Repository Security Hardening Checklist

Branch protection, signing, and access controls

Branch Protection

- ■ Main/production branch protected against direct push
- ■ Require pull request reviews (minimum 2 approvers for sensitive repos)
- ■ Require status checks to pass before merge (CI, SAST, tests)
- ■ Require signed commits on protected branches
- ■ Dismiss stale reviews when new commits are pushed

Access Controls

- ■ CODEOWNERS file configured for security-critical paths
- ■ Repository access follows least privilege (read/write/admin)
- ■ Service account tokens scoped and rotated on schedule
- ■ Fork restrictions configured for private repositories
- ■ Audit log enabled and reviewed monthly

Commit Signing & Provenance

- ■ GPG or SSH commit signing configured for all committers
- ■ Signed commits enforced via branch protection rules
- ■ AI-generated code commits tagged with provenance metadata
- ■ Sigstore/keyless signing evaluated for CI-generated commits