27TH MAY | 10am CEST

Free Virtual Event

DevSecCon

HUNGARY

Madhu Kumar Yeluri
Principal Cloud Architect
@ T-Systems International

Tales Casagrande
Snyk's Ambassador

DEUTSCHE TELEKOM IT SOLUTIONS

Questions?
Join the conversation on Discord
https://devseccon.io/discordcommunity

About the Speaker

Madhu is a qualified Principal Cloud Architect and DevOps Consultant with over 22 years of IT experience working across multiple regions, including Asia, the Middle East, the US, Europe, and the UK. He is helping many customers transform their businesses using the cloud. He is leading diverse teams to drive change and deliver business value at scale. AWS Community Builder, AWS User Group Leader and DevSecCon Chapter Leader for Hungary.

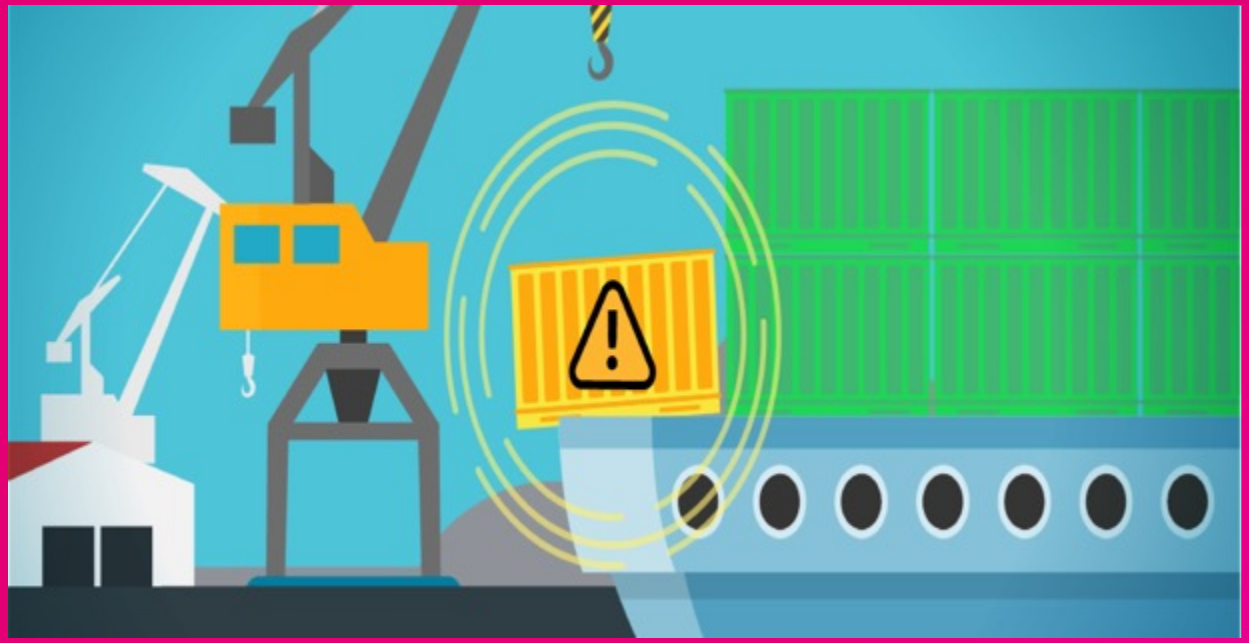
A certified Amazon Web Services (AWS) Solution Architect and Security Specialist. Product lead for container services (Docker, K8s, AWS ECS, and EKS). He has worked with many cloud partners and providers (AWS, Rackspace, Wipro, Google, Oracle, Azure, IBM, and Vodafone) and successfully managed and implemented multiple cloud migration projects replacing business-critical core legacy systems across the telecommunication, financial, banking, insurance, retail, and government sectors.

T · · Systems · Let's power higher performance

https://www.linkedin.com/in/cloudgeek7

DevSecCon HUNGARY

Container Security – Vulnerebilty Scanning



Madhu Kumar

27th May 2022

T · · Systems · Let's power higher performance

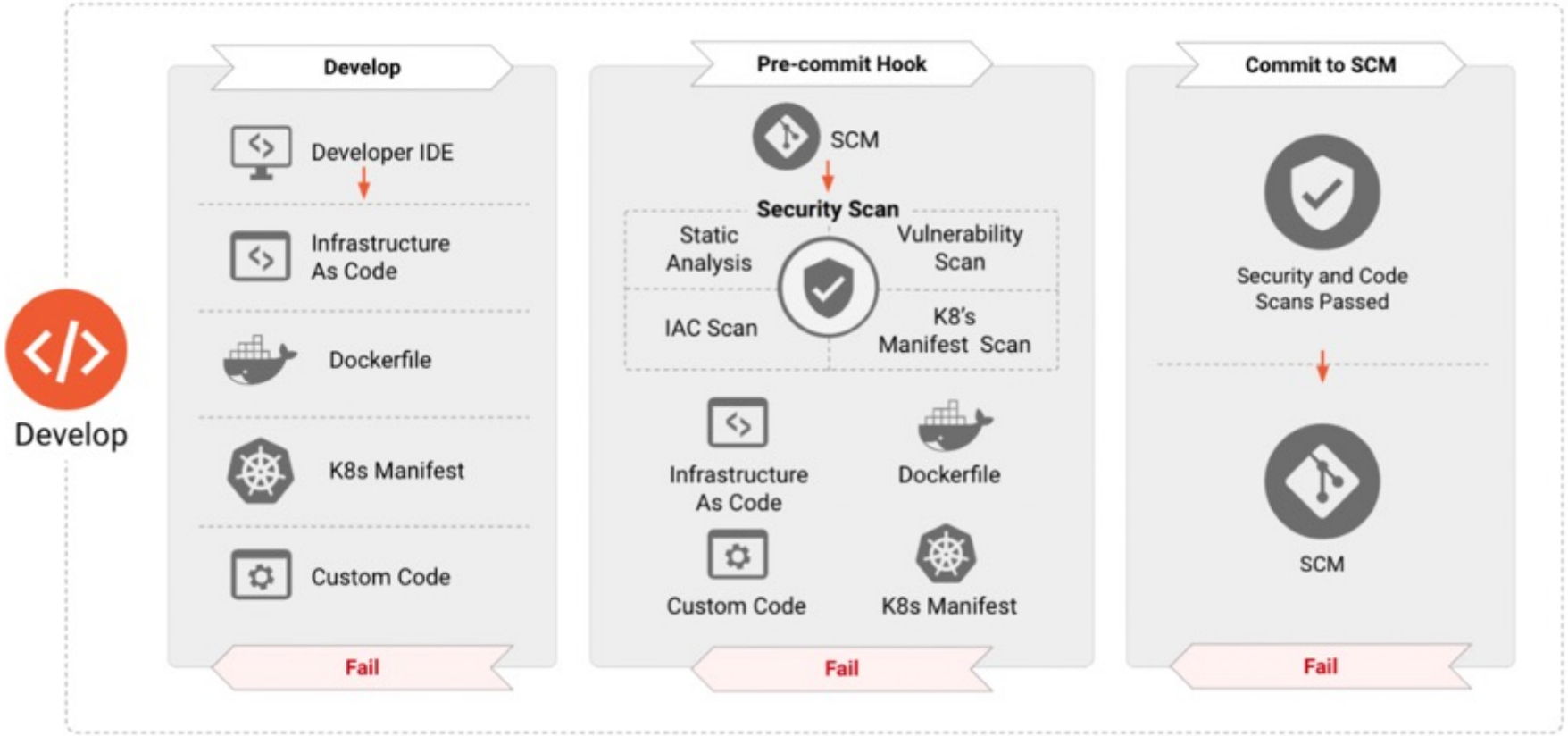
Agenda

- Cloud Native Security Whitepaper v2
- Integrate Security throughout the Application Lifecycle (Develop, Distribute, Deploy and Runtime)
- Dockerfile best practices
- Docker Bench for Security
- Kube Bench for Security
- DockerSlim for better, smaller and more secure images
- Vulnerability scanning for Docker images using AWS ECR, Trivy, Grype and docker scan (Snyk)
- AWS EKS Best Practices for Security
- EKS Responsibility Matrix
- Questions?

Cloud Native Security Whitepaper v2

Ref:
https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

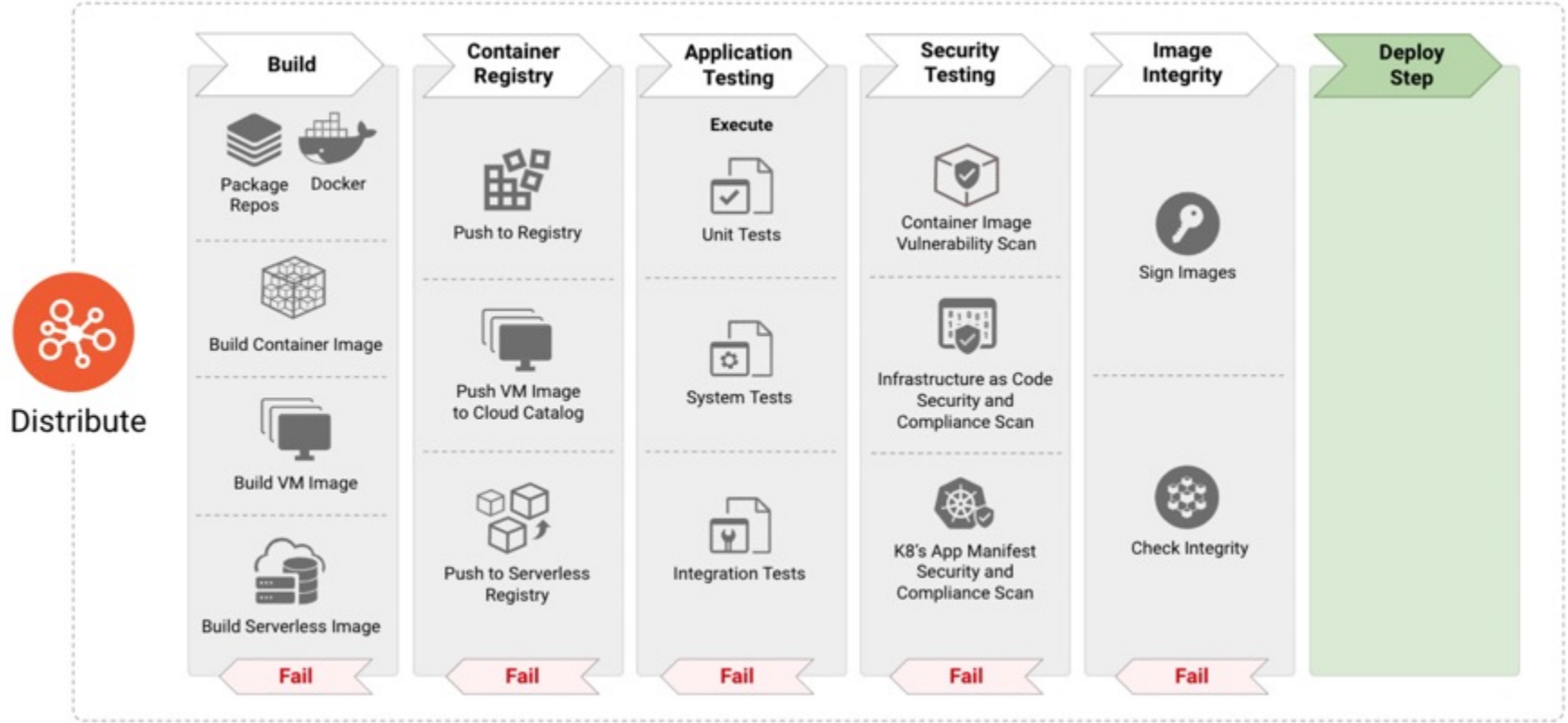
Integrate Security throughout the Application Lifecycle – Develop



Ref: https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/cloud-native-security-whitepaper.md

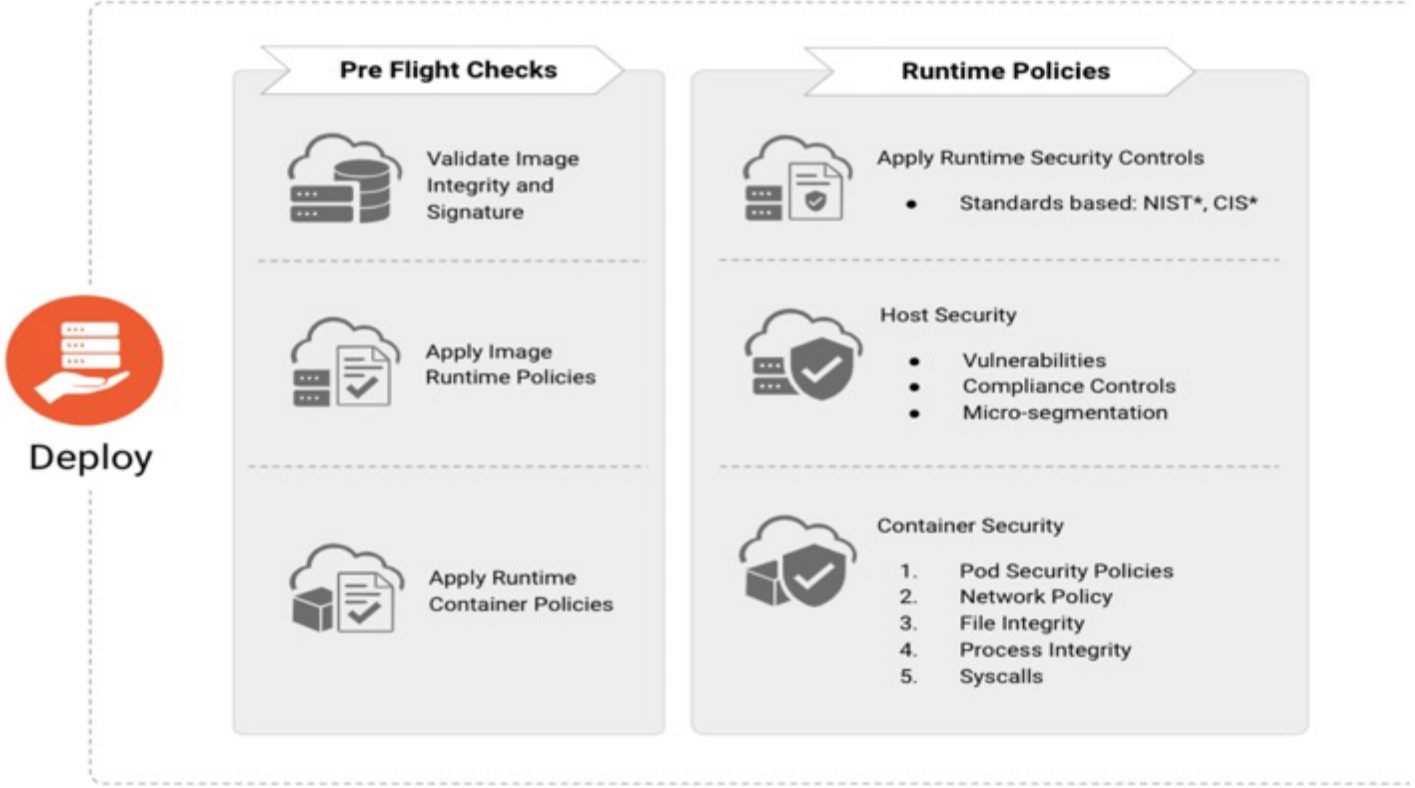
Integrate Security throughout the Application Lifecycle – Distribute

DevSecCon HUNGARY



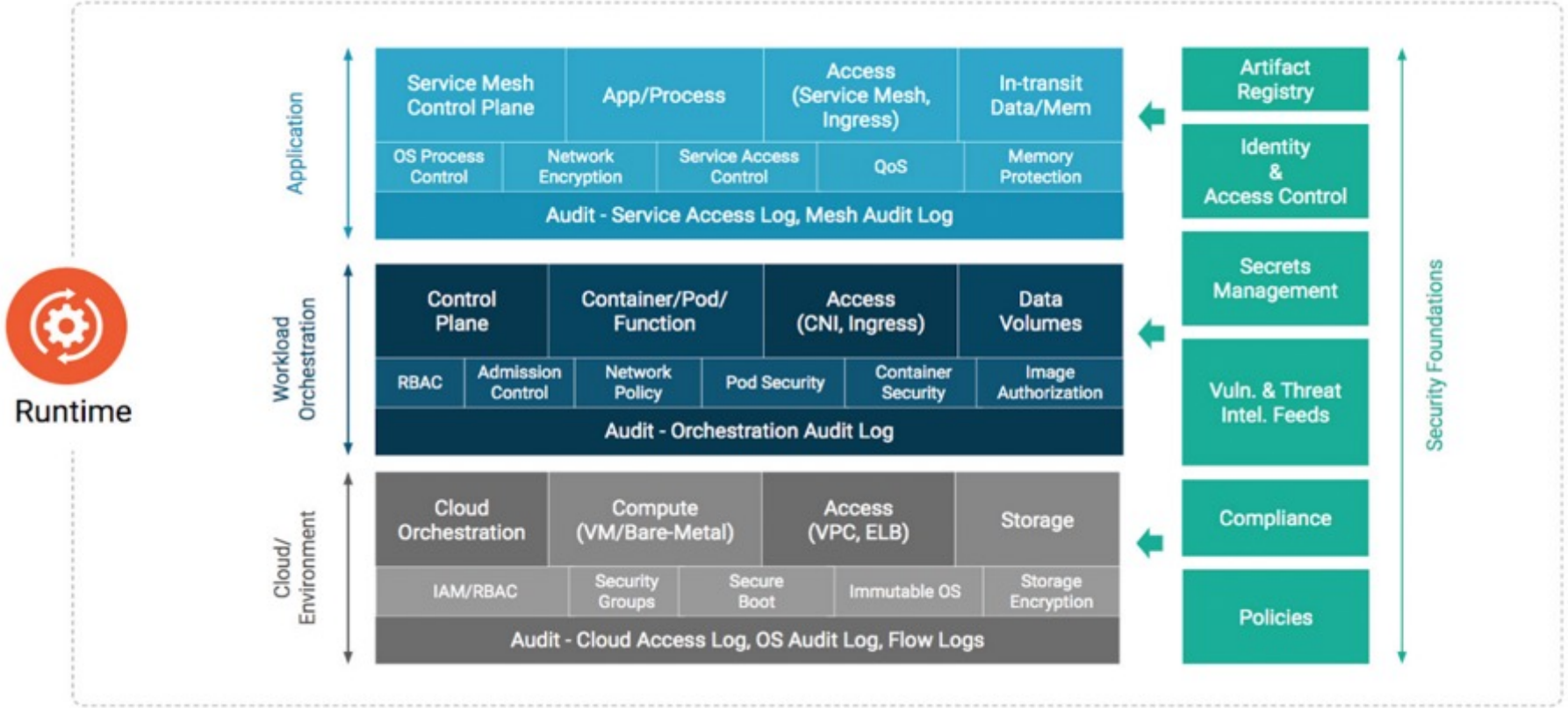
Ref: https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/cloud-native-security-whitepaper.md

Integrate Security throughout the Application Lifecycle – Deploy



Ref: https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/cloud-native-security-whitepaper.md

Integrate Security throughout the Application Lifecycle – Runtime



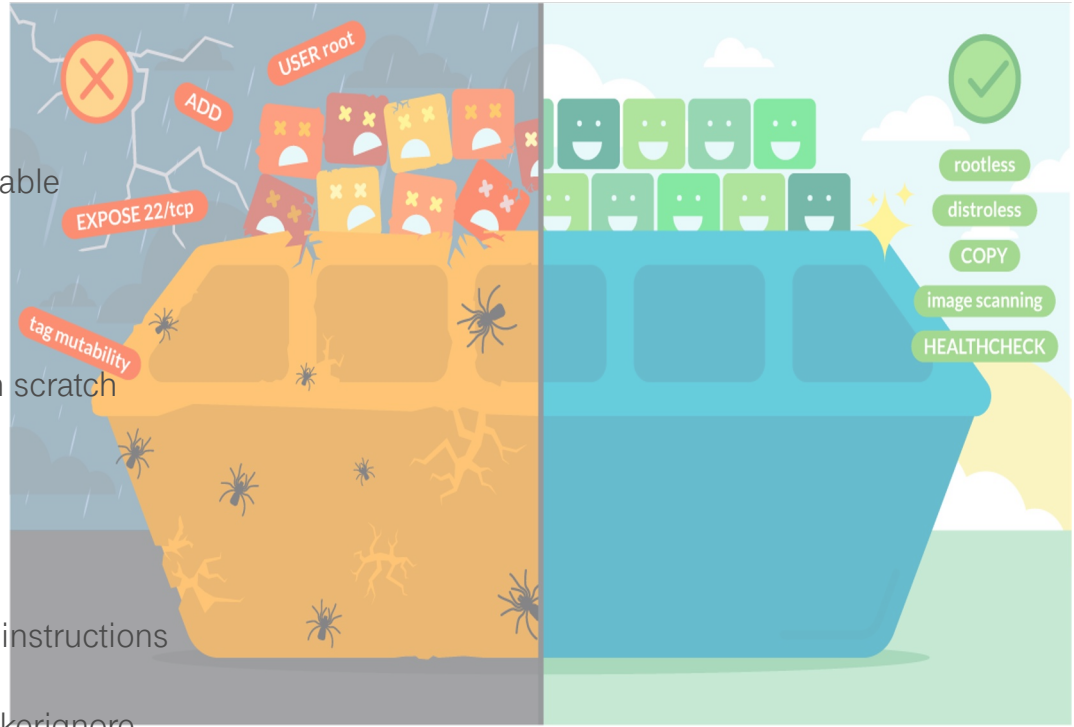
Ref: https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/cloud-native-security-whitepaper.md

Dockerfile best practices

1. **Avoid unnecessary privileges**
   1. Avoid running containers as root
   2. Don't bind to a specific UID
   3. Make executables owned by root and not writable

2. **Reduce attack surface**
   1. Leverage multistage builds
   2. Use distroless images, or build your own from scratch
   3. Update your images frequently
   4. Watch out for exposed ports

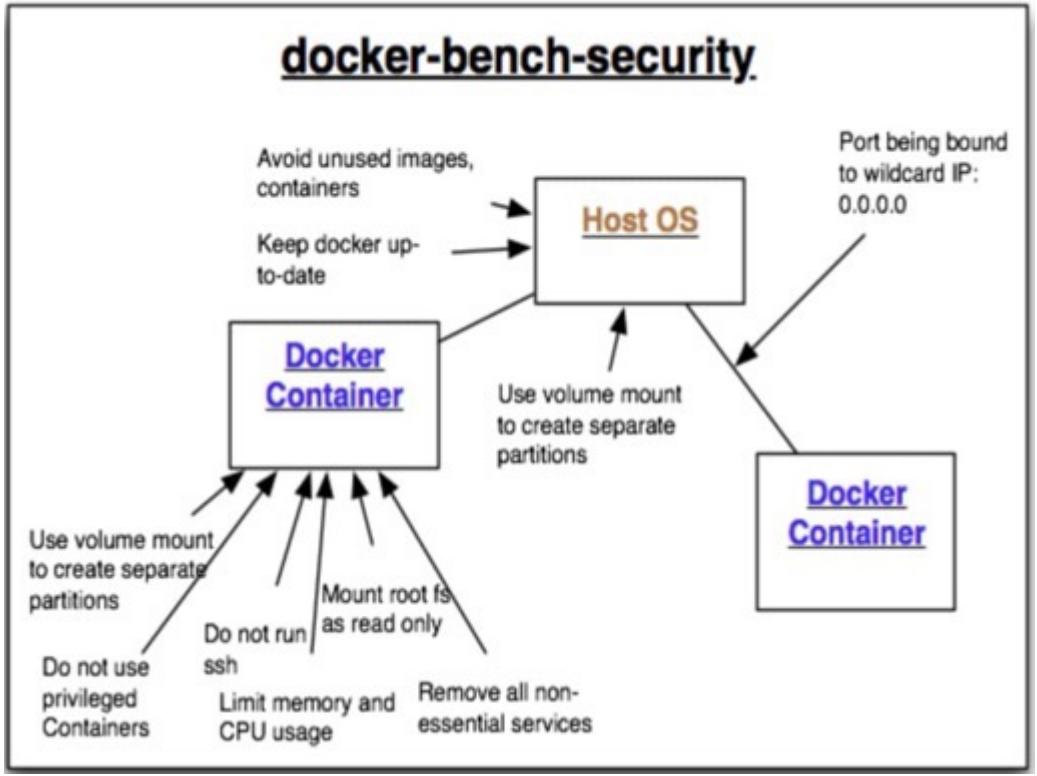
3. **Prevent confidential data leaks**
   1. Never put secrets or credentials in Dockerfile instructions
   2. Prefer COPY over ADD
   3. Be aware of the Docker context, and use .dockerignore



Docker Bench for Security

The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in the Production. The tests are all automated, and are based on the CIS Docker Benchmark v1.3.1.

Docker Bench for Security scans the Docker host for common configuration issues, such as loose settings in configuration files and system rights and questionable defaults. The tool relies on a database of Common Vulnerabilities and Exposures (CVE) to audit the libraries and executables on the system in question.



Ref: https://github.com/docker/docker-bench-security
https://systemweakness.com/automate-docker-security-audits-with-docker-bench-for-security-76b509cd7bb1

Kube-Bench for Security

aqua kube-bench

kube-bench is a tool that checks whether Kubernetes is deployed securely by running the checks documented in the CIS Kubernetes Benchmark.

Tests are configured with YAML files, making this tool easy to update as test specifications evolve.

Ref: https://github.com/aquasecurity/kube-bench
https://www.eksworkshop.com/intermediate/300_cis_eks_benchmark/intro

Vulnerability Scanning for Container Images

Docker Scan (Snyk) and Trivy

Vulnerability scanning for Docker local images allows developers and development teams to review the security state of the container images and take actions to fix issues identified during the scan, resulting in more secure deployments. **Docker Scan runs on Snyk engine**, providing users with visibility into the security posture of their local Dockerfiles and local images.

aqua trivy

Trivy (tri pronounced like trigger, vy pronounced like envy) is a simple and comprehensive scanner for vulnerabilities in container images, file systems, and Git repositories, as well as for configuration issues. Trivy detects vulnerabilities of OS packages (Alpine, RHEL, CentOS, etc.) and language-specific packages (Bundler, Composer, npm, yarn, etc.).

https://systemweakness.com/make-your-containers-better-smaller-and-more-secure-using-dockerslim-82a1ee6fcb96

Docker Slim and Grype

DockerSlim

DockerSlim is a tool for developers that provides a set of commands (build, xray, lint and others) to simplify and optimise your developer experience with containers. It makes your containers betters, smaller and more secure. Minify Docker Images by up to 30x. docker-slim will optimise and secure your containers by understanding your application and what it needs using various analysis techniques.

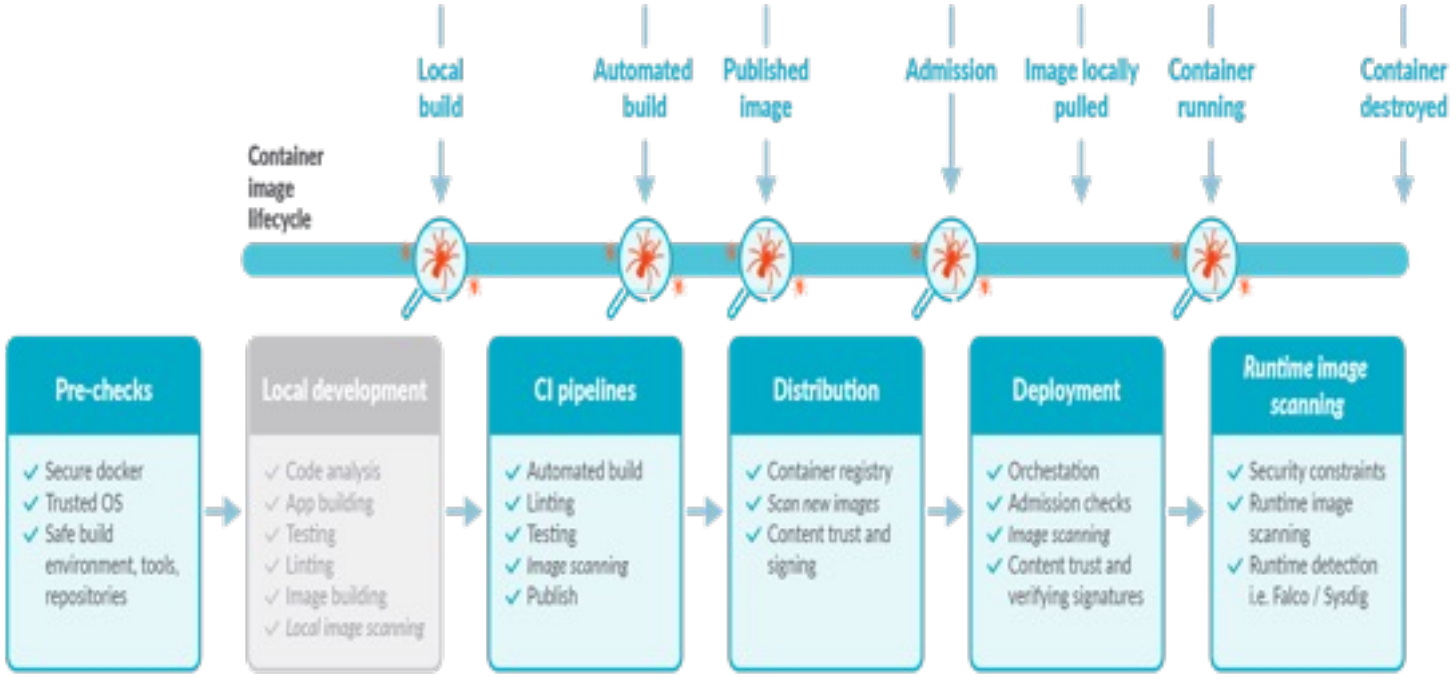
grype

Grype is a vulnerability scanner for container images and filesystems. Easily install the binary to try it out. Works with Syft, the powerful SBOM (software bill of materials) tool for container images and filesystems.

https://systemweakness.com/how-to-scan-vulnerabilities-for-docker-container-images-part1-d50b4c233245
https://systemweakness.com/how-to-scan-vulnerabilities-for-docker-container-images-part2-3e907dd0f66e

Container Image Lifecycle

DevSecCon HUNGARY



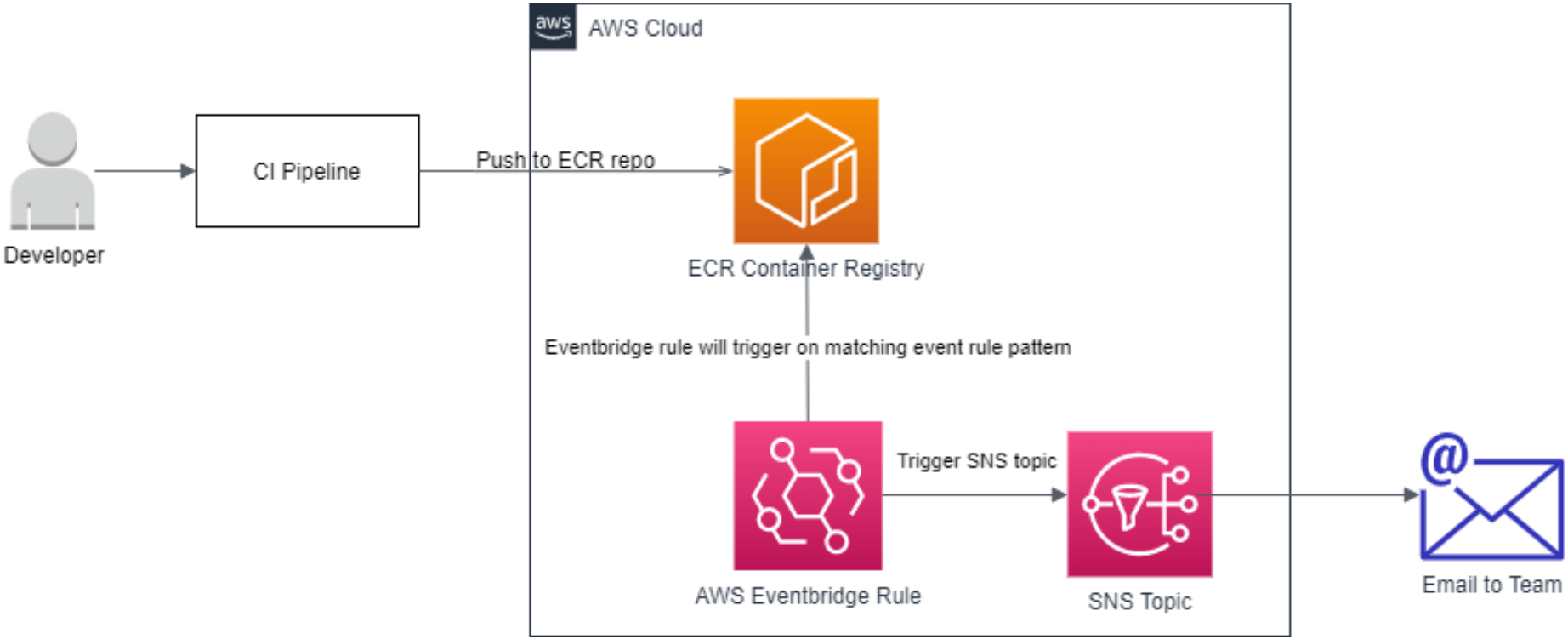
T · · Systems · Let's power higher performance

Running Containers on Amazon Web Services (AWS)

Amazon ECR

Amazon ECS

Amazon Elastic Container Registry (ECR) Image Scanning



Ref: https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html

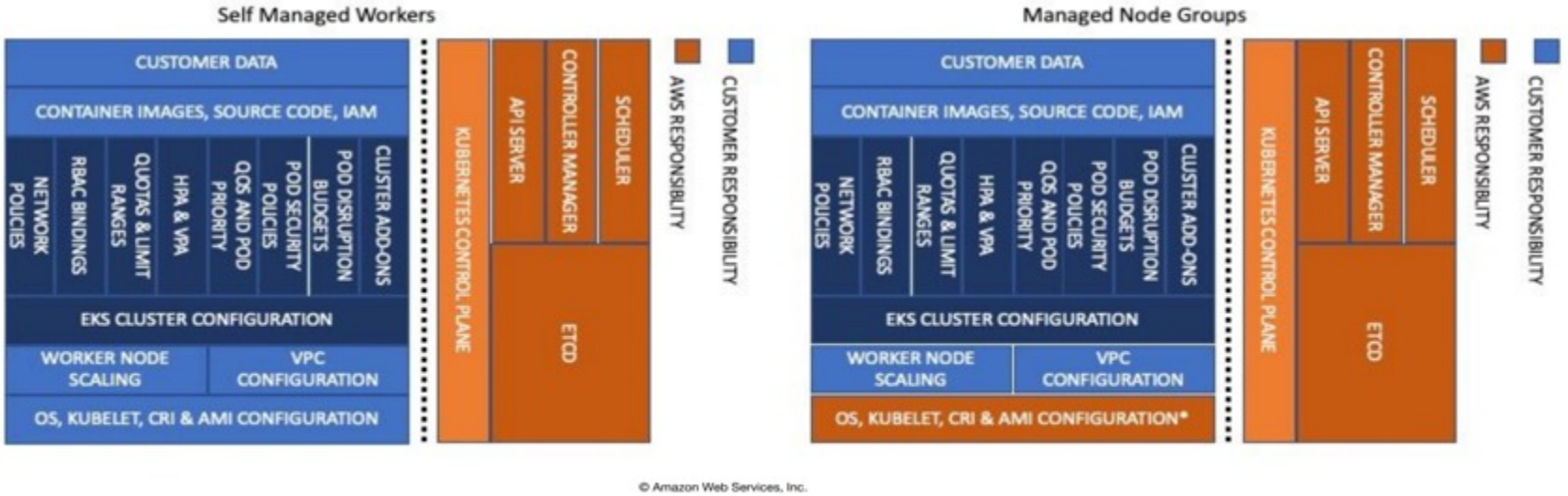
Amazon Elastic Kubernetes Service (EKS) Best Practices for Security

There are several security best practice areas that are pertinent when using a managed Kubernetes service like EKS:

- Identity and Access Management
- Pod Security
- Runtime Security
- Network Security
- Multi-tenancy
- Detective Controls
- Infrastructure Security
- Data Encryption and Secrets Management
- Regulatory Compliance
- Incident Response and Forensics
- Image Security

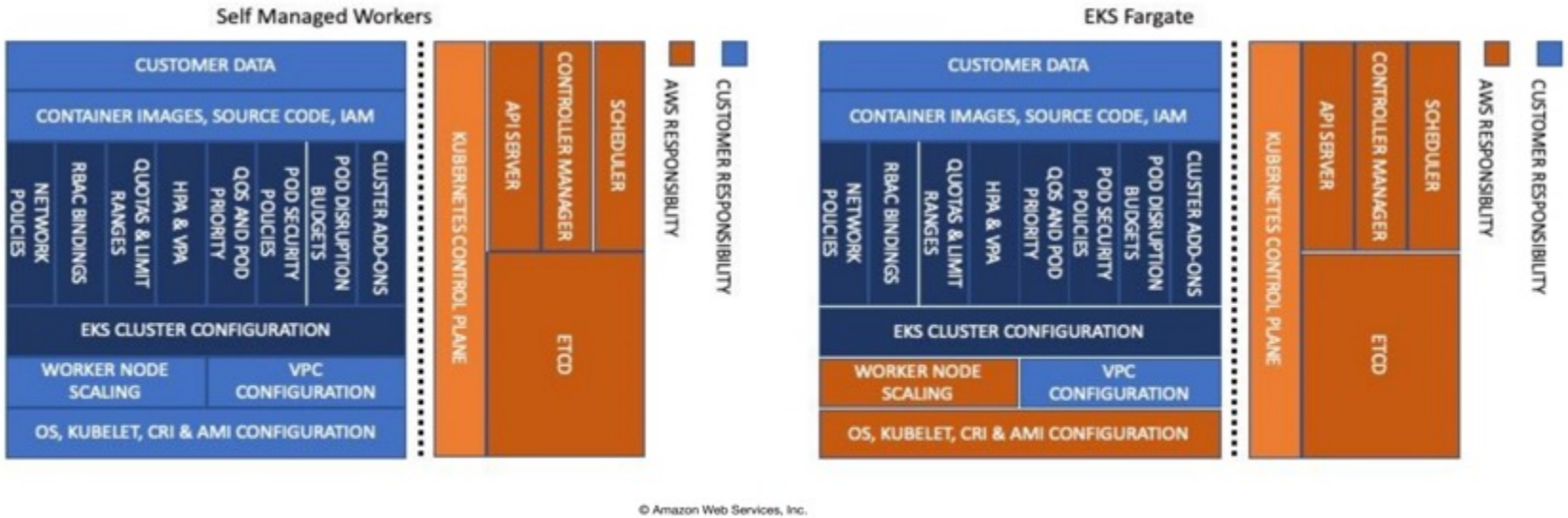
Ref: https://aws.github.io/aws-eks-best-practices/security/docs

EKS Self-Managed Vs Managed – Responsibility Matrix



Ref: https://aws.github.io/aws-eks-best-practices/security/docs

EKS Self-Managed Vs Fargate – Responsibility Matrix



Ref: https://aws.github.io/aws-eks-best-practices/security/docs

DevSecCon
HUNGARY

Questions?

T · · Systems ·

Let's power
higher performance