AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC224

DevSecOps for containers

Scott Ward (he/him)
Principal Solutions Architect
AWS External Security Services

James Bland, Ph.D. (he/him)
Senior Solutions Architect
AWS Partner Network

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

High-level view of the problem

Zooming in on several phases

Q&A

Resources



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

View from 10 kilometers

Directive

- What are our security goals?
- For example, “All prod apps must deploy through an approved pipeline”

Preventative

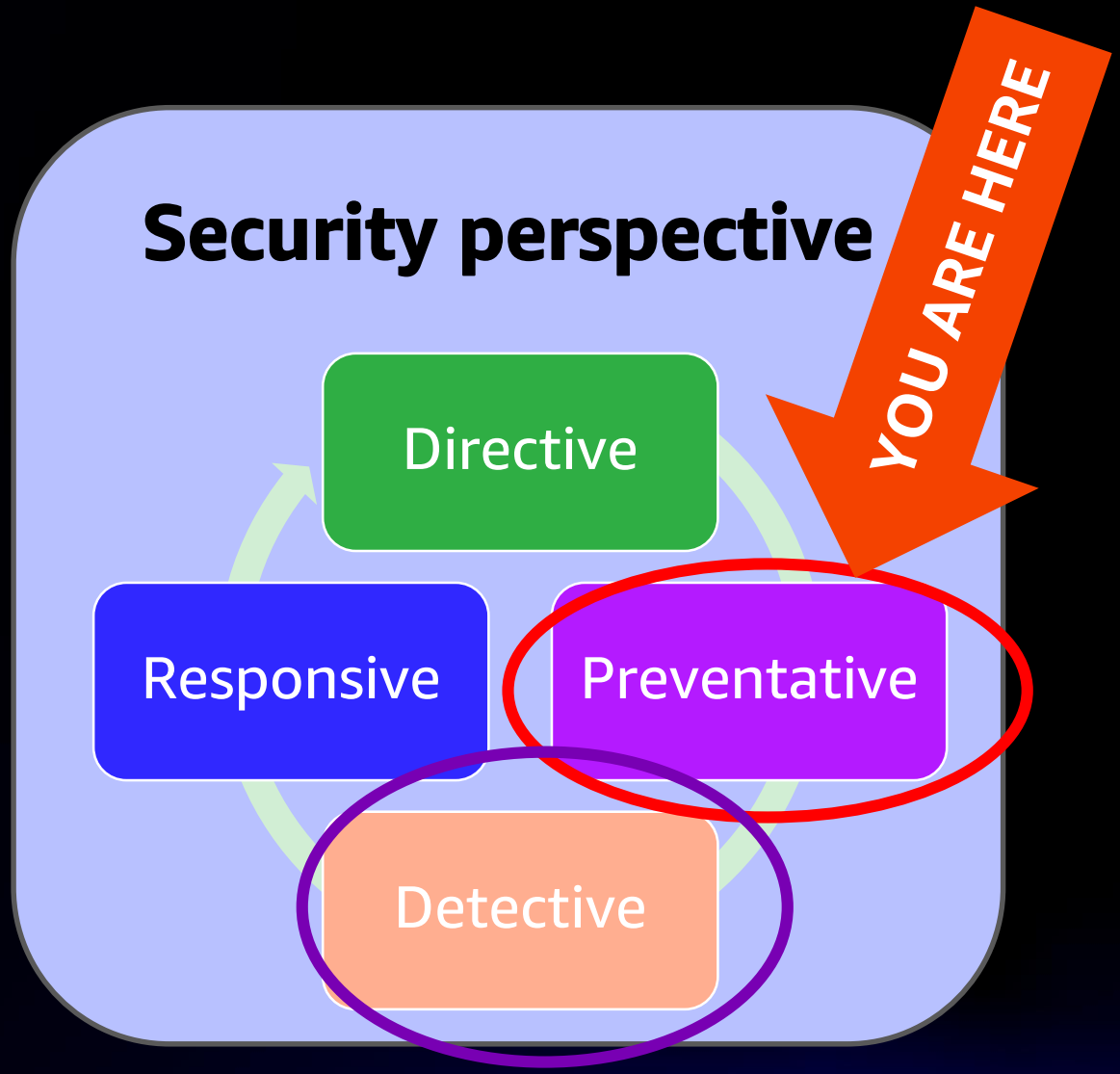
- Stop bad things from happening
- For example, “Code that has X errors may not deploy”

Detective

- Look for bad things happening anyway
- For example, scan what got deployed

Responsive

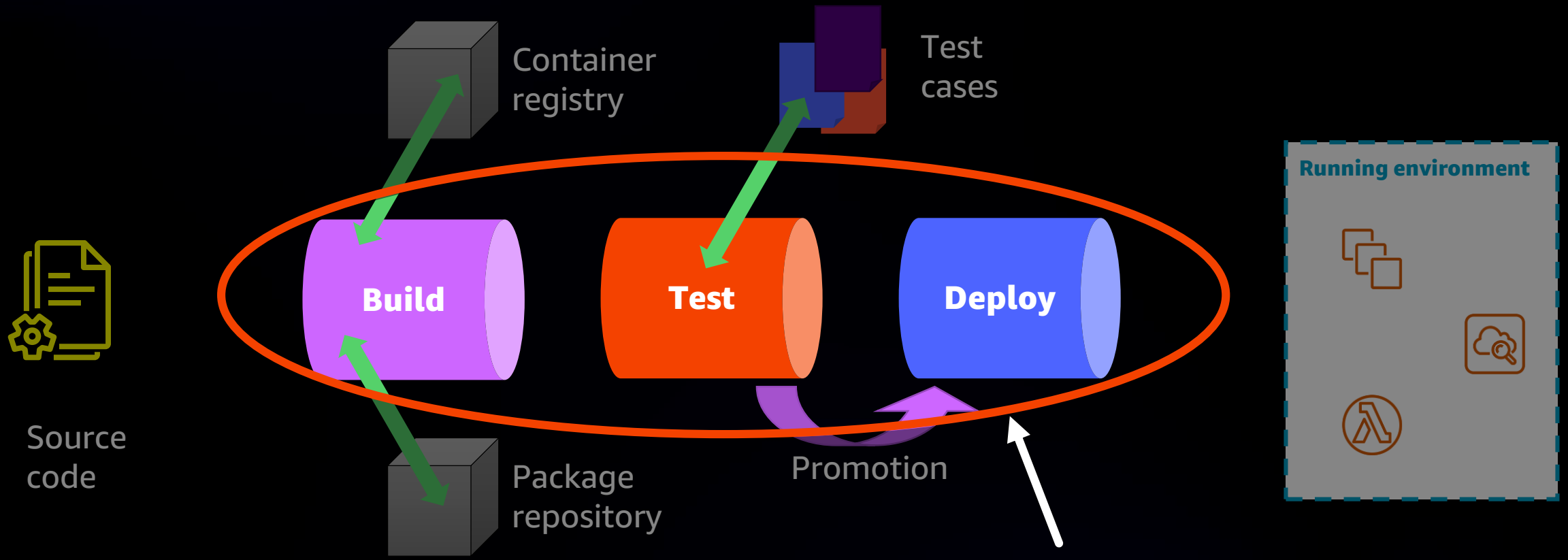
- Fix or alert on bad things detected
- Out of scope for this session



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

View from 1 kilometer

Security **in** the pipeline
Security **of** the pipeline
Security **through** the pipeline



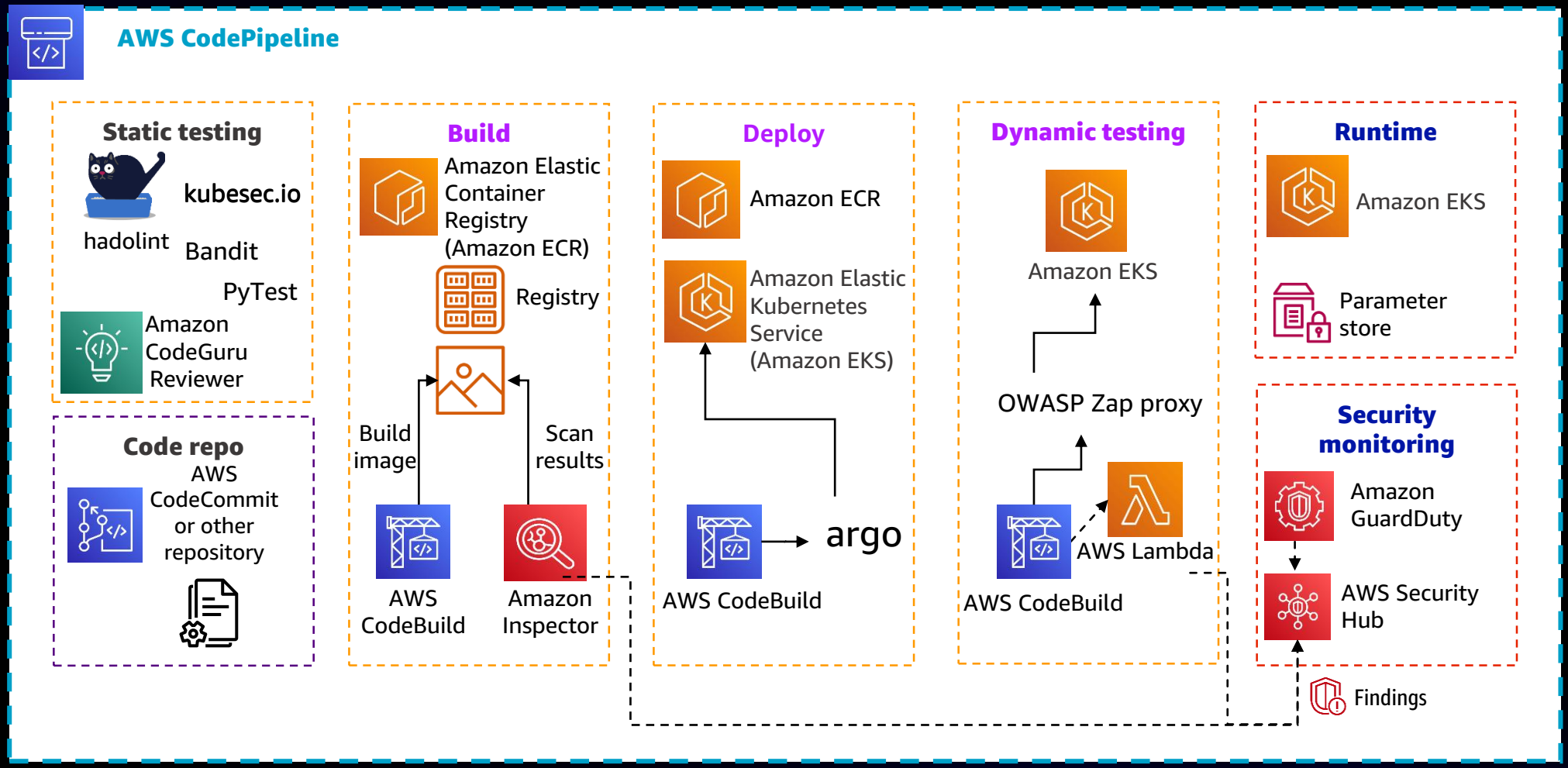
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

View from 1 meter

This is just an example

Kubernetes (could use Docker and/or Amazon ECS)

Python/ AWS Lambda Serverless (could be any language)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

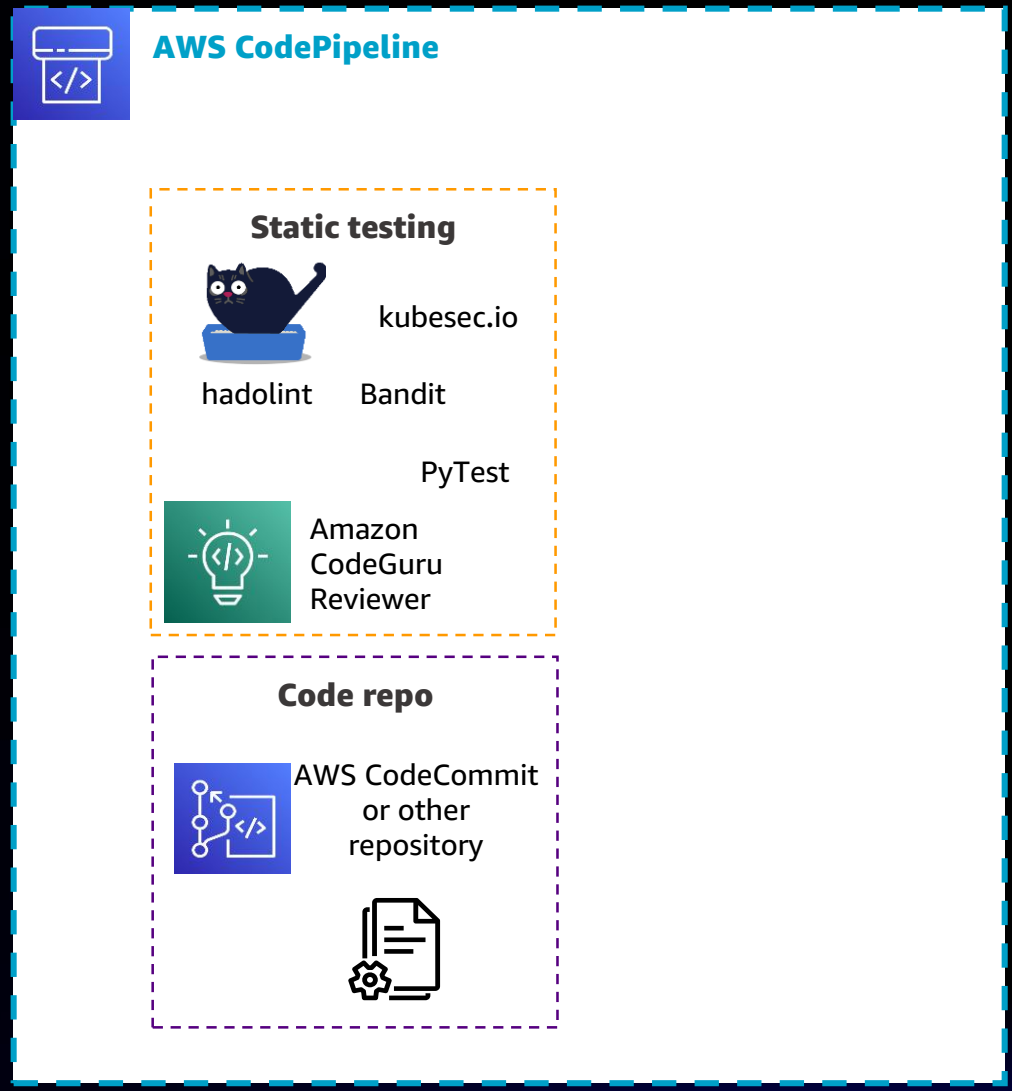
Code phase

Cloud-specific:

- Scan for obviously bad resources (ACK/Crossplane)
  - Public buckets
  - Permissive IAM policies
  - Permissive security groups
- AWS CloudFormation/AWS CDK
  - cfn-nag
  - cfn-guard
  - cdk-guard

Standard security:

- Scan for secrets
- Scan for language-specific issues
- Amazon CodeGuru
- Spotbugs
- Scan for Dockerfile best practices
- FOSSA
- Fortify/SonarQube/and so on



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build phase

Check for known issues in all the layers of your image:

- OS packages
- Libraries
- Files

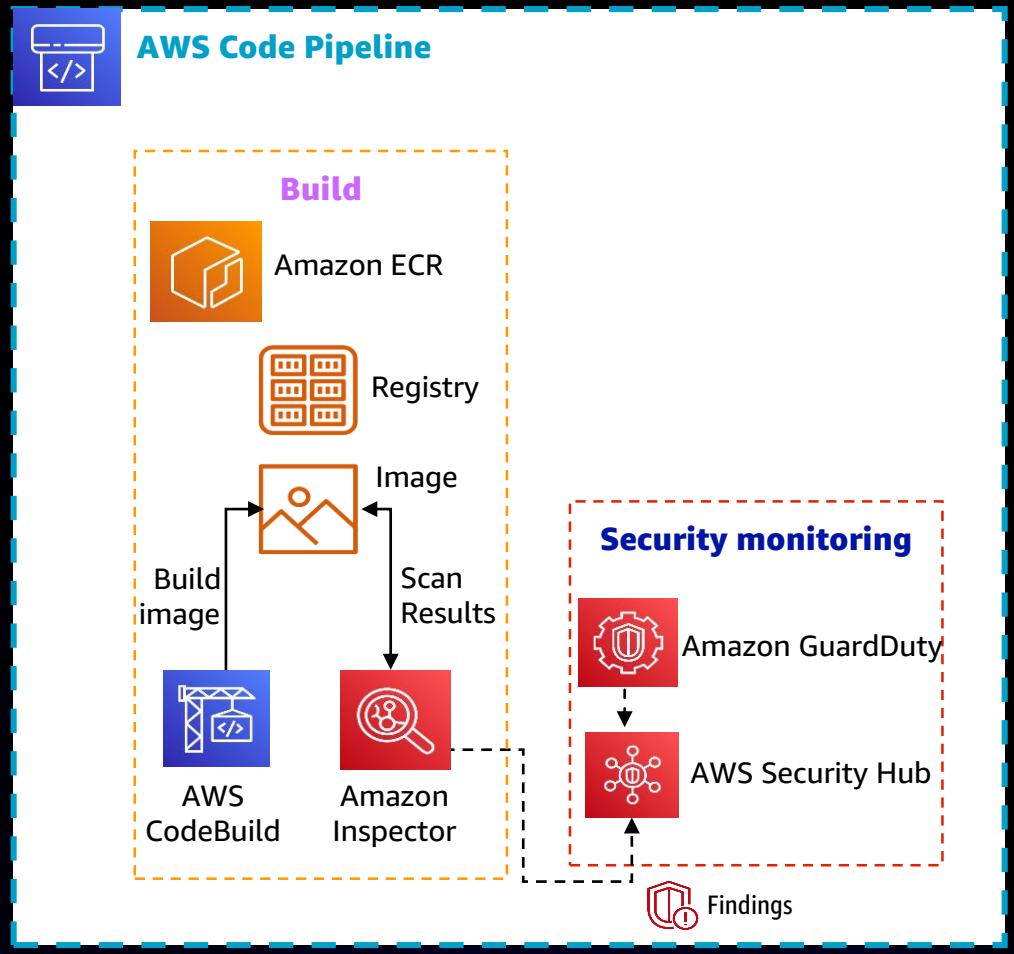
Tools:

- Amazon Elastic Container Registry
- Amazon Inspector
- Clair
- Anchore
- Snyk

New

Amazon Inspector

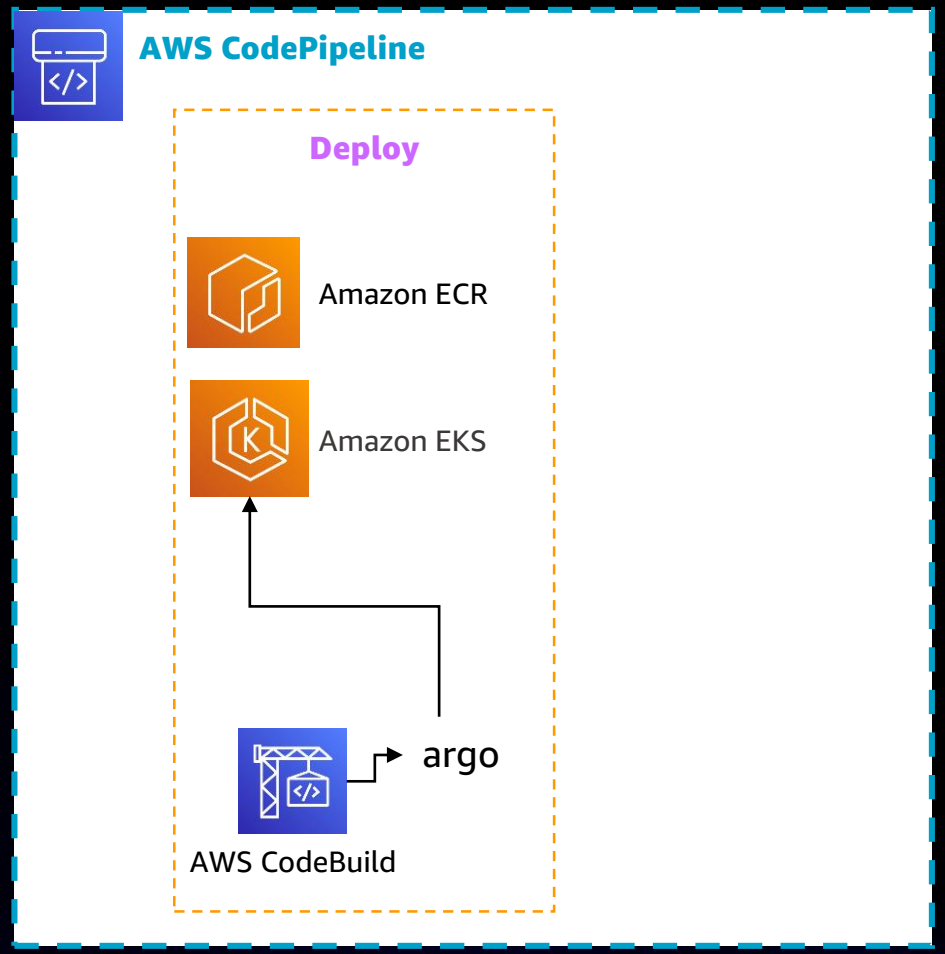
Now with the ability to scan container images for vulnerabilities



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Staging deploy phase

Deploy to staging cluster for additional testing



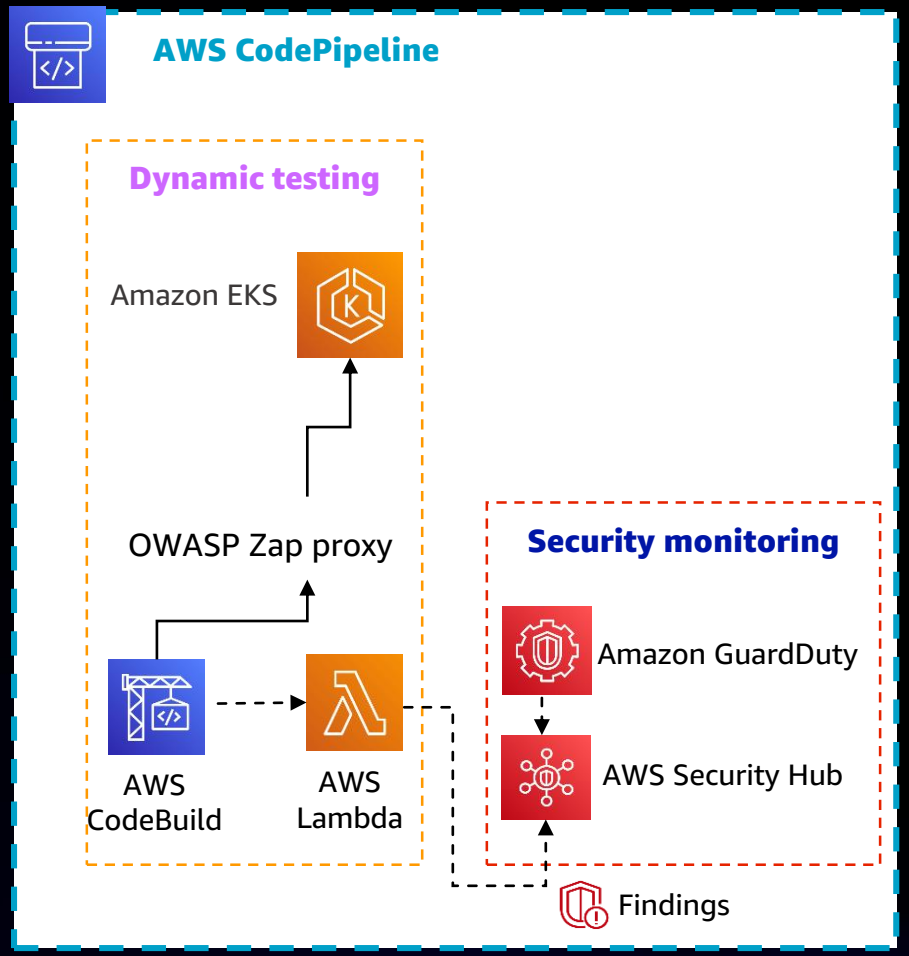
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dynamic test phase

Check for problems you can only see at runtime

Operating system:
- Misconfiguration
- Vulnerable packages
- Listening services
- TLS certificates (or lack of)

Application software:
- Response times/error 500
- SQL injection, XSS, OWASP-type app vulnerabilities
- Information disclosure (HTTP headers, software version information)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Runtime monitoring/management

Not really today's focus, but some quick points

- AWS Security Hub
- Amazon GuardDuty
- AWS CloudTrail
- AWS Config/AWS Config rules

- Cloud Custodian
- Prowler
- ScoutSuite



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

- Hadolint: Haskell Dockerfile linter
- Kubesec.io: Security risk analysis for Kubernetes resources
- Bandit: Python code security scanner
- Anchore: Open-source software for analyzing container images, scanning for security vulnerabilities, and enforcing deployment policies
- Git-secrets: Git commit hook that looks for committed AWS secrets
- Snyk: Commercial tool scanning software dependencies
- Sysdig Falco: Open-source cloud-native runtime security project that detects unexpected application behaviour and alerts on threats at runtime

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Valuable resources

- Building an end-to-end Kubernetes-based DevSecOps software factory on AWS https://aws.amazon.com/blogs/devops/building-an-end-to-end-kubernetes-based-devsecops-software-factory-on-aws/
- Implementing runtime security in Amazon EKS using CNCF Falco https://aws.amazon.com/blogs/containers/implementing-runtime-security-in-amazon-eks-using-cncf-falco/
- Integrating AWS Secrets Manager secrets with Kubernetes Secrets Store CSI Driver https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_csi_driver.html
- Native container image scanning in Amazon ECR (including scheduled rescans strategy) https://aws.amazon.com/blogs/containers/amazon-ecr-native-container-image-scanning/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Scott Ward
scotward@amazon.com

James Bland, Ph.D.
jamband@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.