SSDLC Training — Checklist

Security Testing Pipeline Checklist

SAST/DAST/SCA integration at each SDLC stage

Pre-Commit

■ Secret scanning hook installed (gitleaks, truffleHog)

■ Linting rules include security checks

Pull Request / CI

■ SAST scan runs on every PR (Semgrep, CodeQL, SonarQube)

■ SCA scan checks dependencies for known vulnerabilities

■ License compliance check for new dependencies

■ Quality gate blocks merge if critical/high findings detected

■ DAST scan runs against PR preview environment (if available)

Pre-Release

■ Full DAST scan against staging environment

■ Container image scan (Trivy, Grype) for base image vulnerabilities

■ IaC scan (Checkov, tfsec) for infrastructure misconfigurations

■ SBOM generated and stored with release artifacts

Post-Release

■ Runtime monitoring alerts configured

■ Dependency vulnerability monitoring enabled (Dependabot, Snyk)

■ Periodic penetration testing scheduled (quarterly/annually)