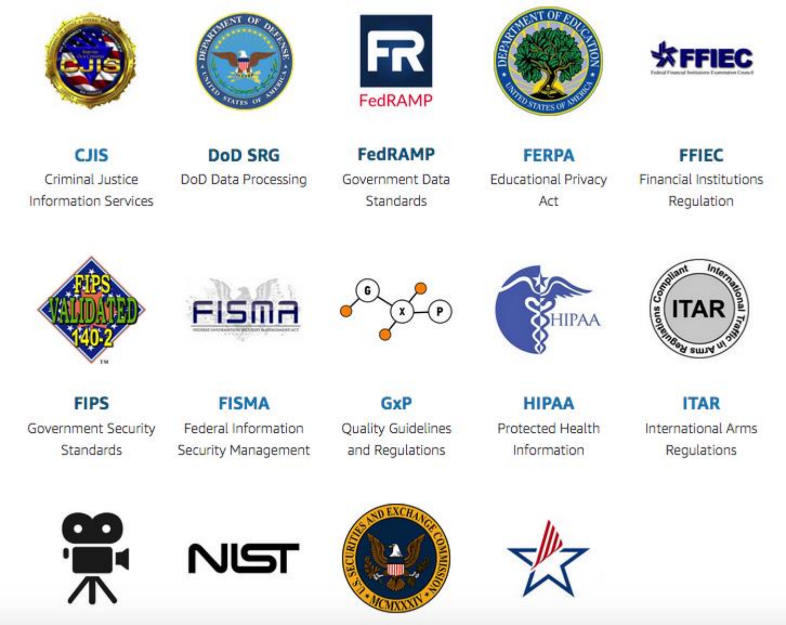
AWS Edge Network Locations:

North America

Edge locations - Ashburn, VA (3); Atlanta GA (3); Boston, MA; Chicago, IL (2); Dallas/Fort Worth, TX (4); Denver, CO; Hayward, CA; Jacksonville, FL; Los Angeles, CA (3); Miami, FL (2); Minneapolis, MN; Montreal, QC; New York, NY (3); Newark, NJ (2); Palo Alto, CA; Phoenix, AZ; Philadelphia, PA; San Jose, CA; Seattle, WA (3); South Bend, IN; St. Louis, MO; Toronto, ON

Regional Edge Caches - Northern Virginia; Ohio; Oregon

United States – Compliance programs and certifications



CJIS
Criminal Justice Information Services

DoD SRG
DoD Data Processing

FedRAMP
Government Data Standards

FERPA
Educational Privacy Act

FFIEC
Financial Institutions Regulation

FIPS
Government Security Standards

FISMA
Federal Information Security Management

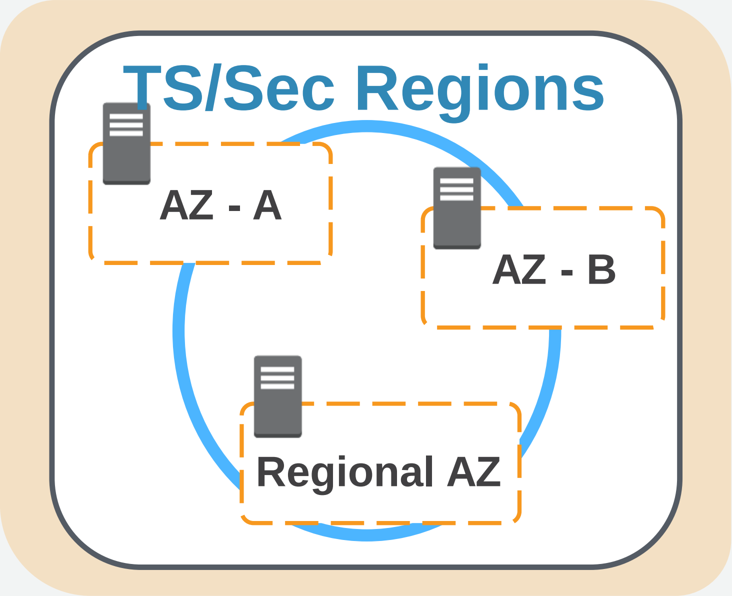
GxP
Quality Guidelines and Regulations

HIPAA
Protected Health Information

ITAR
International Arms Regulations

Secret –Top Secret Regional Architecture

- “Air-gapped” Regions – no public Internet connection
  - Available on JWICS & SIPRNet
  - Available to all 17 members of the Intelligence Community
- 3 Availability Zone (AZ) architecture
  - 2 “Public” AZs – For EC2 Instances and EC2-based services (e.g., RDS, EMR, ELB)
  - 3rd AZ used by regional services (e.g., S3, SQS, SNS, SWF)
- Using multiple AZs enables high availability, fault tolerance, and high durability
- Most API interactions w/ Region use AWS Secure Token Service (STS) via the IC Federated Identity Broker, or via IAM roles for EC2



DEVOPS ADOPTION

Continuous Integration and Deployment

docker
Pivotal Cloud Foundry
GitHub
puppet labs
ANSIBLE
CHEF
OPENSHIFT
vmware

AWS CloudFormation

AWS OpsWorks

AWS CodePipeline

AWS CodeDeploy

AWS CodeCommit

AWS CodeBuild

DEVOPS ADOPTION

Continuous Monitoring and Security

New Relic.

APPDYNAMICS

evident.io

DATADOG

CloudCheckr

Amazon CloudWatch

AWS CloudTrail

AWS Config

DEVSECOPS

Continuous Delivery: Defined and enforceable pipeline for rapid and automated software testing and release

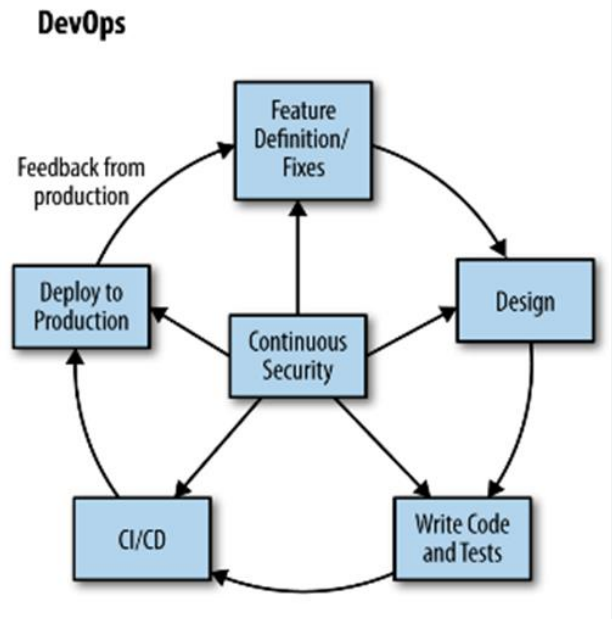
Lean Startup Approach: Employing the notion of simplest and cheapest implementation of an idea

Shifting Security to the Left: Embracing and ensuring security is properly integrated early, and throughout lifecycle

Security as Code: Wiring compliance checks and audit into continuous delivery process and mapping checks into the workflow

Continuous Monitoring: Persistent and integrated assessments during Development, Test and Production cycles

Infrastructure as Code and Containers: Automated packaging and enforcement of security services required for the runtime environment



GovCloud-Secret-Top Secret

GovCloud Region

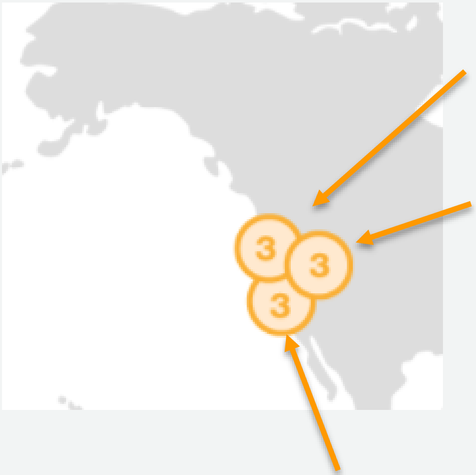
for Controlled Unclassified Information (CUI)

CUI Certifications

- ITAR
- FedRAMP/FISMA High
- DoD SRG IL4 & IL5

3 availability zones

30+ services



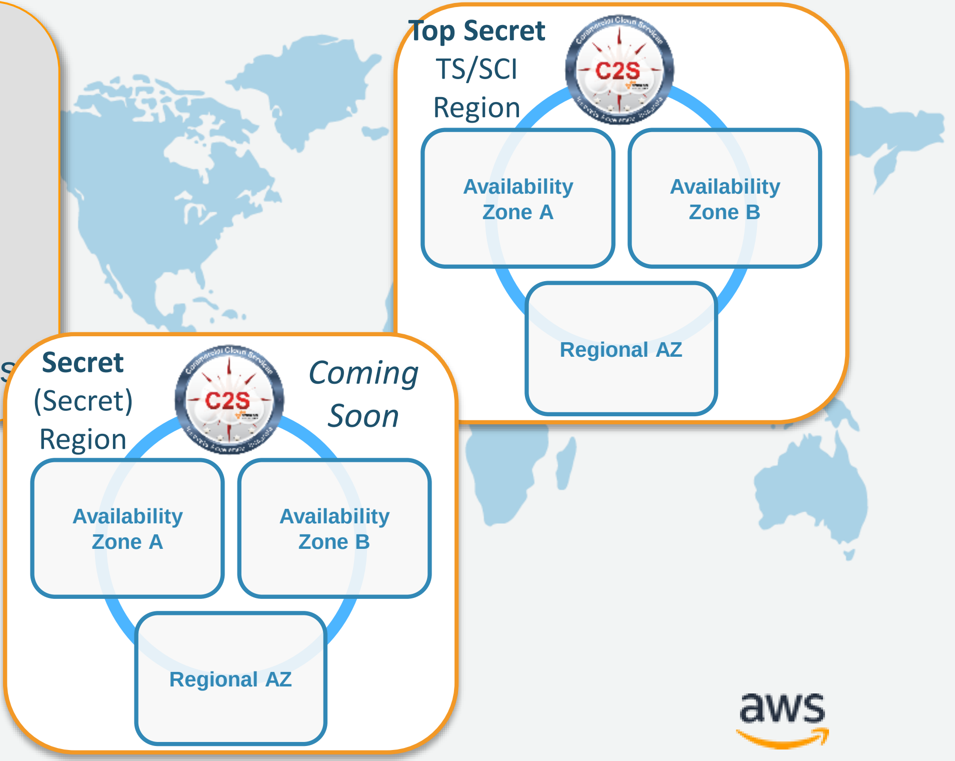
US West-1

US West-2

AWS GOVCLOUD

C2S Secret & TS/SCI Regions

Unclassified Commercial AWS Regions (Global, US, or GovCloud Regions) for Dev/Test, Prototypes, unclassified workloads



Top Secret
TS/SCI
Region

Availability Zone A

Availability Zone B

Regional AZ

Secret
(Secret)
Region

Coming Soon

Availability Zone A

Availability Zone B

Regional AZ

CONTINUOUS DELIVERY (CD) IS…

DevOps software development practice that refers to Deployment stage of the software release process

Key Activities

- ✓ Deployment of all code changes to a testing and/or a production environment
- ✓ Approval of updates to production from test stages

Goals

- ✓ Verify application updates across multiple dimensions before deployment
- ✓ Automate entire software release process
- ✓ Pre-emptively discover deployment issues

aws