aws SUMMIT

INDIA | MAY 25, 2023

GSAWS006

Shifting security to left of CI/CD pipeline

Sathish Kumar Prabakaran
Enterprise Solutions Architect
AWS India

Upendra V
Enterprise Solutions Architect
AWS India

Agenda

- What is DevSecOps
- Pipeline Security
- DevSecOps on AWS
- Demo

What is DevSecOps

Evolve faster than ever

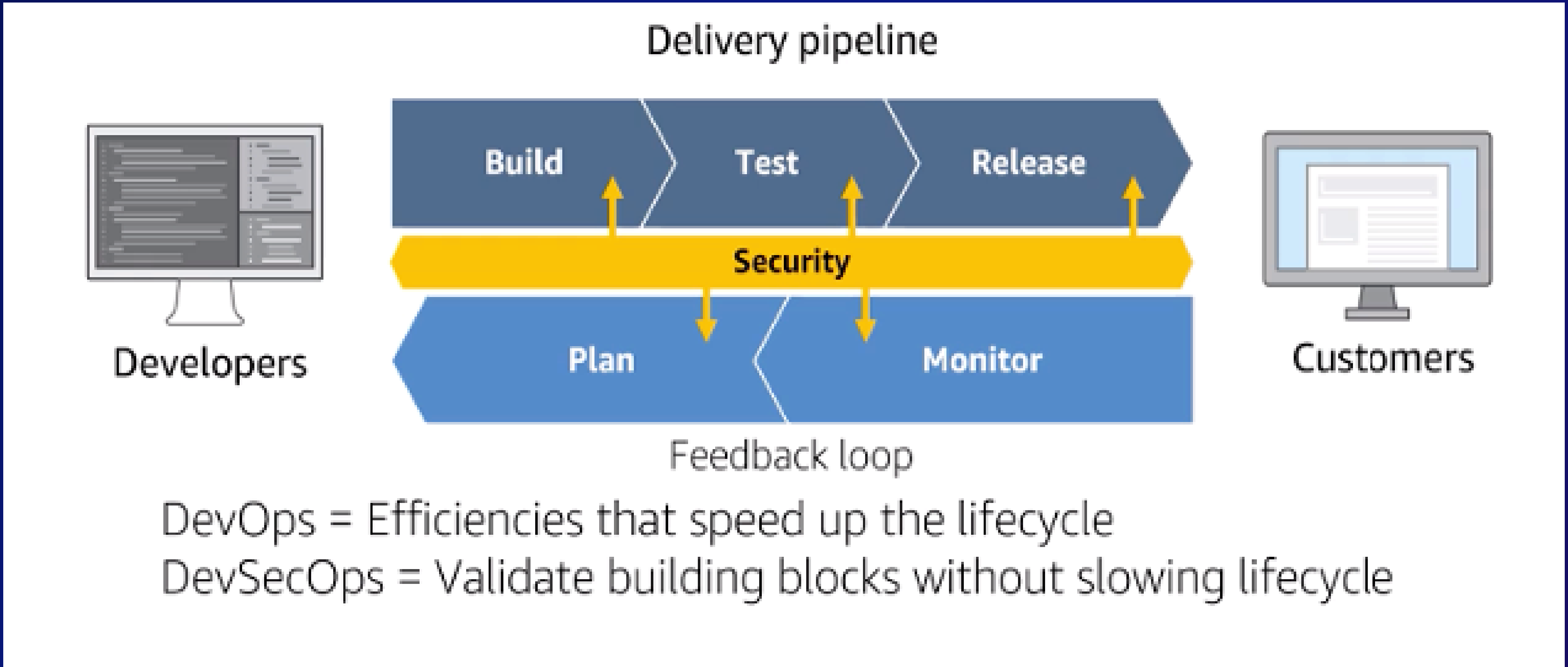
Customers are having to evolve faster than ever

IRRESPECTIVE OF THE INDUSTRY

- PUBLIC SECTOR
- FINANCIAL SERVICES
- HEALTHCARE & PHARMA
- RETAIL
- SUPPLY CHAIN

Billions of cell phones. Pervasive cloud computing. 20 million software developers. Increased automation.

DevOps vs DevSecOps

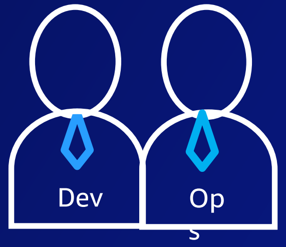


DevOps = Efficiencies that speed up the lifecycle

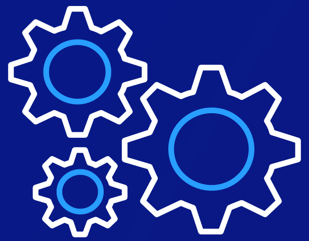
DevSecOps = Validate building blocks without slowing lifecycle

How to implement DevSecOps?

DevSecOps is achieved by integrating and automating the enforcement of preventive, detective, and responsive security controls into the pipeline.

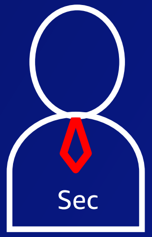


Collaboration



Automation

Speed



Tenets of DevSecOps

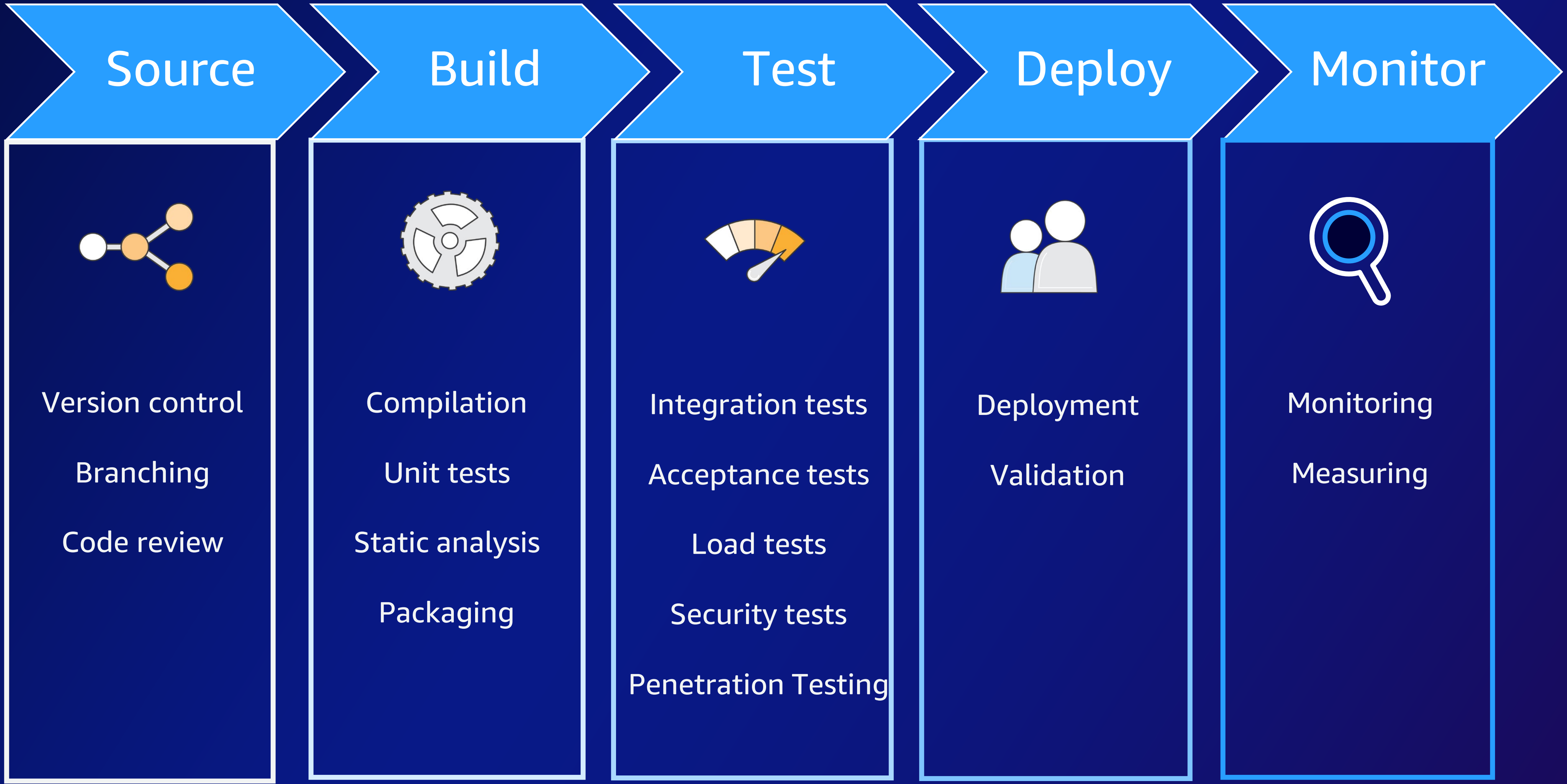
1. Test security as early as possible to accelerate feedback

2. Prioritize preventive security controls

3. Identify and document responses on security incidents

4. Automate, automate, automate

Continuous Integration and Continuous Delivery (CICD)



Source

Version control

Branching

Code review

Build

Compilation

Unit tests

Static analysis

Packaging

Test

Integration tests

Acceptance tests

Load tests

Security tests

Penetration Testing

Deploy

Deployment

Validation

Monitor

Monitoring

Measuring

Pipeline Security

Three major components of DevSecOps

Security of the pipeline

Security in the pipeline

Enforcement of the pipeline

Security of the pipeline

Identity and access management

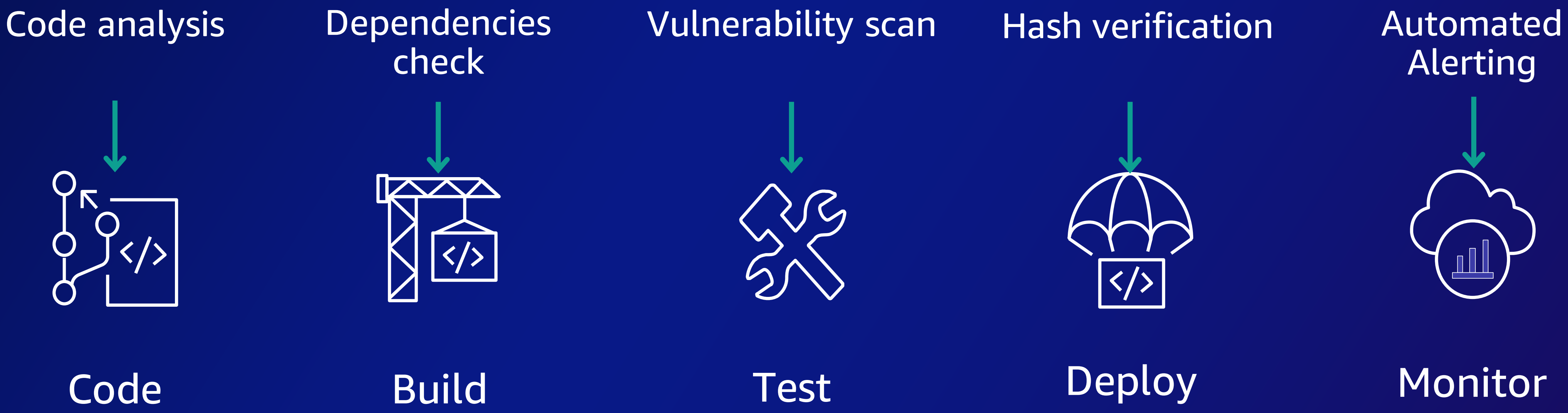
Detective controls

Infrastructure controls

Data protection

Incident response

Security in the pipeline



Code analysis

Code

Dependencies check

Build

Vulnerability scan

Test

Hash verification

Deploy

Automated Alerting

Monitor

Security in the pipeline

1. Protect Sensitive Information
   - Keep passwords and keys out of code/pipeline

2. Software Composite Analysis (SCA)
   - Third party library review
   - Re-use previously vetted/approved code whenever possible

3. Static Application Security Testing (SAST)
   - Review code for vulnerabilities

Security in the pipeline

4. Dynamic Application Security Testing (DAST)
    - Dynamically exercise the application to discover vulnerabilities

5. Interactive Application Security Testing (IAST)
    - Agent based real-time analysis

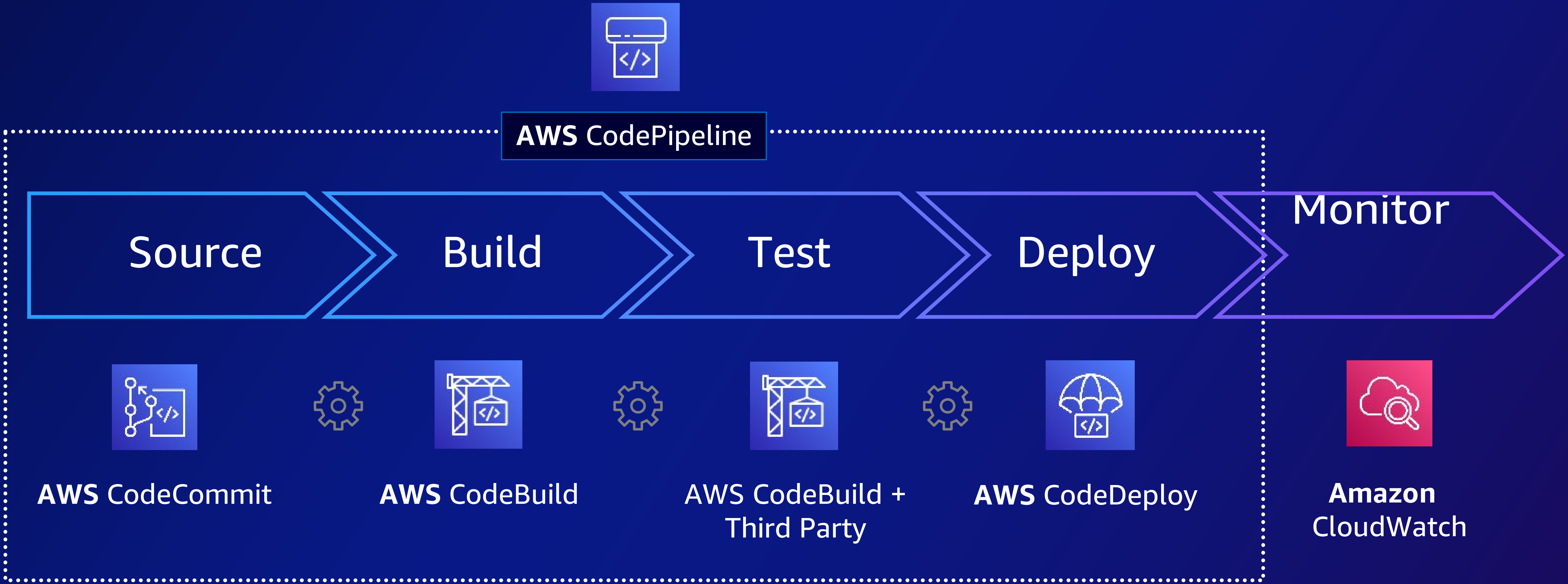
6. Runtime Application Self Protection (RASP)
    - Agent based real-time remediation of security events

Concepts to enforce the pipeline

- Establish environments on separate AWS accounts (e.g. Sandbox, Dev, Test, Prod)
- Humans should have increasingly fewer rights as you progress through environments
- Only the pipeline should be able to “make changes” to Prod. Manual checkpoints to review the test results before pipeline pushes the code to production.

DevSecOps on AWS

AWS Security of the Pipeline on AWS



AWS CodePipeline

Source

Build

Test

Deploy

Monitor

AWS CodeCommit

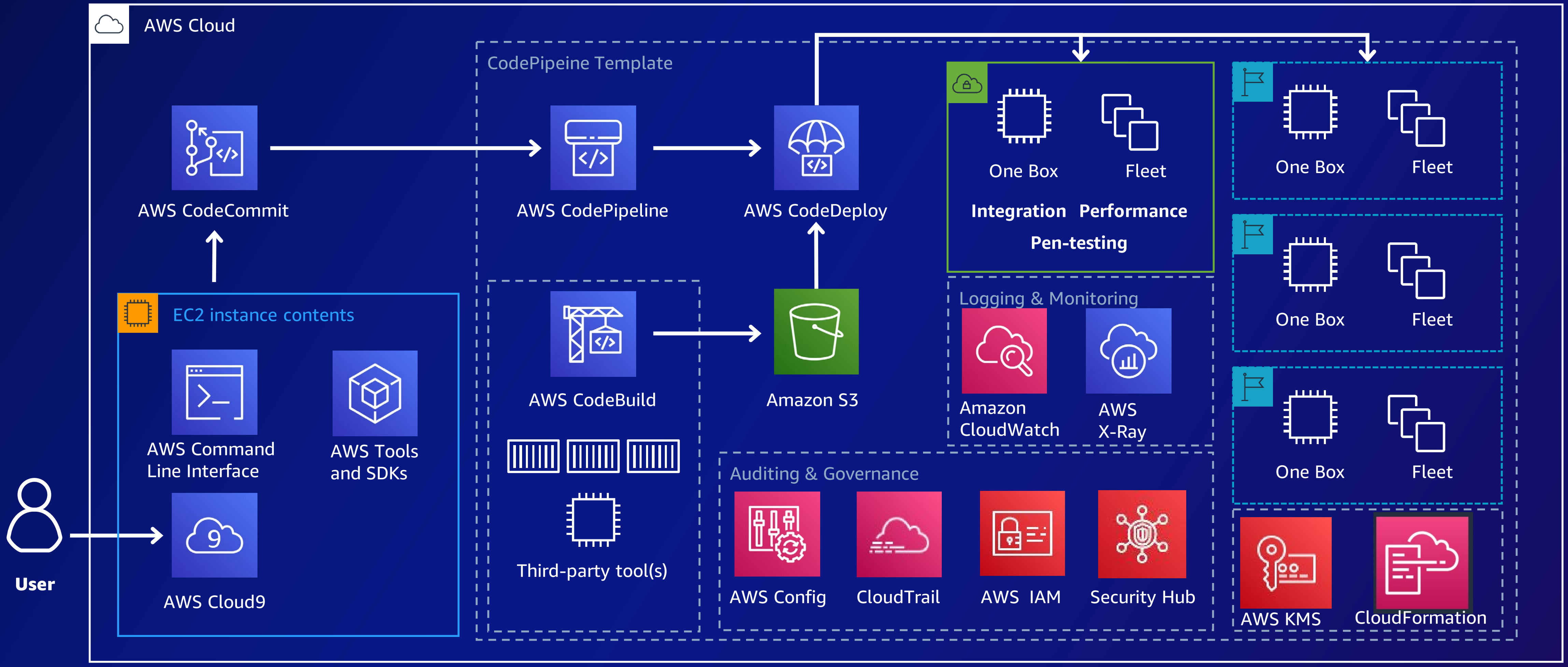
AWS CodeBuild

AWS CodeBuild + Third Party

AWS CodeDeploy

Amazon CloudWatch

DevSecOps – AWS Service Integration



Key Takeaways

- Use Amazon Inspector to manage your build and deploy pipelines services
- Building an end-to-end Kubernetes-based DevSecOps software factory on AWS
- Building end-to-end AWS DevSecOps CI/CD pipeline with open source SCA, SAST and DAST tools
- Integrating security into your container pipeline

Demo

skillbuilder.aws

Your time is now

Build in-demand cloud skills your way

Thank you!

Please complete the session survey

Sathish Kumar Prabakaran
Enterprise Solutions Architect
AWS India

Upendra V
Enterprise Solutions Architect
AWS India