CI/CD Pipeline Design for Secure Software Delivery

Design and implementation of CI/CD pipelines that automate build, test, scan, and deployment, embedding security gates at every stage and producing audit-ready evidence for accreditation.

PRACTICE

DevSecOps and Platform Engineering

CLIENT PROFILE

Mission software team delivering applications to DoD or IC environments that require rapid, repeatable, and auditable release processes

Challenge

- Manual build and release processes causing slow delivery cadence and human error
- Security testing performed late in the lifecycle, creating costly rework
- Lack of traceability from code commit through production deployment

Approach

- Design pipeline templates with standardized stages: build, unit test, scan, artifact publish, deploy
- Embed SAST, DAST, SCA, and container scanning as automated quality gates
- Implement artifact signing and SBOM generation for supply chain integrity
- Create dashboards showing pipeline health, lead time, and security gate pass rates

Typical Outcomes

- Faster release cadence with consistent quality and security enforcement
- Earlier detection of vulnerabilities reducing remediation cost
- Complete audit trail from commit to deployment supporting ATO evidence

Procurement Paths

- DoD ESI for GitLab and JFrog platform licensing
- GSA MAS for pipeline engineering services
- NASA SEWP V and SEWP VI for DevSecOps infrastructure

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- GitLab
- JFrog
- Red Hat
- Palo Alto Networks (Prisma Cloud)

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.