

Securing the AI-Accelerated Software Factory for Defense

The Department of Defense (DoD) is accelerating AI adoption at an unprecedented pace. Special Operations Command (SOCOM) is embedding AI and autonomy at every level, defense software funding is rising and commercial teams are using AI agent swarms to compress 4-8 month projects into two weeks. But speed brings risk. Major studies of AI-assisted development show the same pattern: code volume rising, vulnerabilities increasing and perceived speed outpacing measured gains. AI can ship code four times faster and introduce ten times more vulnerabilities than pre-AI development cycles.

In that environment, bolting AI onto an ad hoc toolchain is not a strategy; it is an attack surface. GitLab's unified Software Development Life Cycle (SDLC) platform treats AI governance as a design principle, not an afterthought.

The Problem with Rolling Your Own AI Stack

Most organizations adopting AI for software development are assembling point solutions; a code completion plugin, an inference framework, a separate scanner. The results are visible in the data:

- Pull request review times are up nearly 500%
- Security incidents per pull request have more than doubled
- 45% of AI-generated code contains OWASP Top 10 vulnerabilities

Adversaries have taken notice. The window between initial access and active exploitation has collapsed from eight hours in 2022 to just 22 seconds today. The throughline across all these risks is that speed without governance is a liability, not a capability.

GitLab's Unified AI-Native Platform

The GitLab Duo Agent Platform brings planning, coding, security analysis and remediation agents into one orchestrated environment. Instead of passing artifacts between siloed tools, GitLab agents share context through Orbit, a knowledge graph that indexes every object in a GitLab instance. A RAG pipeline enriches each prompt with project-specific context, producing outputs tailored to the codebase rather than generic training data.

When a zero-day emerges, teams can task an agent to scan every project for similar exposure, triage results against backlog data, draft patches, open merge request, route human reviewers and add text coverage. The entire workflow is defined and audited like a CI/CD pipeline.

GitLab's dashboard connects AI adoption metrics to team-level DevOps Research and Assessment (DORA) performance data, showing whether AI is truly accelerating delivery or simply masking velocity losses behind higher code volume, a distinction many self-reported studies miss.

Deployment for the Defense Mission

- Operates across classification environments relevant to defense software factories.
- Provides a fully hosted, FedRAMP Moderate-authorized environment.
- Supports self-managed, fully air-gapped deployments across multiple classification levels.
- The model-agnostic platform gives teams the flexibility to bring their own model using a standard LiteLLM interface.

For more, visit: gitlab.com/solutions/public-sector