DevSecOps – The Foundation of Application Migration and Modernization

Introduction to Security Automation and Orchestration

Eric Baran - Segment Lead – DevOps – AWS
Luis Tapia – Sr. Solutions Architect - AWS

November 8, 2018

SESSION OVERVIEW

- DevSecOps - Security Automation and Orchestration (SAO)
  - 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 as the collaborative hub for effective service transformation on AWS.
  - Review of GitHub at the core of Security Automation and Orchestration.

aws

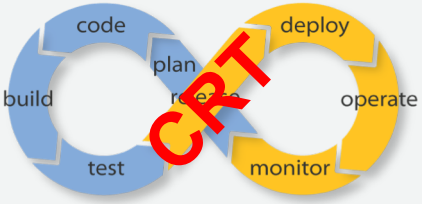
Traditional verses Cloud (Modernized) – Governance

Tradition – Governance

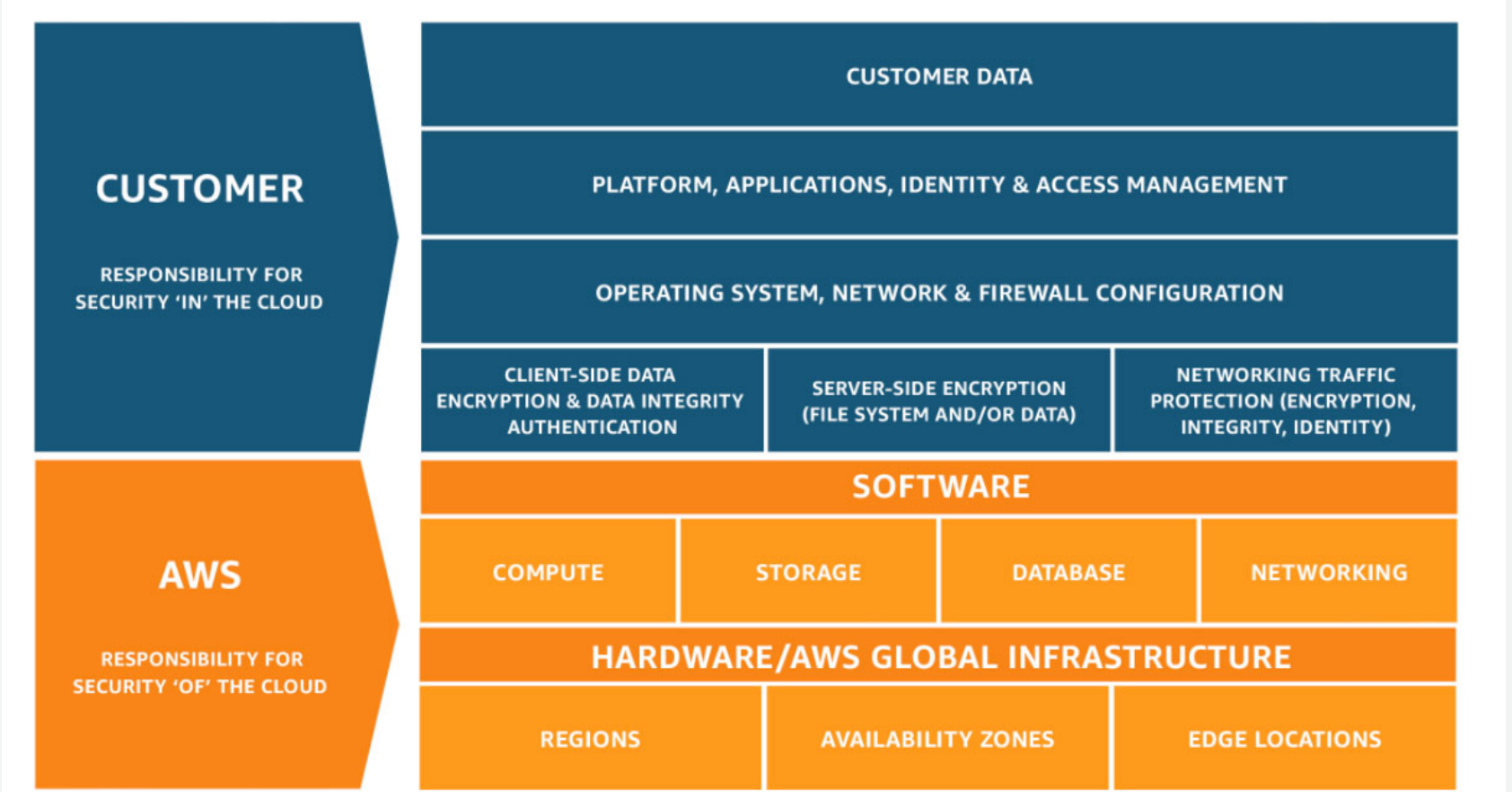
- Information and technology (IT) governance is a subset discipline of corporate governance, focused on information and technology (IT) and its performance and risk management.
- The interest in IT governance is due to the on-going need within organizations to focus value creation efforts on an organization's strategic objectives and to better manage the performance of those responsible for creating this value in the best interest of all stakeholders.

Cloud – Governance

- Technology drives your governance alignment
- Governance is a “Shared Responsibility”
- Automation is the ***Key*** to successful governance
- Pre-Cloud decision making process are paramount (e.g. service selection, policies, frameworks architecture, data protections, etc.).
- Focus is on Continuous Risk Treatments (CRT)



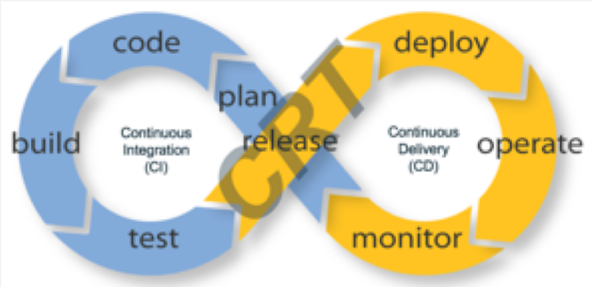
AWS Shared Responsibility Model



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.

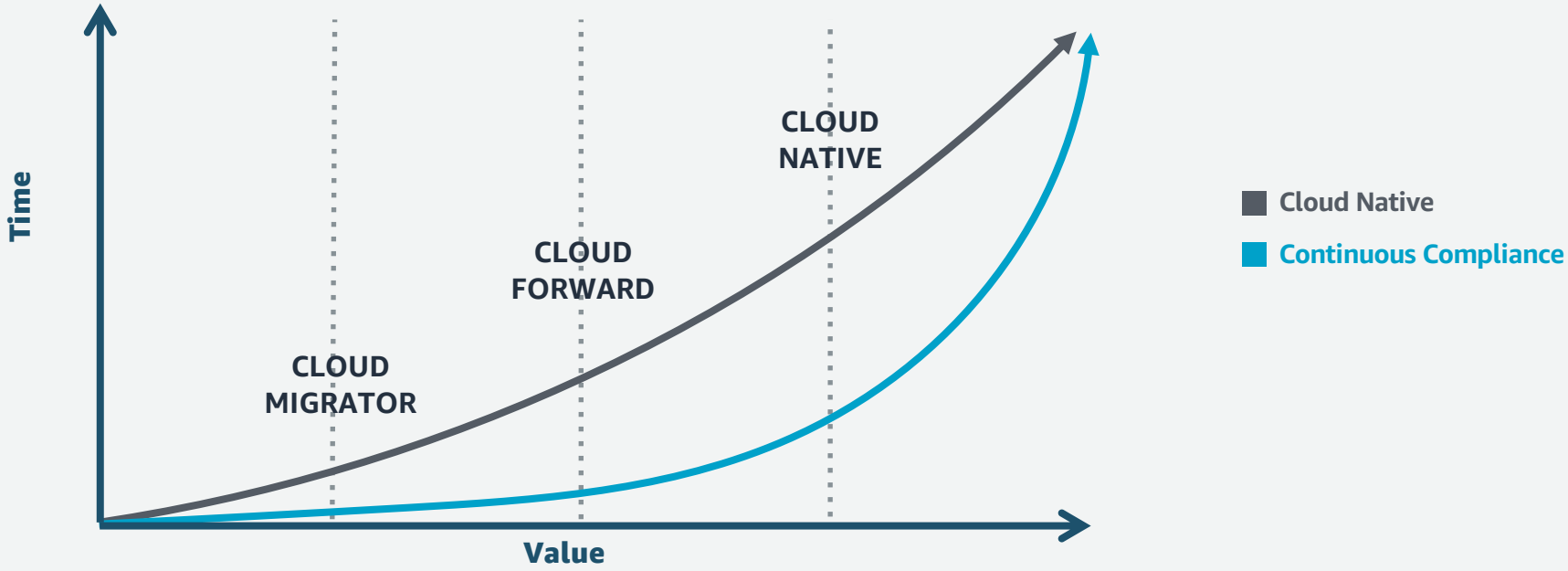
Regulatory Standards – What will SAO Satisfy? – Phase One

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)

aws

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

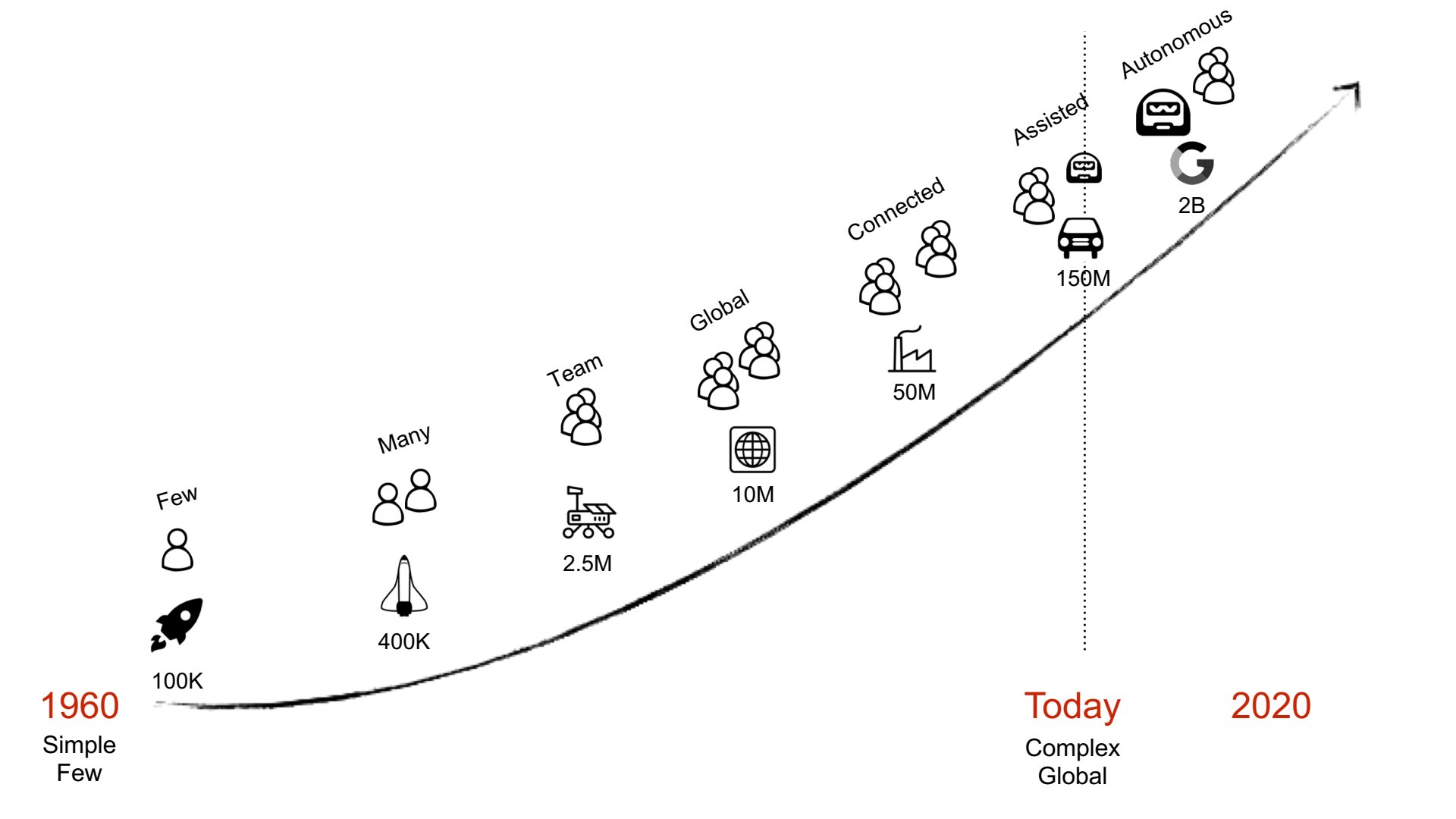
Stages of Security Automation and Orchestration



Software/DevSecOps overview
GitHub + AWS

"The Evolution of Software and Why We Evolved to DevSecOps"

aws


Few
100K
Many
400K
Team
2.5M
Global
10M
Connected
50M
Assisted
150M
Autonomous
2B
1960
Simple
Few
Today
Complex
Global
2020

PERIODIC TABLE OF DEVOPS TOOLS (V2) (V1)

EMBED DOWNLOAD ADD

Os	Open Source
Fr	Free
Fm	Freemium
Pd	Paid
En	Enterprise

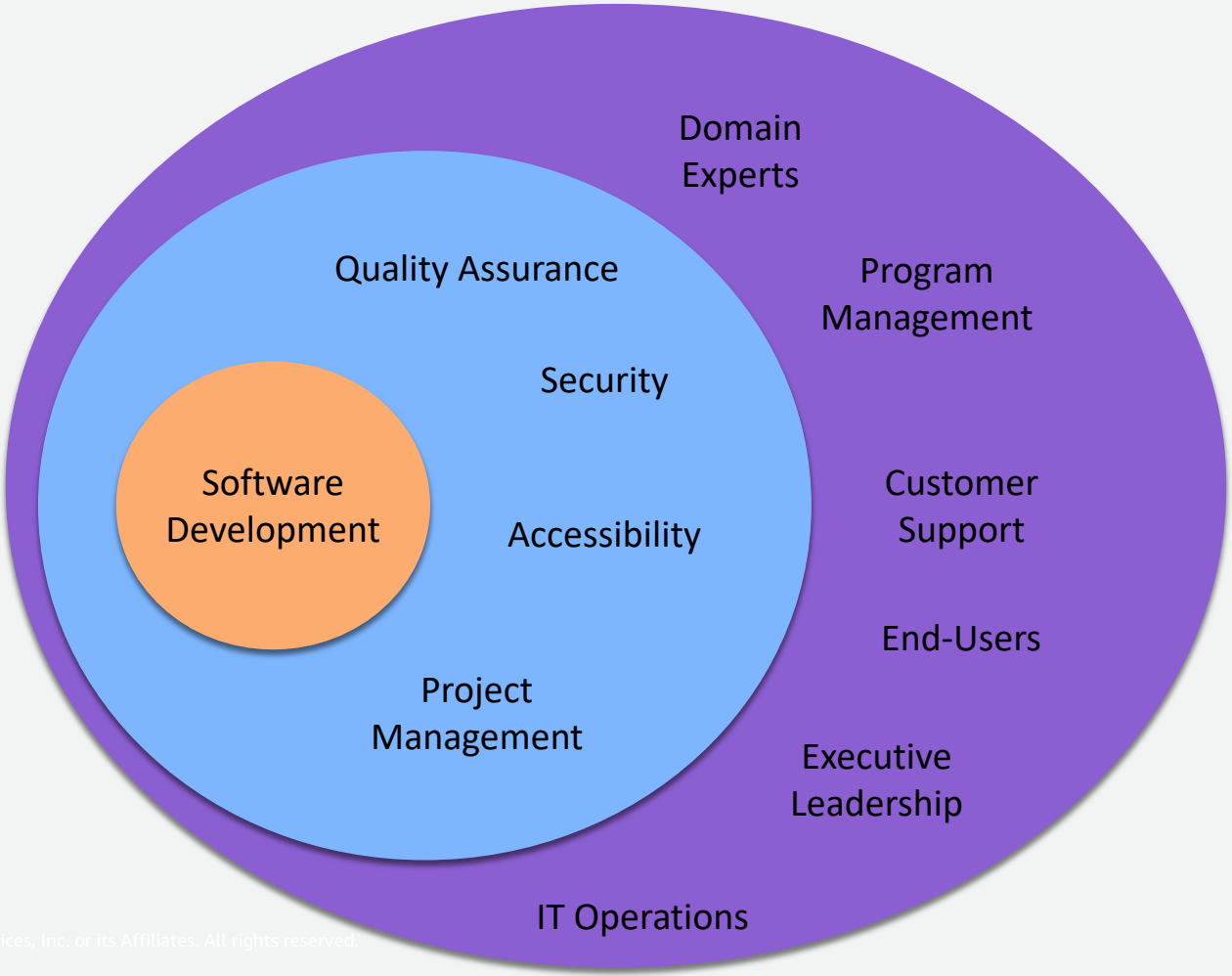
SCM	Database Mgmt	Build
CI	Repo Mgmt	Testing
Deployment	Config / Provisioning	Containerization
Cloud / Iaas / Paas	Release Mgmt	Collaboration
BI / Monitoring	Logging	Security

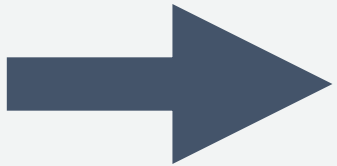
1 Fm Gh Github																		2 Fm Aws Amazon Web Services
3 Os Gt Git	4 Pd Dm DBmaestro												5 En Ch Chef	6 En Pu Puppet	7 Os An Ansible	8 En Sl Salt	9 Os Dk Docker	10 Pd Az Azure
11 Fm Bb Bitbucket	12 Os Lb Liquibase												13 Os Ot Otto	14 En Bl BladeLogic	15 Os Va Vagrant	16 Fr Tf Terraform	17 Os Rk rkt	18 En Gc Google Cloud Platform
19 Os Gl GitLab	20 En Rg Redgate	21 Os Mv Maven	22 Os Gr Gradle	23 Os At ANT	24 Os Fn FitNesse	25 Fr Se Selenium	26 Os Ga Gatling	27 Fr Dh Docker Hub	28 Os Jn Jenkins	29 Pd Ba Bamboo	30 Os Tr Travis CI	31 Pd Gd Deployment Manager	32 Os Sf SmartFrog	33 Os Cn Consul	34 Os Bc Bcfg2	35 Os Lxc Linux Containers	36 En Rs Rackspace
37 Os Sv Subversion	38 En Dt Datical	39 Os Gt Grunt	40 Os Gp Gulp	41 Os Br Broccoli	42 Fr Cu Cucumber	43 Os Cj Cucumber.js	44 Fr Qu Qunit	45 Os Npm npm	46 Fm Cs Codeship	47 Pd Vs Visual Studio	48 Fm Cr CircleCI	49 Fr Cp Capistrano	50 Fr Ju JuJu	51 Os Rd Rundeck	52 Os Cf CFEngine	53 Fr Ds Swarm	54 Os Op OpenStack
55 En Hx Helix	56 En Dp Delphix	57 Fr Sb sbt	58 Os Mk Make	59 Os Ck CMake	60 Fr Jt JUnit	61 Fr Jm JMeter	62 Fr Tn TestNG	63 Os Ay Artifactory	64 Fm Tc TeamCity	65 Fm Sh Shippable	66 Os Cc CruiseControl	67 En Ry RapidDeploy	68 Fm Cy CodeDeploy	69 En Oc Octopus Deploy	70 En No CA Nolio	71 Os Kb Kubernetes	72 Fm Bx Bluemix
73 En Cw ISPW	74 En Id Idera	75 Os Msb MSBuild	76 Os Rk Rake	77 Fr Pk Packer	78 Os Mc Mocha	79 En Xltv XL TestView	80 Os Jm Jasmine	81 Os Nx Nexus	82 Os Co Continuum	83 Fm Ca Continua CI	84 Pd So Solano CI	85 En Xld XL Deploy	86 En EB ElasticBox	87 Fm Dp Deploybot	88 En Ud UrbanCode Deploy	89 Fr Fl Fleet	90 Os Os OpenShift

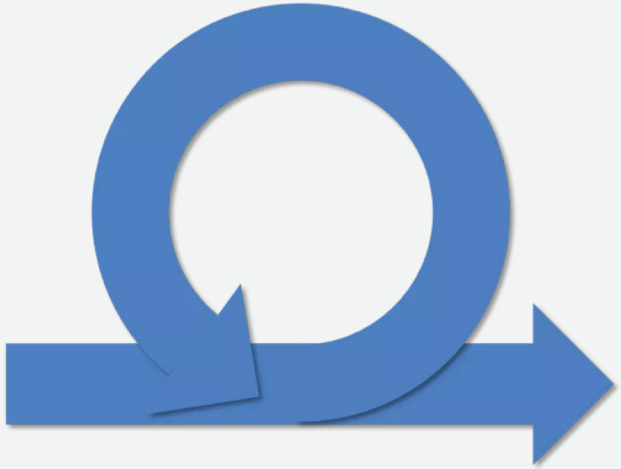
XebiaLabs
Deliver Faster

Follow @xebialabs

91 En Xlr XL Release	92 En Ur UrbanCode Release	93 En Bm BMC Release Process	94 En Hp HP Codar	95 En Au Automic	96 En Pl Plutora Release	97 En Sr Serena Release	98 Pd Tfs Team Foundation	99 Fm Tr Trello	100 Pd Jr Jira	101 Fm Rf HipChat	102 Fm Sl Slack	103 Fm Fd Flowdock	104 Pd Pv Pivotal Tracker	105 En Sn ServiceNow
106 Os Ki Kibana	107 Fm Nr New Relic	108 Os Ni Nagios	109 Os Zb Zabbix	110 En Dd Datadog	111 Os El Elasticsearch	112 En Ss StackState	113 En Sp Splunk	114 Fm Le Logentries	115 Fm Sl Sumo Logic	116 Os Ls Logstash	117 Os Gr Graylog	118 Os Sn Snort	119 Os Tr Tripwire	120 En Ff Fortify







aws

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.

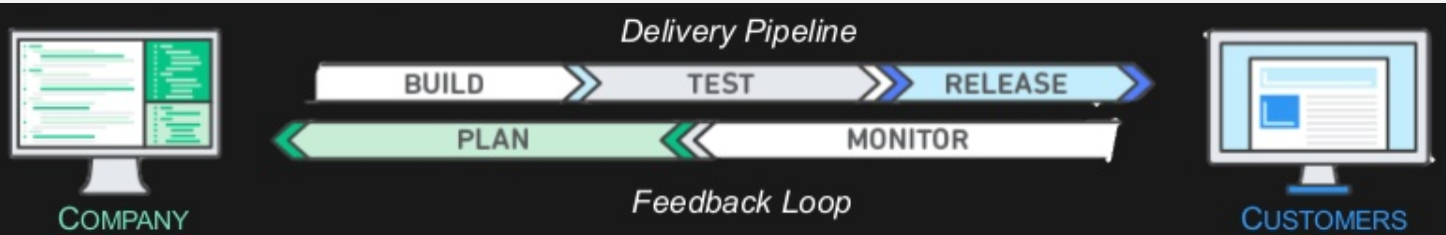
While cloud services has provided streamlined ways to achieve innovation through the principles of DevSecOps and Developer Self-Service, regulated customers are still under mandate to follow strict security, governance, and accreditation standards, which are delivered during the production deployment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

aws

AWS DevSecOps + Infrastructure Services

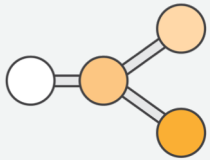
WHAT IS DEVSECOPS?

- 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
  - Everything is code



DEVSECOPS PROCESSES: 4 MAJOR PHASES

- Check-in source code
- Peer review new code



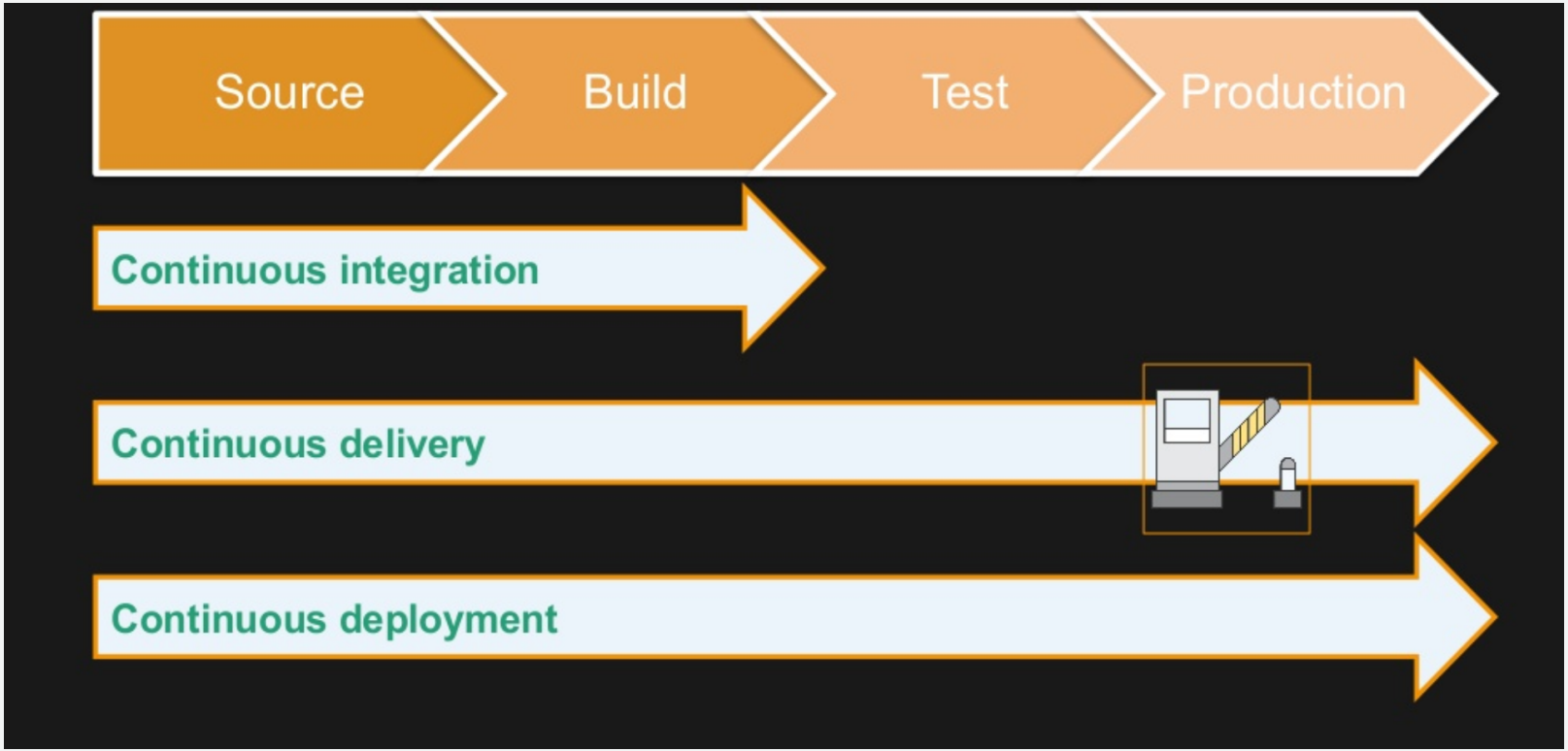
- Compile code
- Unit tests
- Style checkers
- Code metrics
- Create container images

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

- Deployment to production environments
- Continuous Monitoring

aws

DEVSECOPS RELEASE PROCESSES: LEVELS



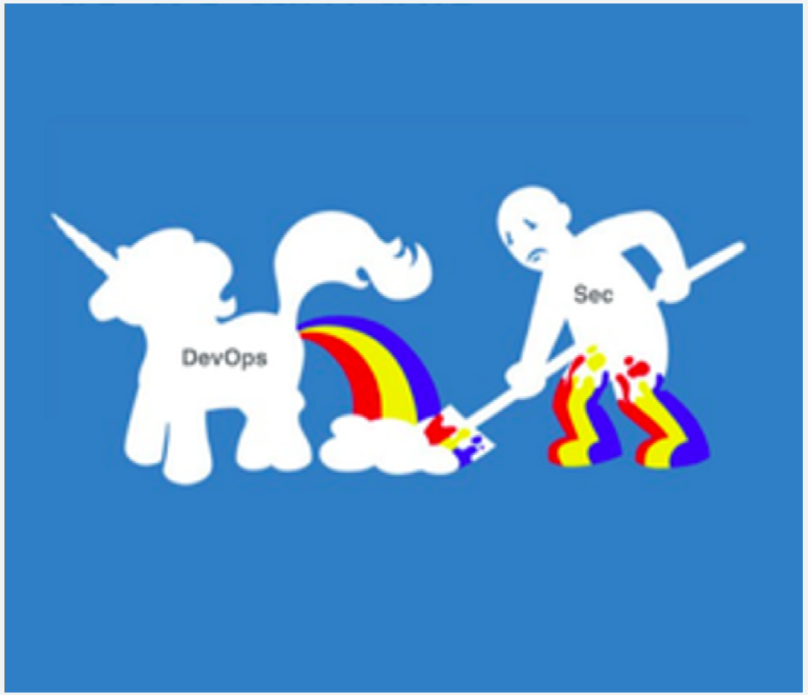
Developer Self-Service – In a Compliance Oriented World

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

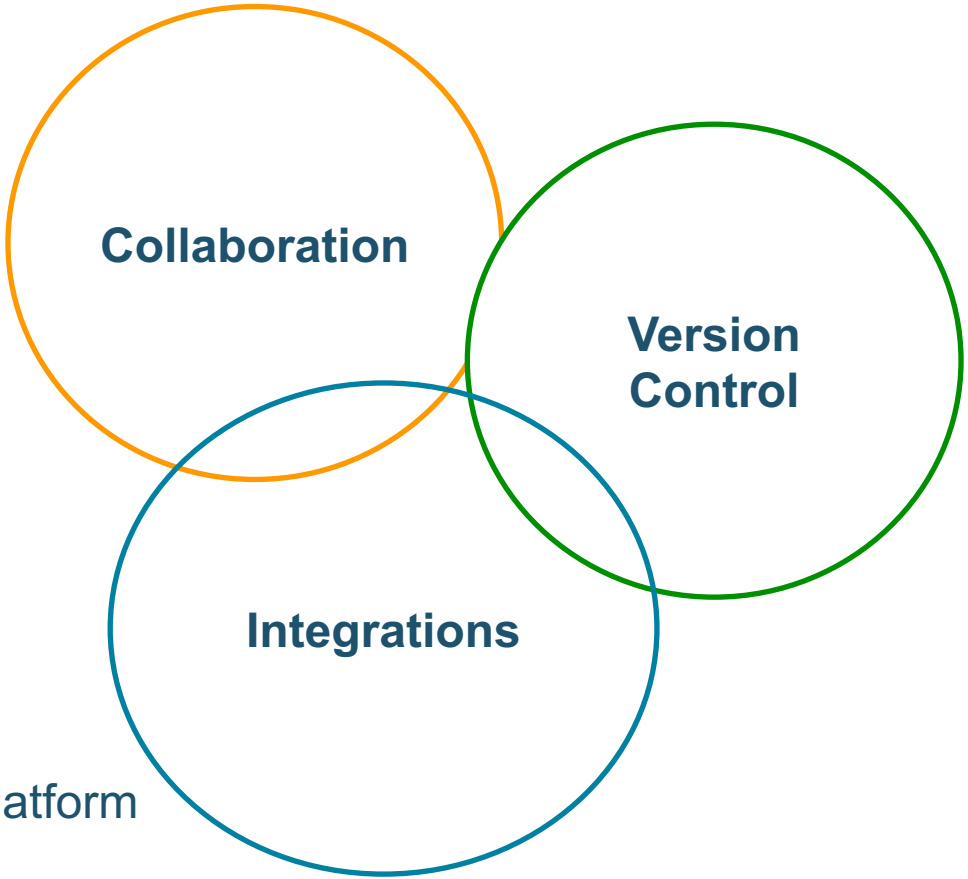
The biggest challenge is breaking out of the traditional security structures and eliminating the divide between developers, operations, and security.

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.

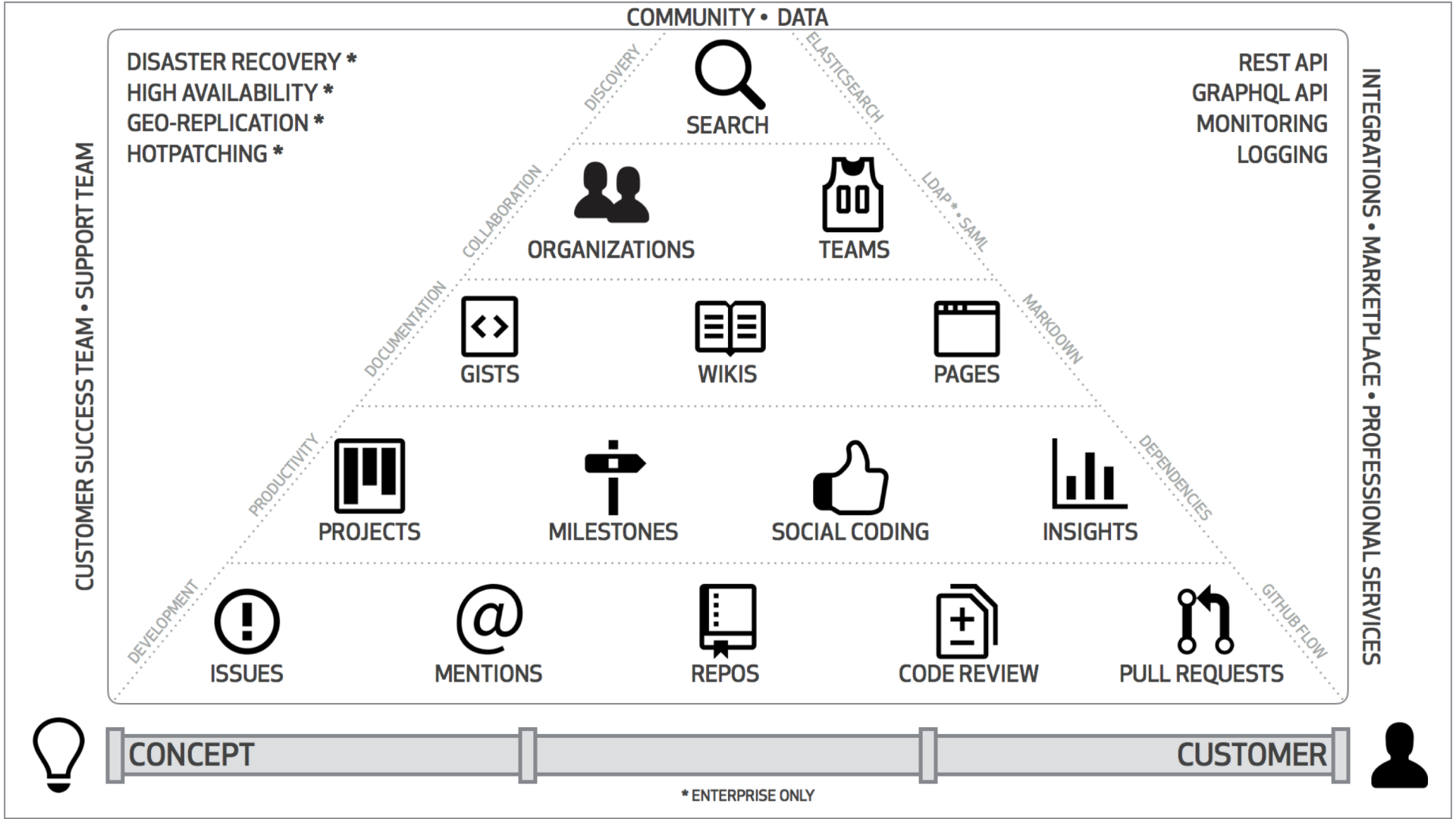
AWSome! But what actually happens in Regulated environments today?



GitHub DevOps + Collaboration Services



The Software Development Platform


COMMUNITY • DATA
DISASTER RECOVERY *
HIGH AVAILABILITY *
GEO-REPLICATION *
HOTPATCHING *
REST API
GRAPHQL API
MONITORING
LOGGING
CUSTOMER SUCCESS TEAM • SUPPORT TEAM
INTEGRATIONS • MARKETPLACE • PROFESSIONAL SERVICES
DISCOVERY
ELASTICSEARCH
SEARCH
COLLABORATION
LDAP * • SAML
ORGANIZATIONS
TEAMS
DOCUMENTATION
MARKDOWN
GISTS
WIKIS
PAGES
PRODUCTIVITY
DEPENDENCIES
PROJECTS
MILESTONES
SOCIAL CODING
INSIGHTS
DEVELOPMENT
GITHUB FLOW
ISSUES
MENTIONS
REPOS
CODE REVIEW
PULL REQUESTS
CONCEPT
CUSTOMER
* ENTERPRISE ONLY

Collaboration

By adopting social collaboration tools, companies can raise productivity by 20-25%

McKinsey and Co. Study

Collaborate on Software Code

Collaborate on Software Code
or
Collaborate on Infrastructure Code
or
Collaborate on Test processes
or
Collaborate on Governance

Everything as Code

Cost of software bugs

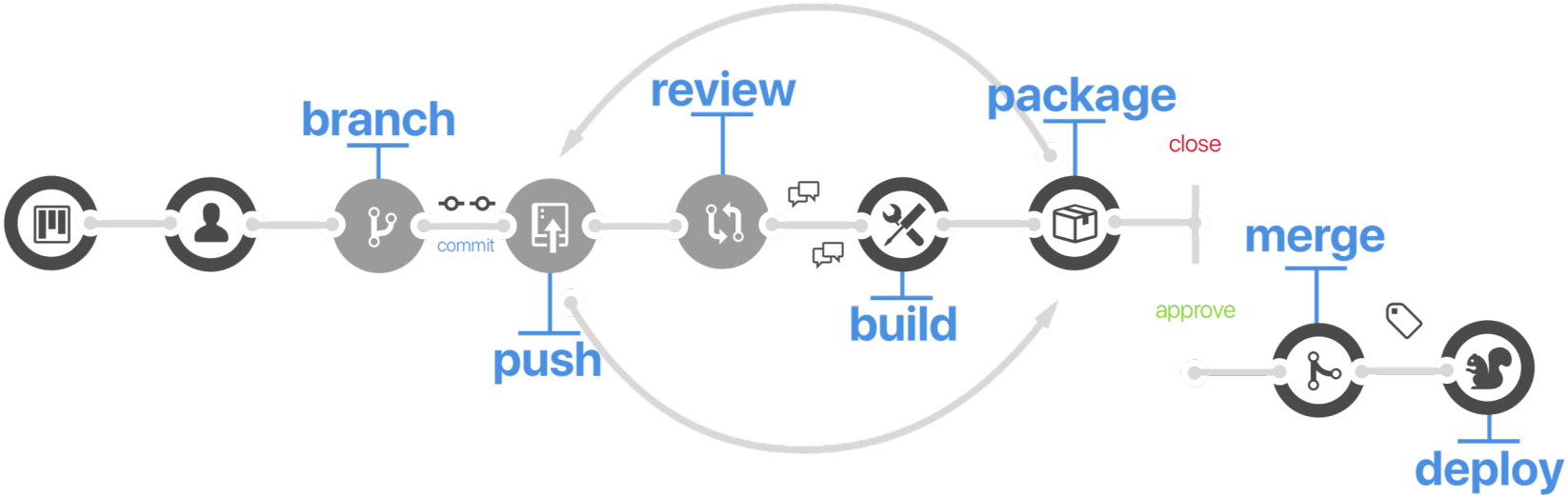
Design and architecture	Implementation	Integration testing	Customer beta test	Postproduct release
1X*	5X	10X	15X	30X

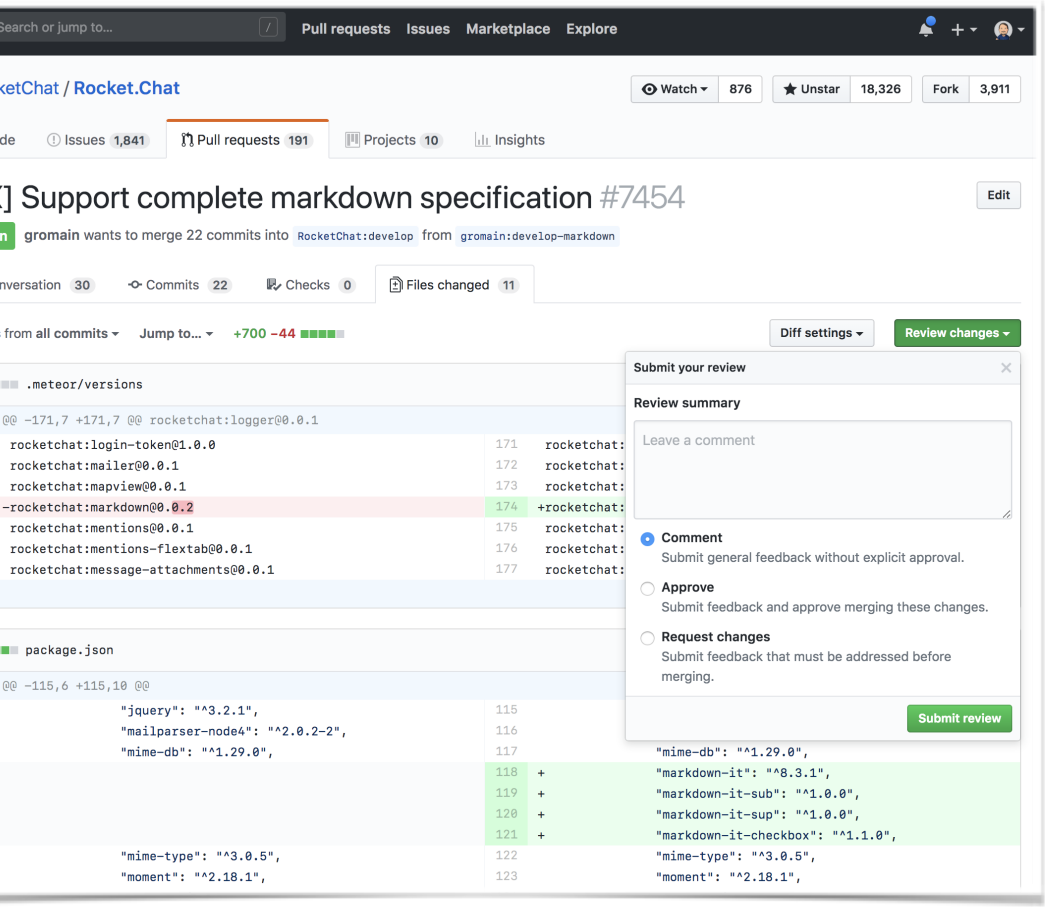
*X is a normalized unit of cost and can be expressed in terms of person-hours, dollars, etc.
Source: National Institute of Standards and Technology (NIST)†

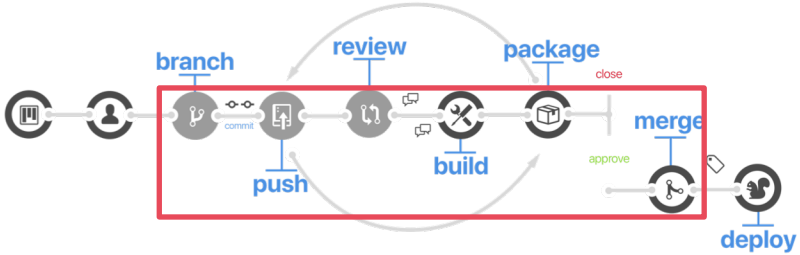
By catching defects as early as possible in the development cycle, you can significantly reduce your development costs.

source: IBM research, 2008 ftp://ftp.software.ibm.com/software/rational/info/do-more/RAW14109USEN.pdf

Modern Developer Workflow







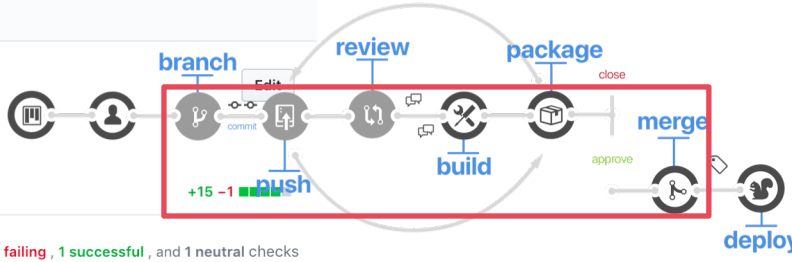
Improve code quality utilizing the integrated code review capabilities

Code | Issues 32 | Pull requests 48 | Projects 4 | Wiki | Insights | Settings

Fix broken layout in profile view #1340

Open **KellyKent** wants to merge 19 commits into `master` from `kellykent/update-deps`

Conversation 8 | Commits 24 | Checks 3 | Files changed 7



`6233092` — Wire up to work with debugger

1 failing, 1 successful, and 1 neutral checks

Super-CI
Failed — 16 hours ago — Re-run all

- core-app-tests
- syntax-linter
- visual-diff

syntax-linter

Re-run

Failed

built **16 hours ago** in **less than 5 seconds** with **1 failure**

`6233092` by **@KellyKent**

kellykent/update-deps

Build report

Inspected 4,287 lines. 3 lines need your attention.

ANNOTATIONS

Check failure on line 9

Super-CI Syntax error: order/properties order

```
Error on LN9 of app/assets/stylesheets/profiles.scss
-----------------------------------------------
9:7    Expected "width" to come before "height"   order/properties-order
```

Show raw output

Check warning on line 84

Super-CI Warning: test all classes used in markup have associated styles

```
The following CSS classes were used in class attributes but have no style rules referencing them:

Class name                    Seen in
-------------------------------------
```

It's not just humans that need to collaborate, but **your tools as well**

Convert team repository permission to details-menu Verified a27c5e6

dgraham requested a review from **github/web-systems** 5 days ago

dgraham commented 5 days ago

I opened github/details-menu-element#11 to ignore clicks on the disabled buttons in this menu.

dgraham added some commits 4 days ago

`Update details-menu to 0.6.2` Verified 176a779

`Read test value from button menu item` Verified 88a4da4

dgraham requested review from **josh** and **keithamus** as code owners 4 days ago

`Convert team project permissions to details-menu` Verified 5fe64a6

dgraham requested a review from **github/github-projects** as a code owner 4 days ago

jakeboxer reviewed on behalf of **github/github-projects** 4 days ago View changes

Projects menu changes look good, 👍 from **@github/github-projects**

dgraham added some commits 4 days ago

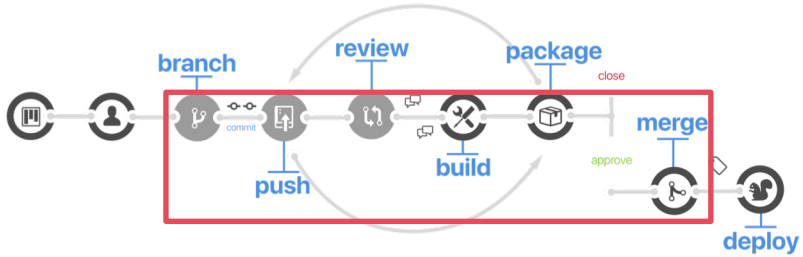
`Convert project permissions to details-menu` Verified b870406

`Remove unused form submit` Verified 6fb42b7

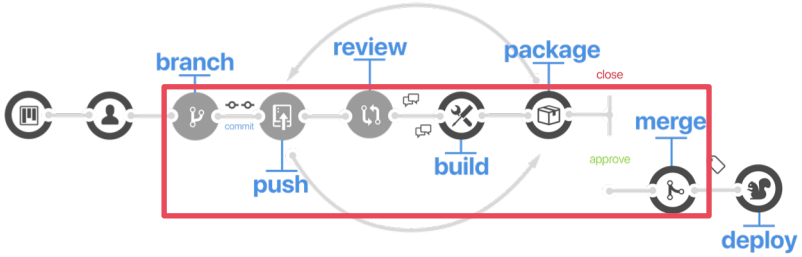
dgraham reviewed 4 days ago View changes

app/assets/modules/github/orgs/repo-permission-select.js

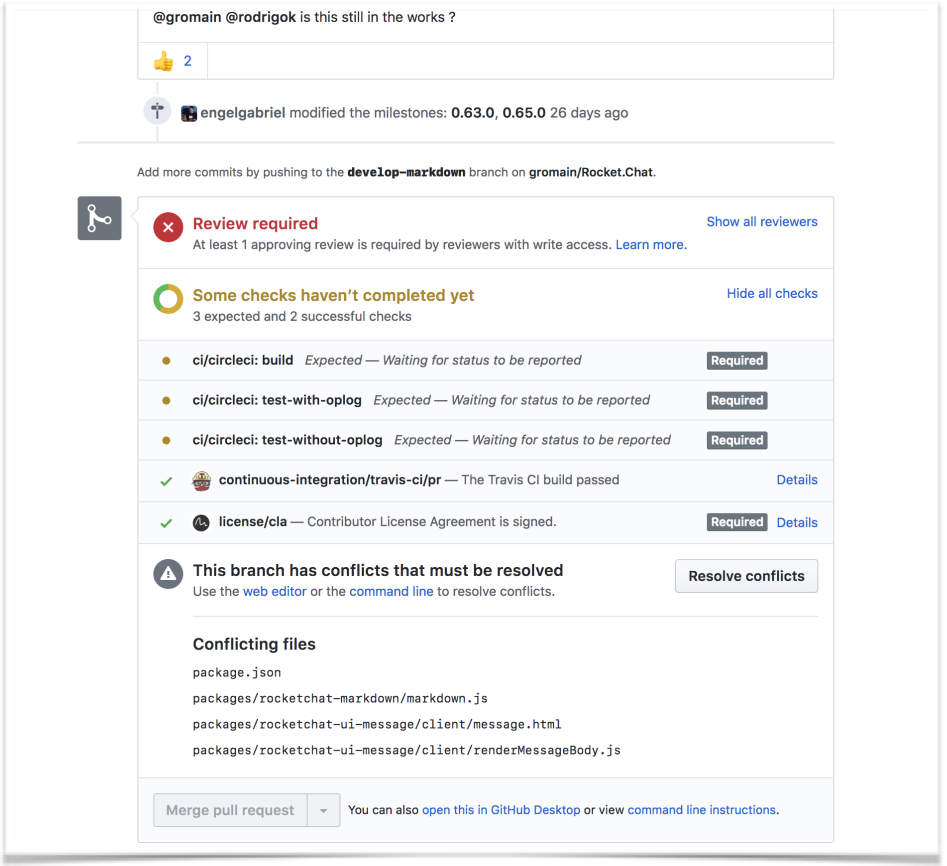
```
8  - // TODO Replace with details-menu and form submit buttons.
9  - on('selectmenu:selected', '.js-select-repo-permission', function(event)
10 -   submit(cast(event.currentTarget, HTMLFormElement))
11 - })
```



and track **those tools** over time



Enforce compliance policies with **branch statuses**, **branch protection**, **required reviews** and inline **conflict resolution**

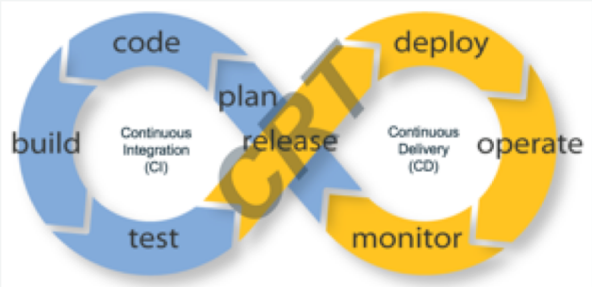


How this makes SAO GitHub + AWS

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.

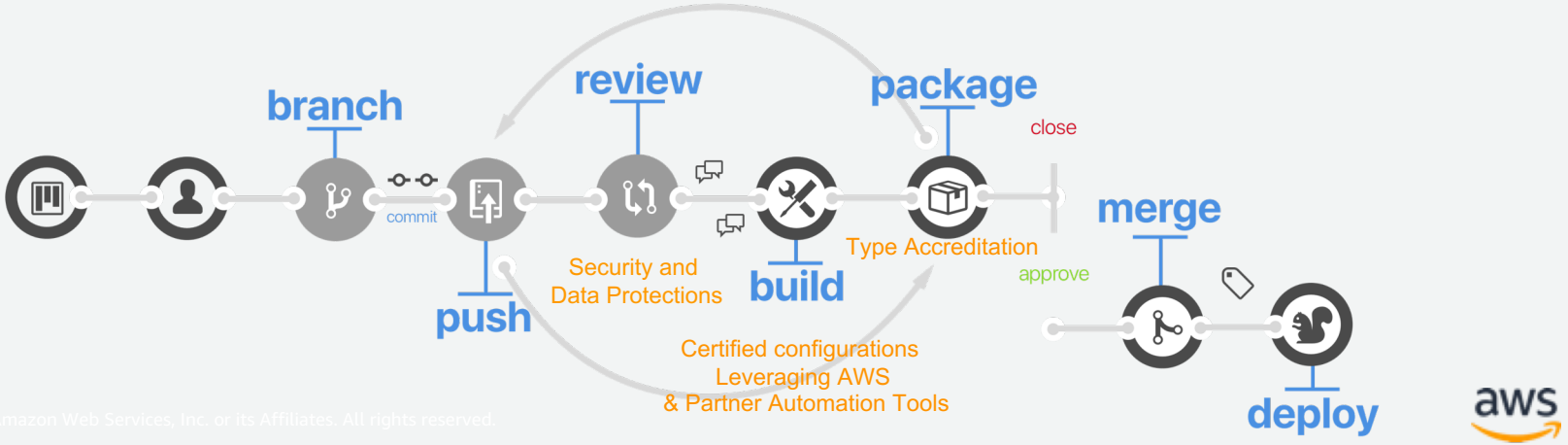


* CRT is a process and technology approached which is designed to detect, maintain and in *MOST* case correct security, compliance and threats associated with an organization's solution and service deployment within their AWS account. CRT processes monitor security controls in real-time to ensure the 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.

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)



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)

aws

AWS + SAO – The Keys Automating Audit

How is auditing easier on AWS?

Auditors demand improvements:

- You're done with manual controls
- Sample testing is not representative
- AWS + Amazon Partner solutions = *Better Together* security capability
- AWS customer audits can be relied on

Goals – SAO Assessment, Audit, Certification

Through - ***Modernizing Technology Governance***:

*Adopting "**prevent**" controls, making "**detect**" controls more powerful and comprehensive*

aws

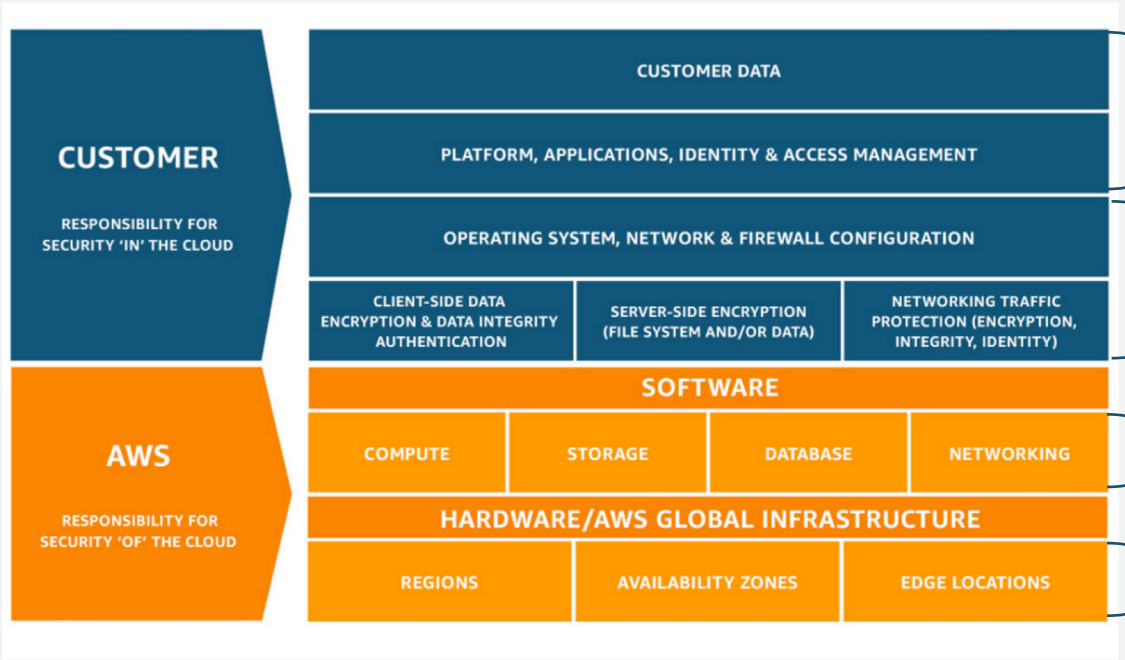
Type Accreditation (Concepts & Practices)

A form of accreditation which is used to authorize multiple architectures for an application deployment or General Support System (GSS) for operation within an approved deployment recommendation with the same type of computing environment. (e.g. AWS region)

A type accreditation can satisfy certification (***Pre-Audit***) requirements only if the application or system consists of a common set of tested and approved environments, software, and underlying infrastructure.

aws

Shared Responsibility – FISMA, FedRAMP & DoD



SAO - FedRAMP authorization package as CODE

Certification, Accreditation and Security Assessment (CA), Awareness & Training (AT), Planning (PL), Personnel Security (PS), Risk Assessment (RA) and System & Services Acquisition (SA)

SAO - FedRAMP Engineering & Operations as CODE

Access Control (AC), Audit & Accountability (AU), Configuration Management (CM), Maintenance (MA), Contingency Planning (CP), Identity and Authentication (IA), Incident Response (IR), Maintenance (MA), System and Communication Protection (SC) and System and Information Integrity (SI)

Media Protection (MP) and Maintenance (MA)

Physical and Environmental (PE) and (Partial) Contingency Planning (CP)

AWS Artifact - FedRAMP Partner Package Customer Responsibility Matrix (CRM)

https://aws.amazon.com/artifact/

AWS – FedRAMP (M & H)
DoD SRG (IL4 & IL5)
DFARS

AWS GovCloud (US)
AWS East/West

Focus areas for Type Accreditations

- **Configuration Management of Operational Controls** - Common controls implementation, (e.g. Provisioning, Managing, Controlling, and Documenting) installations and changes for each deployment is critical to success.
    - It is especially important that configuration of the common security control tracking (e.g. Dashboard) which can control, constrain and guard-rail this process.
    - Deviations should be treat (real-time) based on risks associated with the modifications prior to authorization.
- **Communications** - Effective controls status ***MUST*** be maintained and security control responsibilities tracked in support of the master assessment plan and accreditation.
- **Environmenta**l -Specific Security Impact Analysis based "***As-Built"*** *and* correct desired state
    - **Specific deviations** - an impact analysis must be conducted to determine if any additional risk has been introduced to the overall system due to site

-

AWS FedRAMP ATO's issued in 2018

AWS East/West ATO's

US GovCloud ATO's

SAO – Pilot Deployment's in 2018

ATO's & Certifications

ORION HEALTH

GitHub

WORLD WEB TECHNOLOGY

circleci

SHERLOCK

CORPORATE SEAL OF THE CITY OF SEATTLE 1869

World Vision

CollegeBoard

ATO's and Certifications in Process

Innovest
Forward thinking financial technology

smartsheet

BLUECAT™

splunk>

CONCUR

tyler technologies

SYMPHONY

PEARSON Education

NCR

redhat.

SNC SIERRA NEVADA CORPORATION Space Systems

The International Justice and Public Safety Network (Nlets)

Nlets

A gateway that supports communications between states, US territories, federal agencies, Canada and INTERPOL (International Criminal Police Organization).

Provides for the interstate and/or interagency exchange of criminal justice and criminal justice related information over a computerized, high-speed message switching system.

UNITED STATES MARINE CORPS

ROK TECHNOLOGIES

CloudCheckr

aws

Thank You!

DevOps and Security Better Together – Architecture

Continuous Integration (CI)
Continuous integration is a software development practice where developers regularly merge their code changes into a central repository, after which automated builds and tests are run. The key goals of continuous integration are to find and address bugs quicker, improve software quality, and reduce the time it takes to validate and release new software updates.

Continuous Delivery (CD)
Continuous delivery is a software development practice where code changes are automatically built, tested, and prepared for a release to production. It expands upon continuous integration by deploying all code changes to a testing environment and/or a production environment after the build stage. When continuous delivery is implemented properly, developers will always have a deployment-ready build artifact that has passed through a standardized test process.

Continuous Risk Treatment (CRT)
Continuous Risk Treatment is a modernized continuous monitoring process and technology approached which is designed to detect, maintain and in selected cases correct security, compliance and threats associated with an organization's solution and service deployment within their operational cloud environment as new needs or cyberthreats emerge.

aws

DevOps – SecOps Cont….

Microservices

The microservices architecture is a design approach to build a single application as a set of small services. Each service runs in its own process and communicates with other services through a well-defined interface using a lightweight mechanism, typically an HTTP-based application programming interface (API). Microservices are built around business capabilities; each service is scoped to a single purpose. You can use different frameworks or programming languages to write microservices and deploy them independently, as a single service, or as a group of services.

Infrastructure as Code

Infrastructure as code is a practice in which infrastructure is provisioned and managed using code and software development techniques, such as version control and continuous integration. The cloud's API-driven model enables developers and system administrators to interact with infrastructure programmatically, and at scale, instead of needing to manually set up and configure resources. Thus, engineers can interface with infrastructure using code-based tools and treat infrastructure in a manner similar to how they treat application code. Because they are defined by code, infrastructure and servers can quickly be deployed using standardized patterns, updated with the latest patches and versions, or duplicated in repeatable ways.

Configuration Management

Developers and system administrators use code to automate operating system and host configuration, operational tasks, and more. The use of code makes configuration changes repeatable and standardized. It frees developers and systems administrators from manually configuring operating systems, system applications, or server software.

Policy as Code

With infrastructure and its configuration codified with the cloud, organizations can monitor and enforce compliance dynamically and at scale. Infrastructure that is described by code can thus be tracked, validated, and reconfigured in an automated way. This makes it easier for organizations to govern changes over resources and ensure that security measures are properly enforced in a distributed manner (e.g. information security or compliance with FedRAMP, PCI-DSS or HIPAA). This allows teams within an organization to move at higher velocity since non-compliant resources can be automatically flagged for further investigation or even automatically brought back into compliance.

aws

Sample - SAO Microservices Architecture

CIS Benchmark on AWS - AWS Foundations Benchmark
This Quick Start implements the CIS AWS Foundations Benchmark, which is a set of security configuration best practices for hardening AWS accounts, and provides continuous monitoring capabilities for these security configurations. These industry-accepted best practices provide AWS users with clear, step-by-step implementation and assessment procedures. The goal of this Quick Start is to make the implementation of core AWS security measures straightforward for security teams and AWS account owners. Reference: AWS CIS Foundation Benchmark Quick Start

Amazon Virtual Private Cloud - Modular and Scalable VPC Architecture
This Quick Start provides a networking foundation based on AWS best practices for your AWS Cloud infrastructure. It builds a virtual private network (VPC) environment with public and private subnets where you can launch AWS services and other resources. Use this Quick Start as a building block for your own deployments. You can scale it up or down as needed, and add other infrastructure components and software layers to complete your AWS environment. Reference: AWS VPC Quick Start

CIS Hardened Amazon Machine Images (AMI'S)
Hardened according to a Level 1 CIS Benchmark that is developed in a consensus-based process and that is accepted by government, business, industry, and academia. Hardened according to a Level 1 Benchmark, these version are intended to provide a clear security benefit without inhibiting the utility of the technology beyond acceptable means. Pre-configured to align with industry best practices that are developed and supported by CIS. Reference: CIS AWS Marketplace

GitHub Enterprise on AWS – Quick Start
This Quick Start deploys a GitHub Enterprise is a development and collaboration platform built on Git that enables developers to build and share software easily and effectively. It provides an integrated platform for continuous integration and development, a non-linear workflow for collaboration, and in-depth monitoring and auditing for administrators. By deploying GitHub Enterprise on AWS, you can take advantage of a configurable infrastructure for your coding and deployment tasks. Reference: GitHub Quick Start

Puppet on AWS – Quick Start
This Quick Start automatically deploys a Puppet master and Puppet agents on AWS. Puppet is a declarative, model-based configuration management solution that helps you define the state of your IT infrastructure, and automatically enforces that desired state on your systems. The Quick Start deploys the Puppet master, performs the initial server setup, and creates Linux and Windows-based Puppet agents. Reference: Puppet Quick Start

Linux Bastion Hosts Quick Start
This Quick Start creates a new AWS architecture with bastion host instances, or deploy the bastion hosts into your existing AWS infrastructure. The bastion hosts provide secure access to Linux instances located in the private and public subnets. The Quick Start architecture deploys Linux bastion host instances into every public subnet to provide readily available administrative access to the environment. The Quick Start sets up a Multi-AZ environment consisting of two Availability Zones. If highly available bastion access is not necessary, you can stop the instance in the second Availability Zone and start it up when needed. Reference: Linux Bastion Host Quick Start

Jump box (Windows) Quick Start
This Quick Start reference deployment guide includes architectural considerations and configuration steps for deploying Remote Desktop Gateway (RD Gateway) on the Amazon Web Services (AWS) Cloud. It discusses best practices for securely accessing your Windows-based instances using the Remote Desktop Protocol (RDP) for remote administration.
Reference: RD Gateway Quick Start

Active Directory Domain Services on AWS – Quick Start
This Quick Start deploys Microsoft Active Directory Domain Services (AD DS) on the AWS Cloud. AD DS and Domain Name Server (DNS) are core Windows services that provide the foundation for many Microsoft-based solutions for the enterprise, including Microsoft SharePoint, Microsoft Exchange, and .NET Framework applications.
Reference: AD DS on the AWS Quick Start

Yubico YubiKey - USB-A, Two-Factor Authentication
Multi-protocol security key, providing strong two-factor, multi-factor and password less authentication, and seamless touch-to-sign. Supports FIDO2, FIDO U2F, one-time-password (OTP), and smart card; choice of form factors for desktop or laptop. The Security Key by Yubico combines hardware-based authentication, public key cryptography, and the U2F and FIDO2 protocols to eliminate account takeovers. Reference: Yubico on Amazon

Deep Security on AWS – Quick Start
This Quick Start automatically deploys Trend Micro Deep Security on AWS, using AWS services and best practices. Trend Micro Deep Security is a host-based security product that provides Intrusion Detection and Prevention, Anti-Malware, Host Firewall, File and System Integrity Monitoring, Log Inspection, and Content Filtering modules in a single agent running in the guest operating system. Reference: Trend Micro – Quick Start

SAO Microservices Architecture Cont....

Sherlock Cloud Security – AWS Managed Detection and Response
Elastic-based, high-performance logging and event management modular SIEM which can scale to any size environment. Meets all audit log and alerting requirements, all storage contained within the environment, all controls configured to log data to SIEM and Includes relevant reports and dashboard regarding logging, file integrity, antivirus, user logins, etc. Open platform allows unlimited customization. Reference: Sherlock.io

SAINT (pre-authorized) in AWS
SAINT provides integrated vulnerability scanning, penetration testing, and vulnerability management from an easy-to-use web interface. Powerful dashboards, analytics, reporting, and asset tagging make it easy to manage your results. A large selection of scan policies and report templates help you demonstrate compliance with PCI, FISMA, HIPAA, NERC CIP, SOX, and more. Reference: Saint in AWS Marketplace

The Barracuda CLoudGen WAF
Barracuda WAF detects all inbound web traffic and blocks SQL injections, cross-site scripting, malware uploads, volumetric & application DDoS, or any other attacks against your web applications. The integrated access control engine enables administrators to create granular access control policies for Authentication, Authorization & Accounting (AAA), which gives organizations strong authentication and user control. Refence: Barracuda CloudGen WAF for AWS

CloudCheckr for AWS
CloudCheckr is the comprehensive cloud management platform (CMP) for modern enterprises, resellers, and the public sector. CloudCheckr software enables clients to optimize costs, security, and compliance in the cloud, effectively managing their multi-cloud infrastructure from a unified view. With 550+ Best Practice Checks, CloudCheckr simplifies the way IT, finance, and security teams improve cloud governance, strengthen security posture, and automate key tasks across AWS.
Reference: CloudCheckr in AWS Marketplace

aws