

REPRESENTATIVE USE CASE

Automated Security Scanning Across the Software Lifecycle

Implementation of automated security scanning capabilities (SAST, DAST, SCA, and container scanning) integrated directly into CI/CD pipelines to catch vulnerabilities before they reach production.

PRACTICE

Platform Engineering & Secure Delivery

CLIENT PROFILE

Application development organization needing to integrate automated security testing throughout the SDLC to meet RMF and ATO requirements

Challenge

- Security scanning performed manually and infrequently, missing vulnerabilities in production
- Developers lack visibility into security findings until late in the release cycle
- Difficulty tracking and prioritizing vulnerabilities across multiple applications

Approach

- Integrate SAST and SCA scanning into CI pipelines with developer-friendly reporting
- Implement DAST scanning in staging environments as automated regression gates
- Deploy container image scanning in registries and at admission control
- Centralize vulnerability findings with severity scoring and SLA-driven remediation tracking

Typical Outcomes

- Vulnerabilities detected and reported within minutes of code commit
- Reduced number of security findings reaching production environments
- Auditable security scanning evidence supporting ATO and continuous monitoring

Procurement Paths

- DoD ESI for GitLab (integrated security scanning) and JFrog (Xray)
- NASA SEWP V and SEWP VI for application security platforms
- GSA MAS for application security engineering services

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

Partner Technology Examples

- GitLab
- JFrog (Xray)
- Palo Alto Networks (Prisma Cloud)
- Fortinet

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.