Container und Container Image Security

trivy

Trivy has scanners that look for security issues, and targets where it can find those issues.

Targets (what Trivy can scan):

- Container Image
- Filesystem
- Git Repository (remote)
- Virtual Machine Image
- Kubernetes
- AWS

Scanners (what Trivy can find there):

- OS packages and software dependencies in use (SBOM)
- Known vulnerabilities (CVEs)
- IaC issues and misconfigurations
- Sensitive information and secrets
- Software licenses

kube-bench

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

CIS Scanning as part of Trivy and the Trivy Operator

Trivy, the all in one cloud native security scanner, can be deployed as a Kubernetes Operator inside a cluster. Both, the Trivy CLI, and the Trivy Operator support CIS Kubernetes Benchmark scanning among several other features.