Cloud Waste Scanner

Security Review Checklist

Version 1.0 · 2026-03 · Local-first security and rollout validation

- [ ] 1. Trust Boundary: Confirm provider credentials stay in operator-controlled environment.
- [ ] 2. Trust Boundary: Confirm hosted services do not receive raw provider keys.
- [ ] 3. Access: Verify read-only or minimum IAM scope for scan workflows.
- [ ] 4. Access: Separate production and non-production credential profiles.
- [ ] 5. Transport: Enforce HTTPS and validate proxy route policy.
- [ ] 6. Endpoint: Validate patching, disk encryption, and endpoint telemetry baseline.
- [ ] 7. Token/API: Rotate local API token and record rotation date.
- [ ] 8. Token/API: Verify token regeneration runbook is tested.
- [ ] 9. Evidence: Confirm finding outputs preserve source fields and timestamps.
- [ ] 10. Evidence: Export review package (PDF/CSV) and archive with review notes.
- [ ] 11. Release: Verify checksum/signature before rollout.
- [ ] 12. Release: Attach release gate evidence and approver to change record.
- [ ] 13. Incident: Confirm owner/on-call map for containment and rollback.
- [ ] 14. Incident: Run tabletop for credential leak and route failure scenarios.

Use this checklist during architecture review, rollout sign-off, and recurring governance audits.