GitHub Actions Security Best Practices Checklist

Secret Management

- Use OpenID Connect (OIDC)
- Set least privileged GITHUB_TOKEN permissions
- Use environment secrets with mandatory reviews
- Rotate GitHub Actions secrets
- Don’t print secrets in Actions run logs
- Don’t use structured data as secrets
- Scan GitHub Actions logs for secrets

Workflow Change Management

- Use reusable workflows
- Run sensitive workflows only on trusted code
- Enable Dependabot for GitHub Actions
- Enable branch protection
- Use CODEOWNERS
- Prevent GitHub Actions from creating/approving pull requests
- Disable workflow runs from forked repositories if not required

Self-Hosted Runners

- Secure the underlying infrastructure hosting self-hosted runners
- Use ephemeral runners
- Avoid using self-hosted runners with public repositories
- Harden-Runner Image

Third-party Actions Governance

- Enforce allow specific third-party GitHub Actions policy
- Review third-party Actions
- Fork risky third-party Actions
- Pin third-party Actions

Developer Education

- Leverage GitHub Actions Goat

Prevent Script Injection Vulnerabilities

- Avoid inline scripts
- Use intermediate environment variables for inline scripts

Runtime Security

- Use Harden-Runner