Docker Recommendations

Use Container Images from Trusted Sources: Start with base images from official repositories or trusted sources. Verify the image source and consider using security-scanned base images that have undergone vulnerability scanning.

Implement Image Scanning: Utilize container image scanning tools to identify vulnerabilities and insecure configurations. These tools can help detect security issues early in the pipeline. Examples of such tools include Anchore, Clair, snyk and Trivy.

Apply Image Hardening Techniques: Secure container images by implementing best practices such as reducing the attack surface, removing unnecessary packages, and following security guidelines provided by the Docker community and CIS Docker Benchmarks.

Test Dockerfile : follow best practices by using a linter. Eg hadolint, dockle

Implement Secrets Management: Avoid storing sensitive information in container images. Instead, leverage secrets management solutions such as Docker Secrets or external tools like HashiCorp Vault to securely manage secrets required by applications.

Apply Continuous Integration and Deployment (CI/CD): Automate image builds, testing, and deployments using CI/CD pipelines. Incorporate security checks, testing, and vulnerability scanning as part of the pipeline to ensure security at each stage.

Monitor Container Runtime: Utilize monitoring tools to capture and analyze container runtime events. Monitor logs, network traffic, and container metrics to detect any anomalous behavior or security incidents.

Stay Up-to-date: Regularly update Docker, container images, and dependencies to benefit from the latest security patches and bug fixes. Keep an eye on security advisories and subscribe to relevant notifications.

CIS benchmark link : https://www.cisecurity.org/benchmark/docker

Hadolint docker, lint to check Dockerfile : https://github.com/hadolint/hadolint

Image scan : https://github.com/goodwithtech/dockle