Container Security Checklist

Image hardening, scanning, and runtime protection

Image Hardening

- ■ Use minimal base images (distroless, Alpine, scratch)
- ■ Pin base image versions with digest (not just tag)
- ■ Run as non-root user (USER directive in Dockerfile)
- ■ Remove package managers and shells in production images
- ■ No secrets or credentials baked into images

Scanning & Compliance

- ■ Image scan in CI pipeline (Trivy, Grype, Snyk Container)
- ■ Block deployment of images with critical vulnerabilities
- ■ CIS Docker Benchmark compliance verified
- ■ Image signing enabled (cosign/Notary)
- ■ Admission controller enforces signed images only

Runtime Protection

- ■ Read-only root filesystem where possible
- ■ Resource limits (CPU, memory) configured
- ■ Network policies restricting pod-to-pod communication
- ■ Seccomp/AppArmor profiles applied
- ■ Container runtime monitoring enabled (Falco or equivalent)