SSDLC Training — How-To Guide

How to Integrate SAST and DAST in CI/CD

Tool selection, pipeline config, and quality gates

Step 1: Select Tools

Choose tools based on your language ecosystem and CI platform:

- SAST: Semgrep (multi-language, fast), CodeQL (GitHub native), SonarQube (enterprise)
- DAST: OWASP ZAP (free), Burp Suite (commercial), Nuclei (template-based)
- SCA: Snyk, Dependabot, Trivy, Grype
- Secrets: Gitleaks (pre-commit + CI), TruffleHog (historical scan)

Step 2: Configure Pipeline Stages

Add security scans at these pipeline stages:

- Pre-commit: Gitleaks for secrets scanning (local, fast)
- PR/CI: SAST + SCA on every pull request (block on critical/high)
- Staging: DAST against deployed staging environment
- Release: Full scan suite + SBOM generation + artifact signing

Step 3: Set Quality Gates

Define thresholds that block deployment:

- Critical vulnerabilities: zero tolerance — block immediately
- High vulnerabilities: block unless exception approved by security team
- Medium/Low: track and remediate within defined SLAs (30/90 days)
- False positives: triage and suppress with documented justification

Step 4: Manage False Positives

Use EPSS (Exploit Prediction Scoring System) to prioritize findings by exploitability, not just severity. A CVSS 7.0 with EPSS 0.001 is less urgent than a CVSS 5.0 with EPSS 0.85.