Strengthening the Secure Supply Chain with Open-Source Tools

Paul Yu
Developer Advocate
Microsoft
@pauldotyu | /in/yupaul
Containers are awesome

• Consistent and portable environment
• Easy to manage and orchestrate via automation
• Highly scalable and can improve security
• But... high scalability increases blast radius
Security vulnerabilities galore

- 50+ CVEs reported daily
- Never ending game of whack-a-mole
Where to start

🤔

Cloud native

lego

blocks

This Photo by Unknown Author is licensed under CC BY-NC
GitHub Actions

- Continuous integration and continuous delivery platform
- Workflows trigger off an event
- Runners can be GitHub provided or self-hosted
Flux

- CNCF Graduated project (2022)
- Continuous delivery solution via GitOps
- Image update automation to detect and deploy new images
Eraser

- CNCF Sandbox project (2023)
- Removes non-running images based on vulnerability scans
- Supports Trivy but can integrate with others
Project Copacetic

• CNCF Sandbox project (2023)
• Patch container images based on vulnerability scans
• Supports Trivy but can integrate with others
Demo

- Deploy a sample project into KIND using Flux
- Run Trivy scan on a container to show vulnerabilities
- Run Copa to patch container based on Trivy report
- Deploy patched container to resolve vulnerability

- Configure Flux image update automation
- Run GitHub workflow to automate container patching
- Install Eraser to remove vulnerable image from cluster
Containers are the best thing since sliced bread

Keeping up with container security is challenging

Open-source tools can help to strengthen the secure supply chain

Supply chain security is just one aspect
Next steps

Visit the project sites and contribute
• https://github.com/aquasecurity/trivy
• https://www.cncf.io/projects/copa
• https://www.cncf.io/projects/flux
• https://www.cncf.io/projects/eraser

Follow on social
• https://twitter.com/pauldotyu
• https://linkedin.com/in/yupaul
• https://paulyu.dev
• https://twitter.com/joshduffney
https://aka.ms/cloudnative/JoinOSSDiscord