Security Gotchas Checklist (CI/CD)

Minimal, actionable checks you can run before you ship.

Secrets & Credentials

- No secrets in repo history (`git log -p` + secret scanners).
- Use platform secrets or cloud secret managers; rotate keys every 90 days.
- Mask secrets in logs and disable command echo around sensitive steps.

IAM & Access Control

- Use least-privilege roles for CI (separate from human users).
- Prefer OIDC/WIF over long-lived cloud keys.
- Expire or revoke unused tokens and PATs.

Build & Supply Chain

- Pin action/plugin versions (e.g., `actions/checkout@v4`).
- Verify checksums/signatures for downloaded tools.
- Cache dependencies but do not cache node_modules/vendor across branches without integrity checks.

Artifacts & Storage

- Encrypt artifacts at rest; set short retention (e.g., 7–14 days).
- Avoid public buckets/containers for build outputs.
- Tag artifacts with commit SHA and build number for traceability.

Runtime & Network

- Restrict SSH sources with security groups/NSGs/firewalls.
- Use HTTPS everywhere; redirect HTTP → HTTPS.
- Enable WAF or equivalent protections for public endpoints.

Governance & Hygiene

- Branch protections: require reviews and status checks on main.
- Dependabot/Renovate enabled and not ignored.
- Backup & DR tested; incident response playbooks documented.