



A complete guide to

Implementing

DevSecOps in AWS

aspire SYSTEMS | *attention.
always.*

for more: <https://github.com/cmakkaya>



Table of contents

1. Chapter 1	Introduction	3
2. Chapter 2	Big 5 Reasons to Opt DevOps	4
3. Chapter 3	What is DevSecOps?	6
4. Chapter 4	AWS CI/CD and Support Tools	9
5. Chapter 5	Open Source/AWS Continuous Testing Tools	10
6. Chapter 6	AWS Security, Identity, and Compliance Service	11
7. Chapter 7	DevSecOps Reference Architecture	12
8. Chapter 8	Conclusion	14



Chapter 1

- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6
- Chapter 7
- Chapter 8

Chapter 1

Introduction

With the business landscape evolving every passing day, organizations are expected to stay at the cutting edge to pacify their customers. Today, the first aspect that a customer looks for in an organization's product or service offerings is the software – either the mobile applications or the official website of the company. Businesses have realized that to hold the silver spoon against their competitors, they need to keep reinventing their products or services and always be the first candidate to enter the market with a new set of offerings. This has led to a faster evolution of software development methodologies including Lean, Agile, DevOps etc. to meet these requirements. In order to improve quality, businesses are focused on the user needs early in the project, involve development and operations gradually, and break the project into smaller pieces to allow for frequent testing. The abundance of infrastructure-as-a-service (IaaS) offerings has been an instrumental catalyst in this transformation.

There is also a flip side to this. As businesses start focusing on going digital, the software applications and data are vulnerable to hackers and cybercrimes. The efforts by businesses to move to a secure development cycle have been focused on the traditional methods of security – the waterfall model. While DevOps comes to the fore, traditional security approaches are being discarded

due to the slow and vulnerable nature.

DevOps is a popular approach that makes cybersecurity vigilance a reality by embedding the right tools into your software development lifecycle. In this eBook, we explain why and how implementing DevOps into your existing AWS Cloud applications is paramount for your business.





Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 2

Big 5 Reasons to Opt DevOps

With cloud taking the helm in today's scenario, businesses need to have a robust security plan. However, most of them don't have the time or resources to have a dedicated team that does everything from the scratch. Instead, businesses can start by securing applications based on the risk levels. More often than not, organizations begin with securing the service or applications they know is the right fit or try risking with multiple, expensive security appliances.

While the IT teams are engrossed in transitioning core services, security becomes the least priority. Also, some businesses are still confused about where the CSP's responsibility ends and the customer's responsibility begins, or what is the best way to secure their services and products.

DevOps contributes to both software development teams and the customers, saving organizations a large chunk of money and resources. We have listed 5 reasons why:

1. Innovation

One of the key benefits of the DevOps model is its high velocity. Organizations are able to remain at the cutting edge by being able to adapt to the fluctuating market requirements, innovate faster, and become more efficient in achieving their

business targets.

A global geolocation company achieved 30% reduction in deployment time, 30% reduction in infrastructure costs, and 30-40% less time in CI/CD pipeline.

2. Higher customer satisfaction

As you may imagine, DevOps brings a multitude of business benefits to organizations. By providing end-users with high quality software and excellent experience, DevOps helps create a strong relationship with customers and providing them with more reliable applications, faster. DevOps also helps the IT teams in discovering issues earlier and thus prevent bugs from passing through the development stage and appearing in the final output.

3. Better Collaboration

The introduction of DevOps brings about some serious cultural changes within the organization. The increased communication and collaboration between the internal teams in an organization means the process becomes transparent with open lines of communication – sharing knowledge and best practices to build a successful process.



4. Increased flexibility

As mentioned earlier, with the advent of DevOps, organizations have found a way to adapt to the fluctuating market standards. The IT teams have been able to optimize their time and resources based on the customer requirements.

5. Faster time to market

Through better collaboration between the teams,

DevOps promises shorter development cycle time by increasing the frequency of releasing code into production.

A State of DevOps report from 2019 found that teams that have implemented DevOps deploy 208 times more frequently and 106 times faster than other organizations.





Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

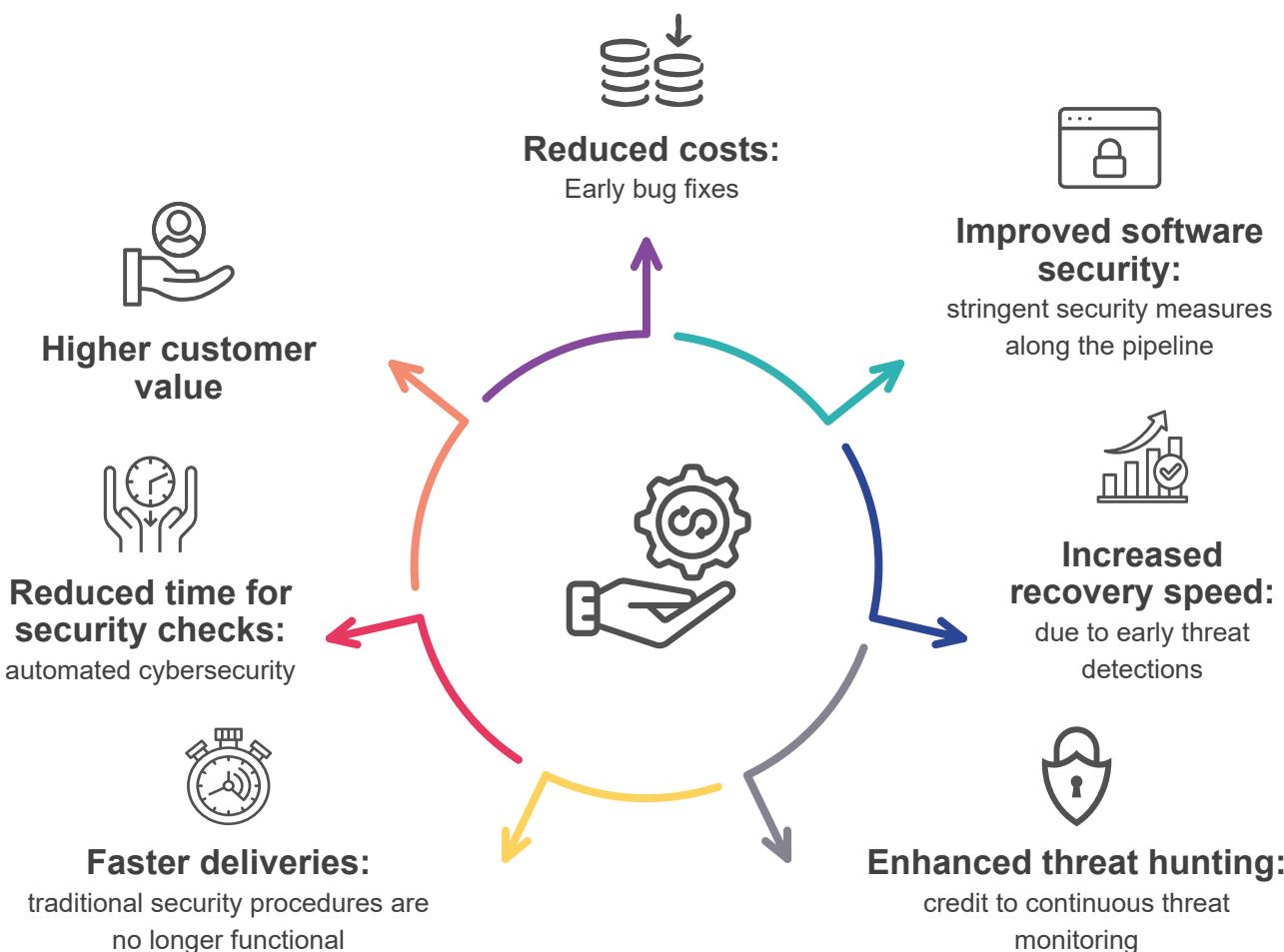
Chapter 3

What is DevSecOps?

DevOps allows companies to deliver new application features and innovative services to customers at a faster pace. DevSecOps takes this one step further by integrating security into the mix. By leveraging DevSecOps, organizations can deliver secure applications at will while the automation takes care of the operations.

DevSecOps implements continuous and automated security mechanisms during the infancy stages of software development and warrants security throughout the cycle.

Integrating security into your IT teams will help you achieve the following:

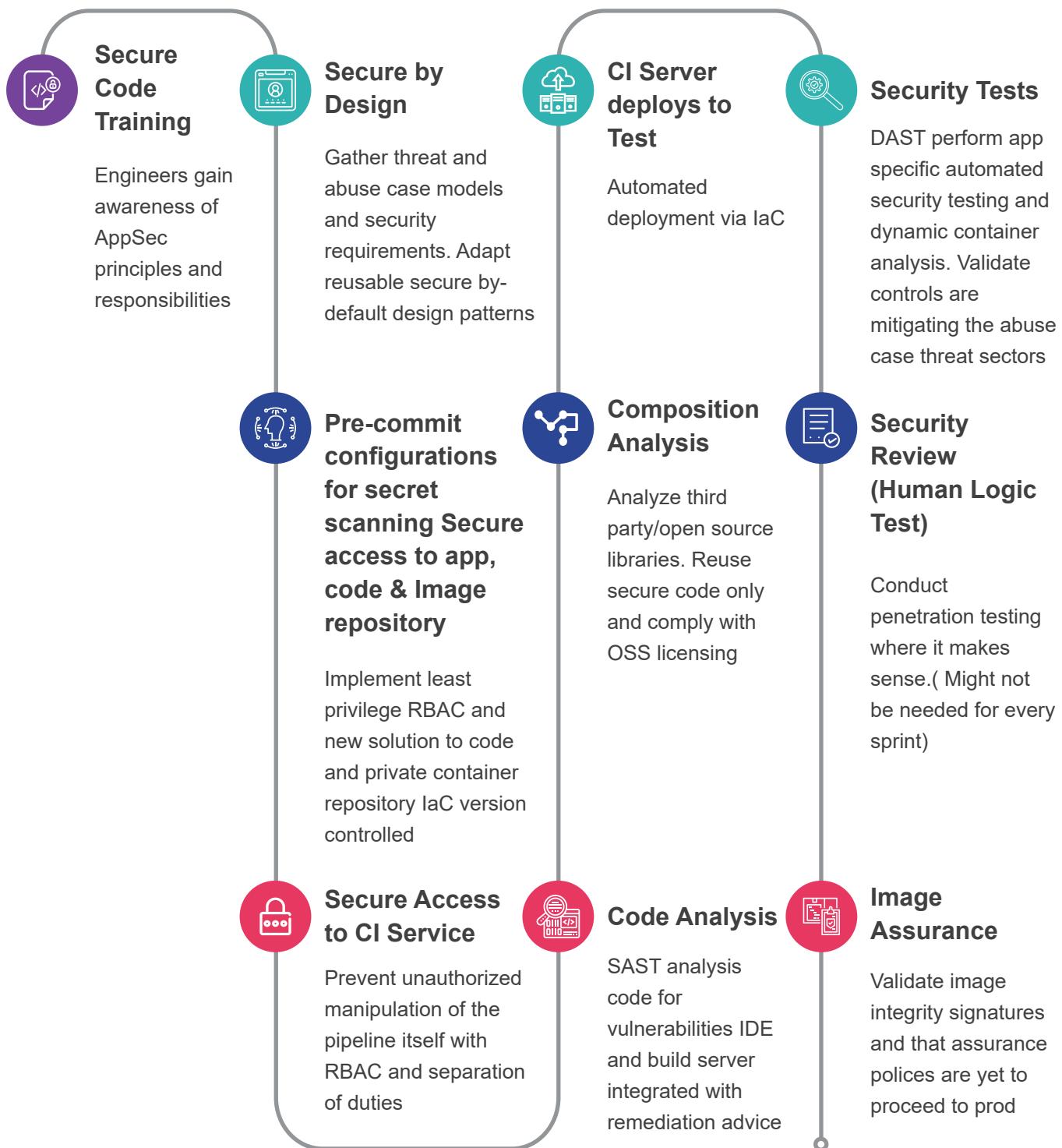




Implementing an end-to-end DevSecOps pipeline is critical to building a successful software delivery, which includes continuous integration (CI), continuous delivery and development (CD), continuous testing, logging and monitoring, auditing and governance, and operations. As DevSecOps breaks down the software development cycle into

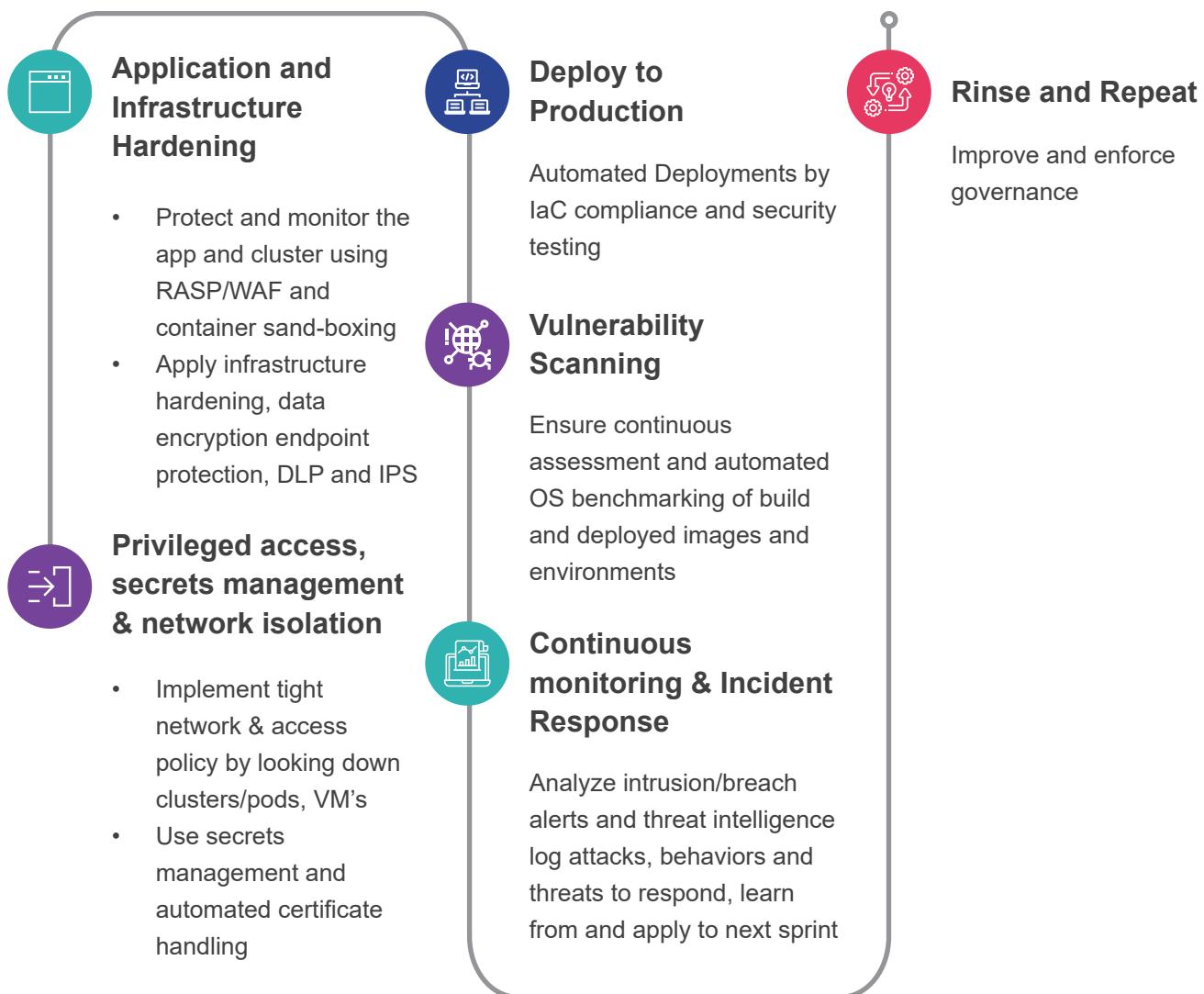
smaller pieces, identifying the vulnerabilities in the initial stages of the development process will help reduce costs and the automation aspect of the process will accelerate the delivery as well.

The below infographic shows the process carried out during the development phase of DevSecOps security controls.





As we move to the production phase, here are a few things that the development teams must keep in mind:





Chapter 4

AWS CI/CD and Support Tools

DEV∞OPS



In this chapter, we discuss the various AWS services and third-party support tools used in this solution.

As far as CI/CD is concerned, we leverage the following AWS services.

AWS CodeBuild	A fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy.
AWS Code Commit	A fully managed source control service that hosts secure Git-based repositories.
AWS Code Deploy	A fully managed deployment service that automates software deployments to a variety of compute services such as Amazon Elastic Compute Cloud (Amazon EC2), AWS Fargate , AWS Lambda , and your on-premises servers.
AWS Code Pipeline	A fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.
AWS Lambda	A service that lets you run code without provisioning or managing servers. You pay only for the compute time you consume.
Amazon Simple Notification Service	Amazon SNS is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication.
Amazon S3	Amazon S3 is storage for the internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web.
AWS Systems Manager Parameter Store	Parameter Store provides secure, hierarchical storage for configuration data management and secrets management.



Chapter 5

Open Source/AWS Continuous Testing Tools

DEV ∞ OPS

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5**
- Chapter 6
- Chapter 7
- Chapter 8

Listed below is the open-source scanning tools available in AWS that are integrated in the pipeline. You could also opt for different tools based on your business requirements. For example, most businesses use the static code review tool **Amazon CodeGuru** for static analysis.

Amazon CodeGuru	Amazon Elastic Container Registry image scanning	Git-Secrets (Secrets Scanning)
For static analysis	Amazon ECR image scanning helps in identifying software vulnerabilities in your container images. Amazon ECR uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project and provides a list of scan findings.	Prevents you from committing sensitive information to Git repositories. It is an open-source tool from AWS Labs.
OWASP ZAP (DAST)	Anchore (SCA and SAST)	Sysdig Falco (RASP)
Helps you automatically find security vulnerabilities in your web applications while you're developing and testing your applications.	Anchore Engine is an open-source software system that provides a centralized service for analyzing container images, scanning for security vulnerabilities, and enforcing deployment policies.	Falco is an open source cloud-native runtime security project that detects unexpected application behavior and alerts on threats at runtime. It is the first runtime security project to join CNCF as an incubation-level project.



Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 6

AWS Security, Identity, and Compliance Service

AWS' security, identity, and compliance services are categorized based on 4 function types:

Authorization

Protected Store

Visibility

Enforcement

Each of these functions has at least 2-3 AWS tools that may suit your business requirements.

Authorization



IAM



AWS RAM



AWS Organizations

Protected Store



AWS CloudHSM



AWS KMS



AWS Secrets Manager



AWS Certificate Manager

Visibility



AWS Artifact



AWS Security Hub

Enforcement



Amazon GuardDuty



Amazon Inspector



Amazon Macie



AWS WAF



AWS Shield



Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

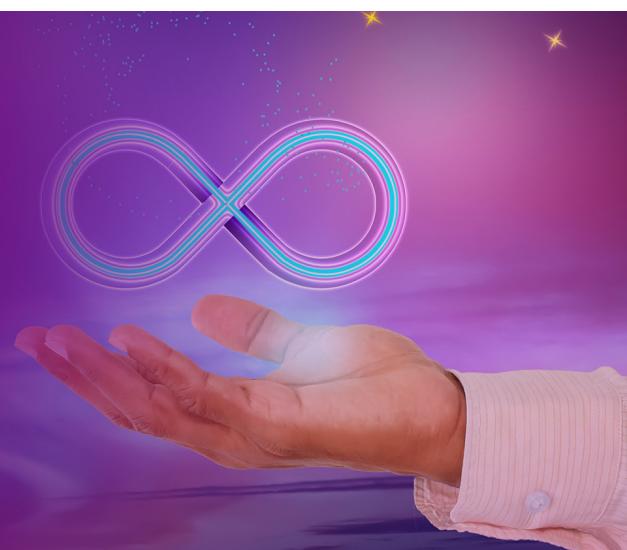
Chapter 6

Chapter 7

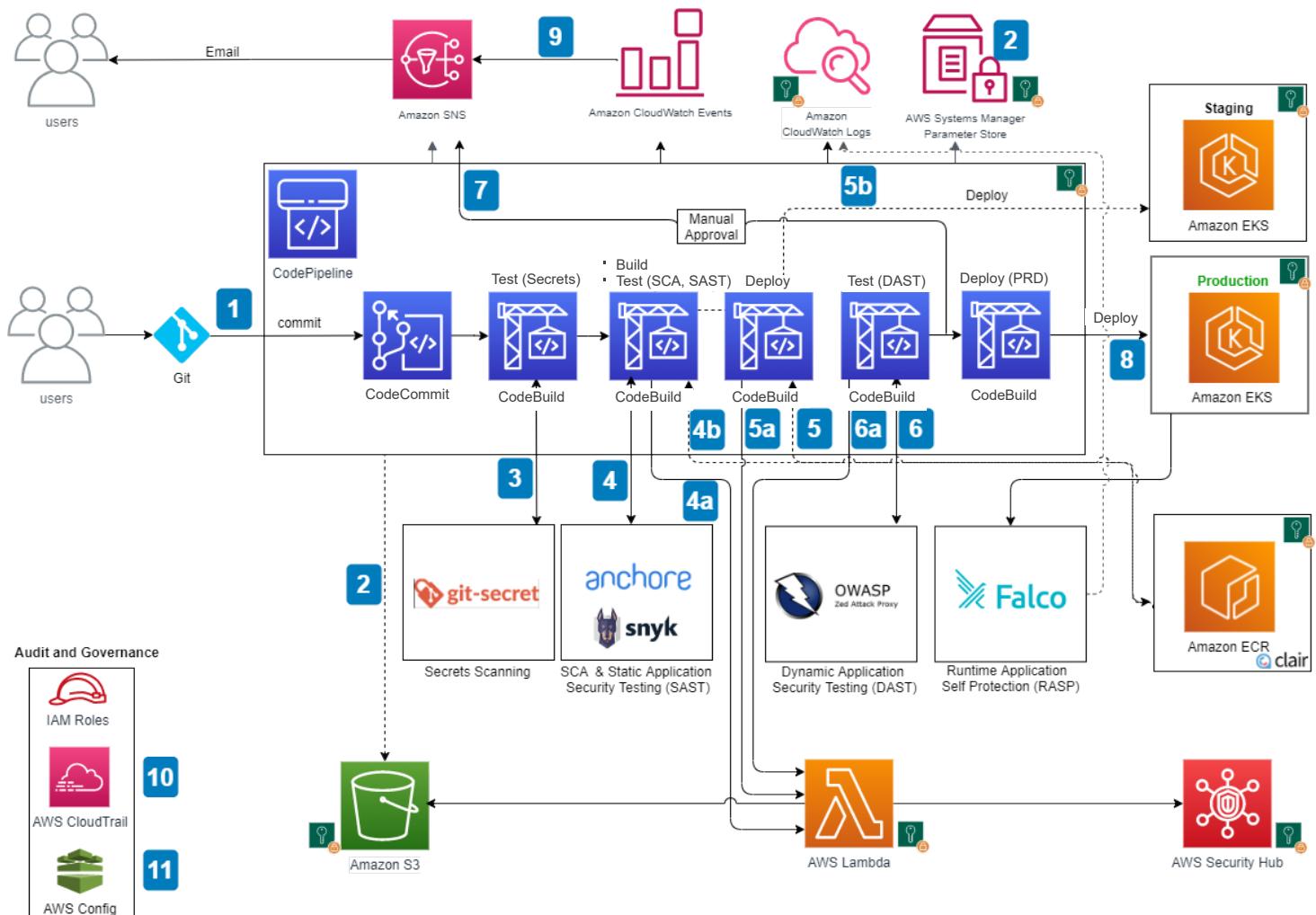
Chapter 8

Chapter 7

DevSecOps Reference Architecture



The following diagram represents the DevSecOps reference architecture on AWS that covers the aforementioned practices, services, and support tools.





Listed below is the chronological sequence of events that are carried out on your AWS cloud.

1. When a user writes the code to a CodeCommit repository, a CloudWatch event is generated, triggering a CodePipeline.
2. CodeBuild packages it and sends the artifacts to an S3 bucket. It retrieves the authentication data from the Parameter Store to kickstart the scanning. As a best practice, we advise you to use AWS CodeArtifact to store the artifacts.
3. While CodeBuild scans the code with an SCA tool (OWASP Dependency-Check) and SAST tool, you can pick one of these during the deployment.
4. If there are any vulnerabilities found from these tools, CodeBuild invokes the Lambda function. The Lambda function converts the results into AWS Security Finding Format (ASFF) and posts them on Security Hub. Security Hub aggregates the findings in a single repository and the Lambda function also uploads the same into an S3 bucket.
5. CodeDeploy deploys the code to the Elastic Beanstalk environment in case of no vulnerabilities.
6. Once the deployment succeeds, CodeBuild triggers the DAST scanning with the OWASP ZAP tool.
7. If there are any vulnerabilities, step 4 is followed again.
8. In case of no vulnerabilities, the approval stage is ready and an email is dispatched to the approver for action.
9. Once approved, CodeDeploy deploys the code to the Beanstalk environment.

10. During the pipeline run, CloudWatch Events records the build state changes and sends out email notifications to all the subscribers through SNS notifications.
11. CloudTrail tracks the API calls and sends notifications on critical events happening on the pipeline.
12. Finally, AWS Config keeps track of all the configuration changes of AWS services.

Security in the pipeline is implemented by using IAM roles and S3 bucket policies with SCA, SAST, and DAST security checks.

As a best practice, encryptions must be enabled for code and artifacts, irrespective of whether at rest or transit.





Chapter 8

Conclusion

DevOps is a commendable approach if you are looking to improve software engineering and maintenance processes. However, companies can only achieve maximum advantage if security is integrated into your DevOps practices.

Organizations that have implemented DevSecOps have enjoyed enhanced automation throughout the software delivery pipeline, thereby eliminating cyber-attacks and ensuring pro-active security.

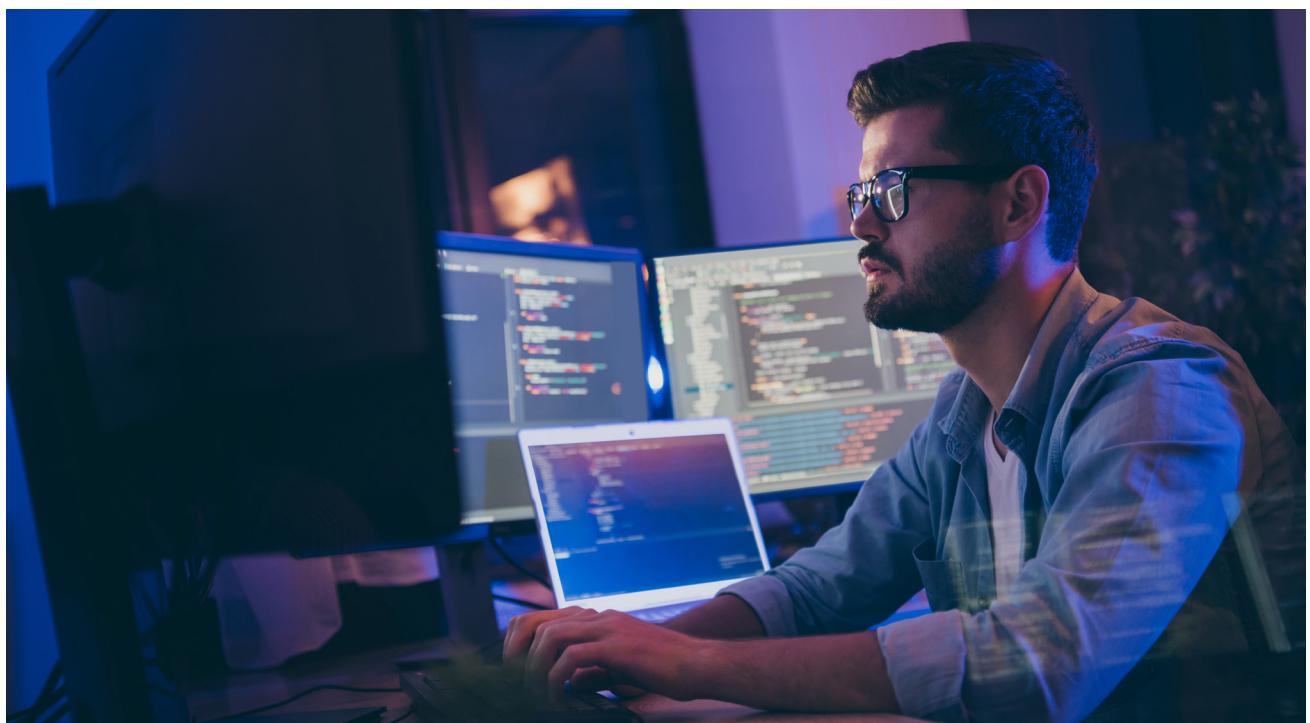
So, why engross your cloud security teams with

Dev Ops

cyber-attacks and ticket resolutions when you have DevSecOps in the fore?

Schedule a free consultation with our experts to get started.

Watch our latest webinar to know how integrating security into your DevOps framework tightens your AWS Cloud security. Adopting DevSecOps will help your security teams focus on other value-added activities.





About Aspire Systems

- Global technology services firm with core DNA of Software Engineering
- Specific areas of expertise around Software Engineering, Digital Services,
- Testing, and Infrastructure & Application Support
- The vertical focus among Independent Software Vendors, Retail, Distribution & Consumer Products and BFSI
- 3000+ employees; 150+ active customers
- Oracle Global Platinum Partnership with OCI & R12.2.9, Domain Expertise
- Well Rounded Team covering Cloud Architects, Solution Experts & Application
- Consultants
- CMMI Maturity Level 3, ISO 9001:2015, and ISO 27001: 2013 certified
- International headquarters in Singapore with presence across US, Mexico, UK, The Netherlands, Poland, Middle East, and India
- Recognized 11 consecutive times as "Best Place to Work for" by GPW Institute

Contact Us

For more info contact: info@aspiresys.com or visit www.aspiresys.com

NORTH AMERICA

+1 630 368 0970

POLAND

+48 58 732 77 71

INDIA

+91 44 6740 4000

MIDDLE EAST

+971 50 658 8831

NETHERLANDS

+31 (0)30 800 92 16

UNITED KINGDOM

+44 203 170 6115

SINGAPORE

+65 3163 3050

MEXICO

+52 222 980 0115