ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

By Malini Rao

Security Tools in CI/CD Pipeline on Cloud

Disclaimer:
I am not promoting or endorsing any cloud service provider or products in this presentation and ensuring responsible cyber security. No confidential information is disclosed in this presentation. The views expressed are my independent views and any usage of third party images, research statistics sources are clearly highlighted in the presentation slides.

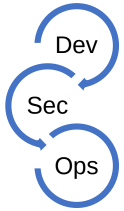
Agenda

- Who Am I
- What is DevSecOps or Security for DevOps?
- Cloud computing & DevSecOps
- Cloud Computing- Shared responsibility model
- Latest Data breaches on Cloud & App layer
- Lessons Learned: Top Threats in cloud & DevOps environment
- Develop Robust and Effective DevSecOps on cloud strategy
- Typical CI/CD Pipeline
- Security Best Practices for CI/CD Pipeline on cloud
- Security tools to consider in CI/CD Pipeline on AWS, Azure and GCP cloud
- Q&A

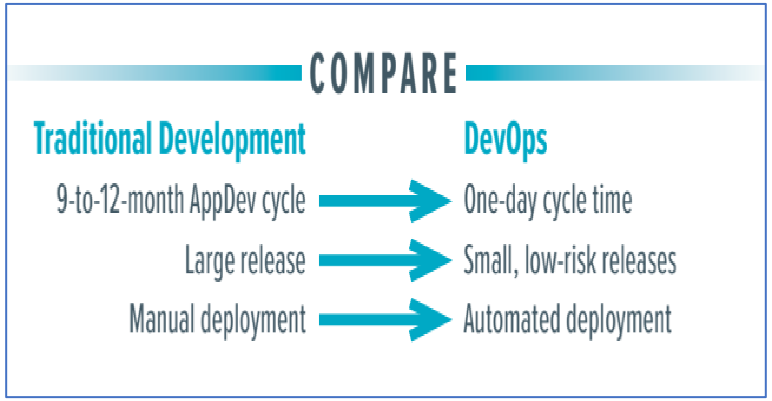
Who Am I?

- Cyber security professional with over 2 decades of experience in information security, Cyber security, Cloud security, Governance, Risk & Compliance
- Promoter of Women in Cybersecurity and Board Member of w-cs, ISSA www.w-cs.in
- Worked with Large IT service providers, Big 4's, Financial services organizations and Fortune 500 clients globally as Cyber security & GRC Solution Architect and in Global Leadership roles.
- National and International speaker on cybersecurity topics
- Published various articles, whitepapers in cybersecurity magazines
- Recognized as one of the Top 10 Women cybersecurity power players globally Ref: https://www.scmagazine.com/home/security-news/women-in-security/women-in-security-powerplayers/
- CISSP, CISM, CCSK, ISO 27001, Azure and AWS Solution Architect Certified
- Voracious reader and learner, Love travelling, Active Blogger
- Twitter: @MaliniRaocyber1
- LinkedIn: https://www.linkedin.com/in/malini-rao-cissp®-cism-ciam-prince-2-ccsk-65919b4

What is DevSecOps?

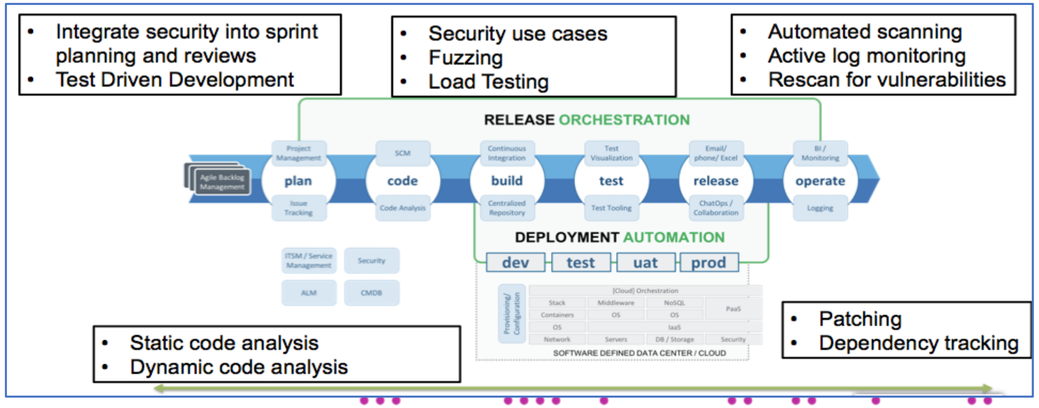


- Integrating DevOps + Security = DevSecOps
- The goal of DevOps is to give development teams more ownership in deploying and monitoring their applications by automating infrastructure provisioning and deployment of applications in a faster way and ship higher quality products.
- Adding security to this same automation is the goal of DevSecOps. Companies should create strong security policies and standards without slowing down the development process.
- Security has to be integral part of the DevOps process and automated to not slow down the DevOps process
- Implementing DevSecOps means creating a **"security as code"** culture, where security is integrated within all phases of SDLC Lifecycle and DevOps practices—keeping regulations and security top of mind while maintaining speed, agility and the innovation needed to stay ahead of cyber attacks



COMPARE

Traditional Development	DevOps
9-to-12-month AppDev cycle	One-day cycle time
Large release	Small, low-risk releases
Manual deployment	Automated deployment



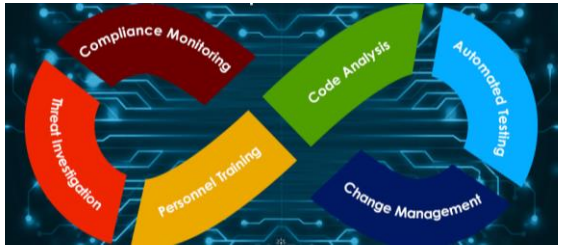
- Integrate security into sprint planning and reviews
- Test Driven Development

- Security use cases
- Fuzzing
- Load Testing

- Automated scanning
- Active log monitoring
- Rescan for vulnerabilities

- Static code analysis
- Dynamic code analysis

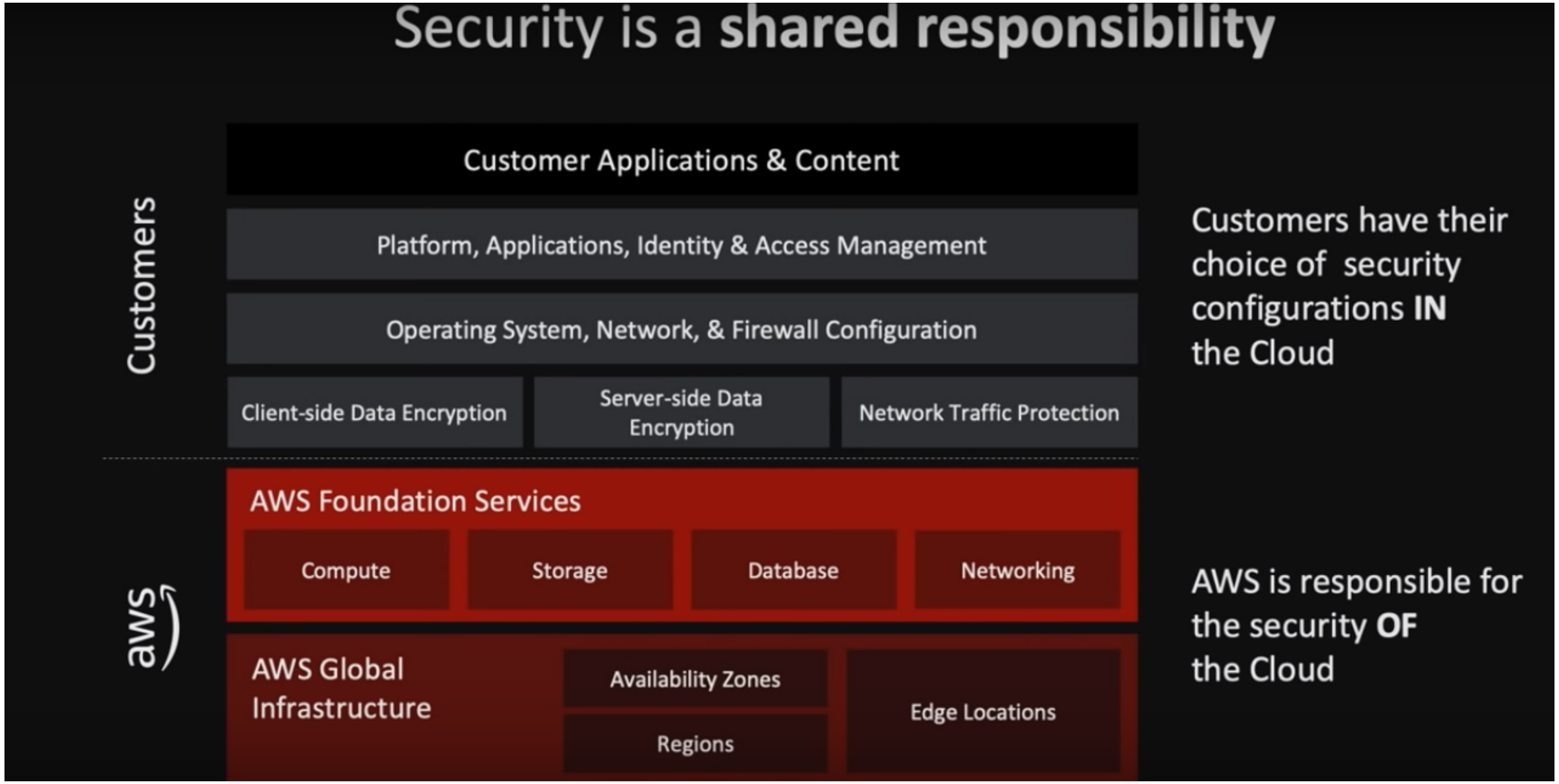
- Patching
- Dependency tracking



Cloud Computing & DevSecOps

- Organizations are adopting to cloud as it is
  - On demand
  - Pay as you go model
  - Cheap (CAPEX Vs OPEX)
  - Elastically scalable
  - Self service
  - Enhanced Flexibility
  - Rapid Implementation and time to value: Cloud implementations can be rapid relative to on-premise variants. For instance, an on-premise premise implementation could take three months, while a SaaS application of the same relative complexity and scope would only take two weeks. When organizations can deploy their key applications quicker, the return on investment and impact is also realized more rapidly.
  - Enhanced and robust security without add on applications
- Organizations are adopting to Devops culture cause of similar reasons as speed of deployment, automation, security, on demand fits well with cloud computing models of SaaS, PaaS and IaaS.
- The DevSecOps market is expected to expand at a compound annual growth rate of 31.2 percent from $1.5 billion in 2018 to $5.9 billion in 2023 as per MarketsAndMarkets
- Cloud deployment of DevSecOps offerings helps organizations with deploying code during the production process, providing enhanced security, performance and scalability. Adoption of DevSecOps offerings is highest among large enterprises due to faster development and release cycles, as well as the need for early integration of security tools into the DevOps process.

Cloud Computing- Shared Responsibility Model



Security is a **shared responsibility**

Customers

Customer Applications & Content

Platform, Applications, Identity & Access Management

Operating System, Network, & Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

Customers have their choice of security configurations **IN** the Cloud

aws

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones | Regions | Edge Locations

AWS is responsible for the security **OF** the Cloud

Source: AWS shared responsibility model

Copyright ©- Malini Rao

Latest Data Breaches on Cloud & App Layer

- Target
  - Sophisticated kill chain including exploitation of a vulnerable web application which resulted in hackers stealing names, mailing addresses, phone numbers and email addresses from over 70 million shoppers
- JP Morgan
  - Vulnerability on website built maintained by third party vendor in support of a charity which resulted in user names and passwords for 76 million households and 7 million businesses accounts were stolen
- Community Health
  - Targeted a flaw in open SSL CVE 2014-0160 better known as Heart Bleed which resulted in theft of social security numbers and other personal data belonging to 4.5 million patients

Latest Data Breaches on Cloud & App Layer

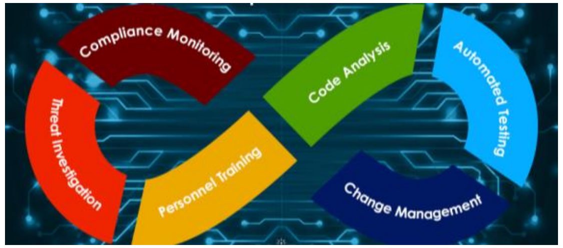
- Face book: 540 Million Facebook users records on exposed servers due vulnerability in AWS S3 bucket
- Uber: Uber fined £385,000 for data breach affecting millions of passengers. In November 2016, attackers obtained credentials to access Uber’s cloud servers and downloaded 16 large files, including the records of 35 million users worldwide. The records included passengers’ full names, phone numbers, email addresses, and the location where they had signed up. Drivers were also affected, with 3.7 million, including 82,000 from the UK, having their weekly pay, trip summaries and, in a small number of cases, driver’s license numbers accessed. 2 Hackers compromised Uber’s Github which contained access to keys to AWS and hackers stole PII of 57 Million individuals held data for ransom and was publicly disclosed late in 2017
- Capital One: A software engineer in Seattle hacked into a server holding customer information for Capital One and obtained the personal data of over 100 million people In one of the largest thefts of data from a bank. The suspect, Paige Thompson, 33, left a trail online for investigators to follow as she boasted about the hacking, according to court documents in Seattle, where she was arrested and charged with one count of computer fraud and abuse. Ms. Thompson, who formerly worked for Amazon Web Services, which hosted the Capital One database that was breached, was not shy about her work as a hacker
- Accenture: World’s first Cyber Resilience startup Up Guard discovered in its Cyber Risk survey that Accenture left at least 4 AWS S3 storage buckets unsecured. And as a result of this flaw, the data on these storage media was available for download. The data exposed in this security goof-up were authentication credentials, secret API data, digital certificates, decryption keys, customer data, and other meta info which could be easily used by cyber crooks to mint money. It was revealed in the security analysis that more than 137GB of data was available for public access and some of the data might have been siphoned by hackers to post on the dark web
- Verizon- Nice Systems, which is a 3rd party vendor working for Verizon, committed a configuration blunder on an AWS S3 bucket which exposed names, addresses, account details, and pin numbers of millions of US-based Verizon customers. ‘Nice’ agreed that the mistake was committed by one of its engineers who reportedly created a cloud-based file repository for storing customers call data which is used by Verizon for backend office and call center operations. The info included customer phone numbers, their names, and PIN which was alarming as this info can be used by attackers to gain false access to the accounts and get cloned SIMS. This incident also highlighted the fact that how alarming is the storage of sensitive info on 3rd party vendor.
- Booz Allen Hamilton- Technology consulting firm Booz Allen hired Up Guard to carry out security assessment on both its internal and externa computer systems. This assessment discovered that 60,000 files were on a public access on AWS S3 bucket owned by an intelligence and defense contract of Booz Allen. The cache is said to have exposed 28GB of data and this includes credentials of senior engineers, passwords of US Government systems, and over half a dozen of files containing unencrypted passwords of government contractors holding top Secret Facility Clearance. Following the incident, US Senator Claire McCaskill who holds a top rank in Senate Homeland Security and Government Affairs Committee issued a public statement saying the data breach was true and Booz Allen will be held seriously responsible for the leak of sensitive info.

Top Security Threats in Dev Ops and Cloud environment

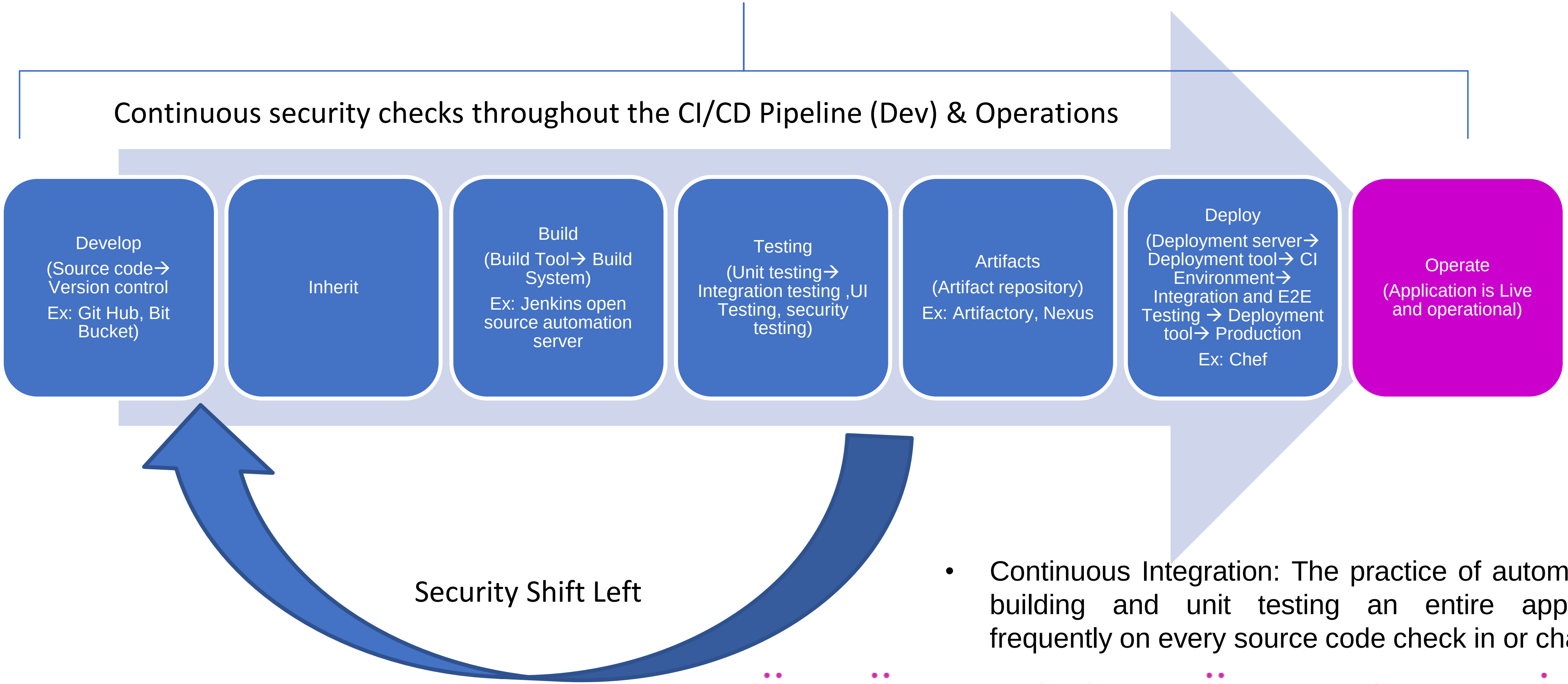
- Application abuse and misuse
- Account Take over, Bots, scrapers
- Data security
- Insecure application build
- Still following Waterfall method of security testing in Devops pipeline instead of continuous agile security testing with feedback loops built in.
- Unauthorized access
- Insecure cloud key management practices
- Risky applications, data and user access which are uncontrolled and lacks visibility, Passwords stored in clear text format and stored on Github/Bitbucket, Sharing of passwords, API Keys are exposed, Keys leaked in many ways such as hardcoded, code repo misconfigs, code repo hacked, Phishing, Exploits, Unsecured and exposed storage buckets such as S3 buckets and google cloud storage, exposed Databases such as MongoDB, Elasticsearch, Redis leading to data leakage
- Misconfigured servers and Unauthorized access
- Risky web sites are exposed to bad guys
- Threats from Insider/Insider attack
- Lack of cloud security awareness and user hygiene
- Breaking and entering attacks such as Brute Force attacks, Remote code execution, container escapes, supply chain attacks
- Malware, crypto jacking, ransomware leading to data breach

Robust & Effective DevSecOps strategy on cloud

1. Seamless collaboration of security team with Dev & Ops Team of on prem and cloud environment if hybrid cloud,
2. Security team's role here is to enable, be fast, non-blocker and automate as much as possible to ensure value enablement and always be part of Dev-Sec-Ops team as one team.
3. Regular security training and learning for Development and Operation team to ensure application security best practices are followed right from Day 1 such as security by design, secure coding/programming principles are followed, Identity & Access Management Principles are followed such as least privilege and need to know access with no sharing of passwords and secure key management on the cloud, Bug bounty program are invited and rewarded for identifying vulnerabilities such as bug crowd, hacker one, threat hunting exercises are conducted regularly including red teaming, blue teaming exercises.
4. Visibility of data into the cloud and DevOps environment
5. Encryption for data at rest and in transit such as SSL/TLS certificates application and renewals in a timely manner
6. Continuous Security Automation checkpoints built into the CI/CD Pipeline in line with speed of Devops build and release process and able to provide feedback on success or failure of pipeline execution based on the security checks and repeatable mechanism to push changes to the production
   - software vulnerability testing, Security at time of code build, commit and before production code checks
   - docker container security checks
   - Kubernetes orchestration security checks
   - Automate deployment tasks i.e Artifacts that came in from Jenkins are the ones deployed on production
   - Self service workflows and runbooks
   - Source code scans at the run time for identifying and detecting zero-day vulnerabilities and automated patching, self healing capabilities built into the code
   - Continuous auditing capabilities compliance checks to regulatory requirements including third party vendor risk assessments
   - Cloud Security Monitoring, Logging, Alerting & Notifications for configuration changes, compliance, audit,, hardening
   - Incident Response process including threat investigations should be implemented and tested on a regular basis
   - Reporting & Dashboarding with metrics



Typical CI/CD Pipeline



Continuous security checks throughout the CI/CD Pipeline (Dev) & Operations

Develop (Source code→ Version control Ex: Git Hub, Bit Bucket)

Inherit

Build (Build Tool→ Build System) Ex: Jenkins open source automation server

Testing (Unit testing→ Integration testing ,UI Testing, security testing)

Artifacts (Artifact repository) Ex: Artifactory, Nexus

Deploy (Deployment server→ Deployment tool→ CI Environment→ Integration and E2E Testing → Deployment tool→ Production Ex: Chef

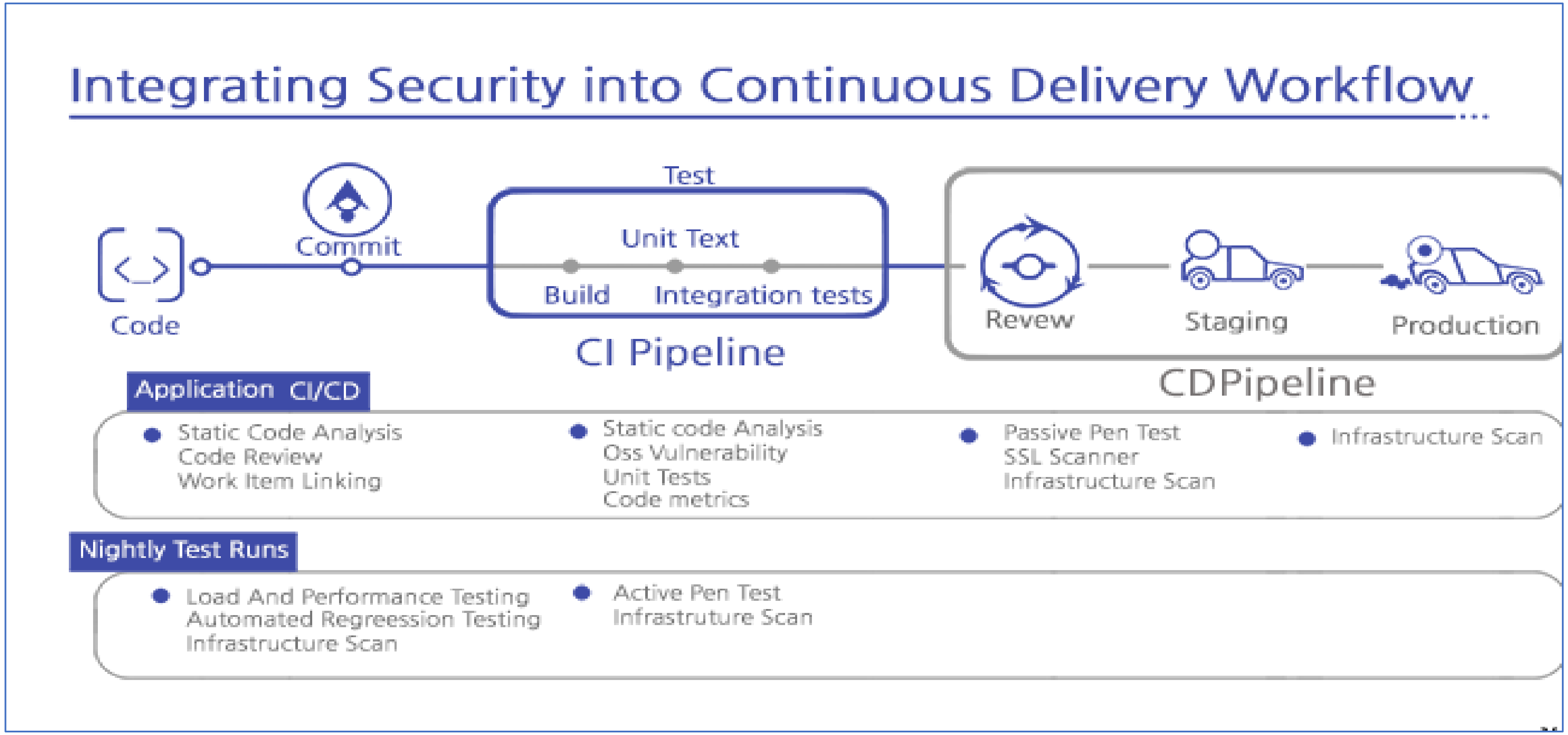
Operate (Application is Live and operational)

Security Shift Left

- Continuous Integration: The practice of automatically building and unit testing an entire application frequently on every source code check in or changes

Copyright ©- Malini Rao

Continuous Security validation in CI/CD Pipeline



Integrating Security into Continuous Delivery Workflow

Application CI/CD

- Static Code Analysis
  Code Review
  Work Item Linking
- Static code Analysis
  Oss Vulnerability
  Unit Tests
  Code metrics
- Passive Pen Test
  SSL Scanner
  Infrastructure Scan
- Infrastructure Scan

Nightly Test Runs

- Load And Performance Testing
  Automated Regreession Testing
  Infrastructure Scan
- Active Pen Test
  Infrastruture Scan

Security Best Practices for CI/CD Pipeline on cloud

Things we need to check	How do we check?
• Software Vulnerabilities for source code, license, version including for open source (OSS) in CI/CD Pipeline at the time of development/build, at the time of testing and before deployment to production, Common vulnerabilities and exposure (CVE), • Track and alert users about open source risks throughout the DevSecOps pipeline.	• Static application security testing (SAST) • Dynamic application security testing (DAST) • Interactive application security testing (IAST) • Real time application self protection (RASP)
API Security	SAST, DAST, IAST
Cloud Infrastructure Vulnerabilities	Infrastructure vulnerability assessment
Infrastructure as code Vulnerabilities	Infrastructure vulnerability assessment
Container and VM image vulnerabilities	Container and VM Image scan
Continuous auditing and Compliance to regulatory requirements such as CIS Benchmarks, PCI-DSS, SOC-2 and other regulatory requirements	Audit and compliance as code
Data visibility, Identity and access management, control over data travel	Cloud Access security broker (CASB)
Cloud monitoring, logging, alerts, notifications	Cloud security monitoring and logging
Reporting, dashboards with metrics capabilities	One click reporting with metrics capabilities as per IAM role assigned
Identity and Access management on cloud	User and role provisioning and user lifecycle management on cloud
Data security	Encryption of data at rest and in transit

Standards & Frameworks to consider

- OWASP Top 10 Risks for Web applications and API https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- Cloud control matrix from cloud security alliance
- Behavioral Driven Development Framework for security
  - BDD-Security is a security testing framework that uses natural language in a Given, When, Then Gherkin syntax to describe security requirements as features. Those same requirements are also executable as standard unit/integration tests which means they can run as part of the build/test/deploy process
  - https://iriusrisk.com/open-source/
- NIST Cyber security framework and cloud computing reference architecture
- ISO 27018: 2019, its guidance for cloud service providers who process personally identifiable information (PII)
- MITRE Attack Framework for predicting, detecting and investigating advanced cyber threats https://attack.mitre.org

ADDO
ALL DAY DEVOPS

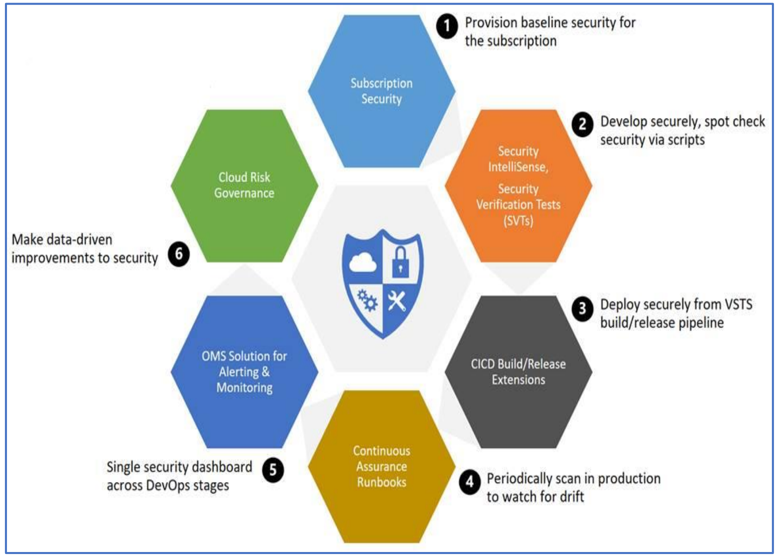
Security tools to consider for CI/CD Pipeline on AWS, Azure & GCP

Type of Checks	AWS Inbuild solutions	Azure Inbuilt	GCP Inbuilt	Open Source tools	Commercial tools with API Integration
Cloud security command center for infrastructure security	AWS Security hub	Azure Security center https://docs.microsoft.com/en-us/azure/security-center/security-center-intro	Google cloud security command center	NA	• NA
Software Vulnerabilities testing for source code, license, version including for open source (OSS) in CI/CD Pipeline at the time of development/build, at the time of testing and before deployment to production, API Security	AWS Inspector https://aws.amazon.com/inspector/	Secure DevOps Kit for Azure https://azsk.azurewebsites.net/03-Security-In-CICD/Readme.html	Google cloud security scanner https://cloud.google.com/security-scanner/	OWASP ZAP (API is limited) https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project Gauntlt Command line testing framework Supports BDD syntax to allow readable and structured tests and assists with improving collaboration between the teams that are building the application.	SAST, DAST, IAST: • CA Veracode • Checkmarx • Sonar Cloud RASP: • Contrast • Signal Sciences • Waratek Open source vulnerabilities scanning • Whitesource
Container security	None	None	Yes in Kubernetes orchestration	Clair, An API-driven static container security analysis with a huge CVE database https://github.com/coreos/clair OpenSCAP, Anchore, Dagda	Aqua security

Security tools to consider for CI/CD Pipeline on AWS, Azure & GCP

Type of Checks	AWS Inbuild solutions	Azure Inbuilt	GCP Inbuilt	Open Source tools	Commercial tools with API Integration
Visibility into the cloud & CI/CD Pipeline, Continuous Auditing capabilities and Governance, Risk & Compliance to regulatory requirements on cloud, SOC on cloud, threat detection on cloud, Incident response, threat hunting, A satisfactory level of threat protection to ensure that the security risk of using the cloud is acceptable	AWS Macie only has data discovery and data classification capabilities as per regulatory requirements	• Azure CASB • Azure Sentinel • Azure security center	Not available, integrates with commercial tools, some features in google command center		• Netskope • Sky High networks • Twist lock • Dome 9 security • Mcafee • CyberArk
Identity & Access Management on cloud	AWS IAM	Azure AD	GCP IAM	NA	• Okta IAM
Encryption of data at rest and in transit	• Encryption at AWS EC2 and AWS Storage S3 Bucket levels • AWS Key management services (KMS)		GCP uses AES 256-bit encryption and KMS		
Cloud infrastructure level controls like Firewall, Load balancer, DDoS attack monitoring solutions	• Yes as part of virtual private cloud	• Yes	Yes	NA	• Many are available such as Palo Alto, Checkpoint, Mcafee
Cloud security monitoring, threat detection and response	• Amazon Inspector, • AWS Cloud trail, • AWS Config, • Amazon Guard duty • AWS Security hub	• Azure sentinel • Azure Devops Kit • Azure security center	Google command center	OSSIM	• Threatstack • Alienvault • Evident.io • CASB Solutions • Splunk
Cloud security reporting, dashboards, metrics	• AWS Macie	• Azure Devops kit	https://status.cloud.google.com/	NA	• Cavirin cyberposture intelligence • Continnum Security • Threat Modeler

Secure DevOps Kit for Azure


1 Provision baseline security for the subscription
Subscription Security
2 Develop securely, spot check security via scripts
Security IntelliSense, Security Verification Tests (SVTs)
3 Deploy securely from VSTS build/release pipeline
CICD Build/Release Extensions
4 Periodically scan in production to watch for drift
Continuous Assurance Runbooks
5 Single security dashboard across DevOps stages
OMS Solution for Alerting & Monitoring
6 Make data-driven improvements to security
Cloud Risk Governance

https://azsk.azurewebsites.net/03-Security-In-CICD/Readme.html

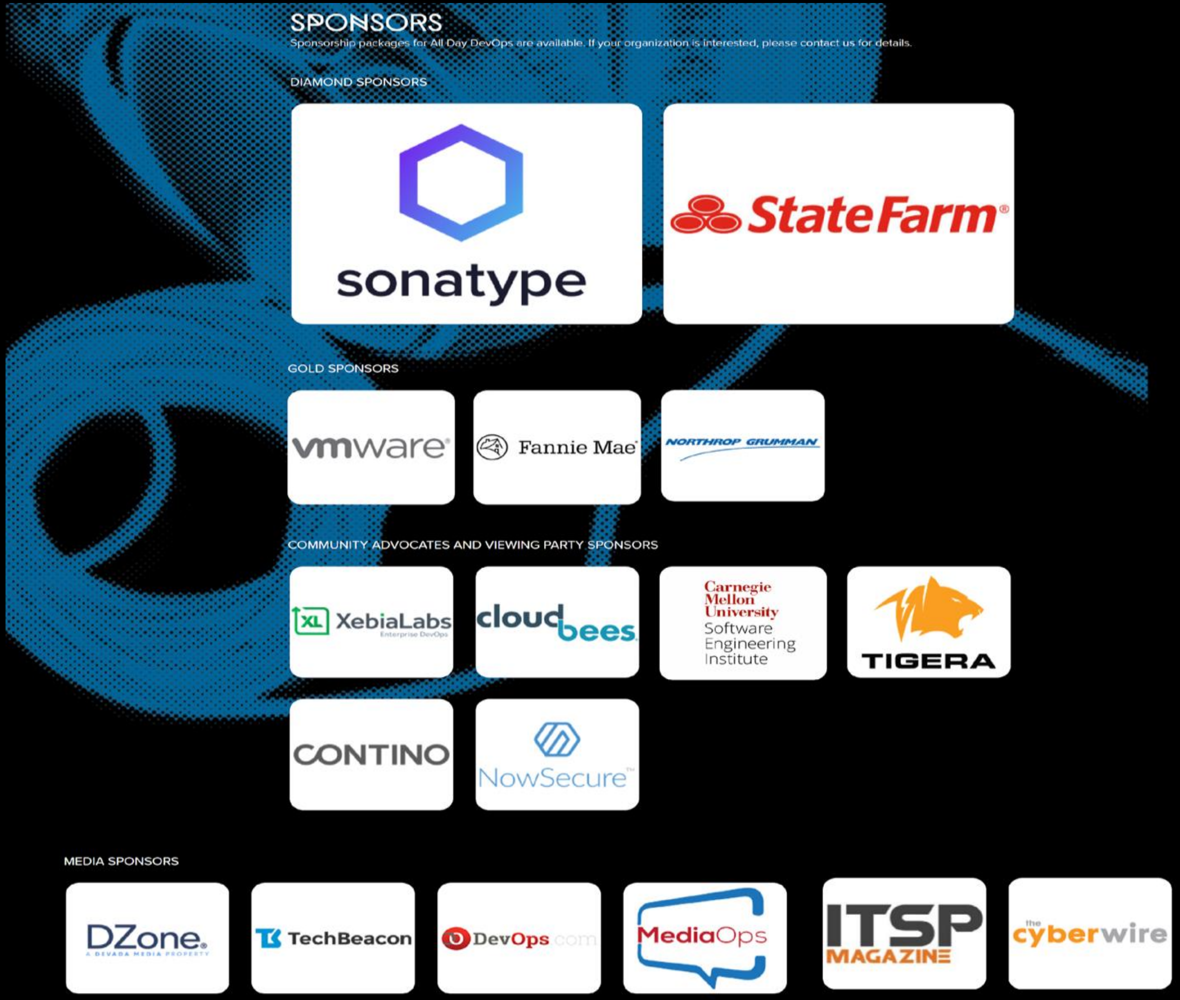
- Subscription security. This ensures that a subscription is configured and provisioned with necessary security controls.
- Secure development. This provides the ability to write secure code and spot check secure configuration of cloud resources.
- Continuous integration and continuous deployment (CI/CD) extensions. These integrate security testing into CI/CD workflows.
- Continuous assurance. This ensures that the security state stays compliant and doesn’t drift over time.
- Alerting and monitoring capabilities. These check for security events and provide an effective remediation path for subscription and application security issues.
- Telemetry dashboards. These get aggregate views of security patterns and trends to make concerted improvements

Stakeholders	Relevant AzSK capabilities
Subscription Owners	Check the overall security health of the Azure subscriptions Ensure that artifacts such as Alerts for important activities, ARM policy, resource locks, RBAC roles, etc. are properly provisioned
Development or Engineering Teams	Get inline support with security tips and corrections while writing code for Azure apps Test that Azure resources they are using for application/solutions are configured and deployed securely Enable security in CICD by including various security tests in the build/release pipelines
Deployment Teams	Ensure that a solution being deployed to a target Azure environment has an assured level of security
Operations Teams	Track security state in a 'continuous' manner and ensure that there is no downward 'drift' from a secure state
Compliance Teams	Ensure that various, often challenging, compliance requirements (e.g., SOX) are met for Azure-based solutions
Security Teams	Use all the above depending on their InfoSec domain (Architect, Analyst, etc.)

References

- OWASP Top 10 risks for web applications and API
- https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- Cloud control matrix from cloud security alliance
- Awesome Devsecops resources on Github: https://github.com/devsecops/awesome-devsecops
- https://cloudsecurityalliance.org/research/working-groups/devsecops/
- https://devops.com/automated-security-testing-continuous-delivery-pipeline/
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://cloud.google.com/security/
- https://aws.amazon.com/security/
- https://azure.microsoft.com/en-in/product-categories/security/

Q&A



SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

GOLD SPONSORS

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

MEDIA SPONSORS