DN GitSecOps Reference Architecture (self-hosted)

(GitOps + DevSecOps + Security-as-Code) https://www.linkedin.com/in/martinholovsky/

v0.4 (06-2025)

Core Kubernetes Infrastructure

- Kubernetes Distribution: K3s
- Container Runtime: containerd
- Distributed KV Store: etcd
- DNS Management: ExternalDNS
- Multi-Cluster Management: Argo CD
- Multi-Network Clustering: Submariner
- Cloud Native Network/CNI: Cilium
- Infrastructure-as-Code: OpenTofu
- Policy-as-Code: Kyverno
- Configuration Management: Kustomize

Application, Deployment & Data Management

- Git Platform: Forgejo or Github
- Base image: Alpine & Scratch (static)
- Serverless: WasmEdge (on Knative)
- Continuous Integration/Delivery: Argo
- Container Registry: Harbor
- Cloud Native Storage: Longhorn
- Multi-Model Database: SurrealDB
- Streaming/Message Broker: RabbitMQ
- Backup & DR: Velero

Observability, Monitoring & Testing

- Metrics: VictoriaMetrics
- Logs: VictoriaLogs
- Visualization: Grafana
- Network flow visibility: Hubble (Cilium)
- Service Map: Hubble (Cilium)
- Process-level events: Tetragon (Cilium)
- Tracing: Tetragon (Cilium)
- Logging Agent: Vector
- Resilience & Testing: Chaos Mesh

Security & Access Control Management

- Identity Management: Kanidm
- Workload Identity: SPIRE
- Container Attestation: Cilium
- Secrets Management:
- ESO + OpenBao Vault + Yubi/Nitro HSM
- Image Signing: Sigstore (cosign)
- Code & Artifact Signing: Sigstore
- Network Policies: Cilium
- API Gateway: Emissary-Ingress
- Web Application Firewall: Coraza

Runtime Security & Auditing

- Threat Detection: Falco
- Threat Response: Tetragon (Cilium)
- Application Profiling: Tracee
- Vulnerability Scanning: Trivy
- Container Best Practices: Dockle
- System Call Enforcement: KubeArmor
- Process-level Enforcement: AppArmor
- Posture Management: Kubescape
- Security Benchmark/Audit: Kubescape
- DNS Security: Cilium

Application Security

- Static Application Security Testing:
- - Opengrep
- Dynamic Application Security Testing:
- - OWASP ZAP
- Software Composition & Secrets:
- - Trivy + Talisman (pre-commit)
- Application Vulnerability Management:
- - DefectDojo
- Web Fuzzing: FFUF, Radamsa
- Threat Modeling: AttackTree

Web Application Security & Performance

DDoS Protection, CDN, Web Application Firewall, API Gateway, Bot Management, DNS Security, Web Optimization: CloudFlare

Proposed reference architecture for deploying and managing secure, scalable, and observable microservices on Kubernetes using K3s, Cilium, Argo CD, and other open-source tools.

Key requirements in mind:

- Kubernetes-Native
- Resource Efficient
- Scalable
- Declarative
- Immutable Infrastructure
- Multi-Cluster support
- Service Mesh capabilities
- Built-in Security
- eBPF preferred (no side-cars)
- As unified as reasonably possible
- Open Source preferred

Defensive.Network