facebook-evidence-cover.md

Evidence cover note for Facebook reviewers
Date: 2025-10-24T17:29:00Z (UTC)
Purpose

This cover note explains the evidence attached for the AutoPromote app's Data Access Renewal review. It points reviewers to the files that demonstrate:
- collection of admin/application audit logs and a weekly review process,
- automated dependency scanning of the server-side backend (server-side dependency scan output), and
- an example automated alert/ticket created from the scan output.
Files included (locations in repository)
- docs/audit-logs-collection-review-policy.md — The audit log collection & review policy (states weekly review cadence, logged events and escalation steps). Please highlight the sections that describe "review frequency & process", "what we log (minimum required)", and "Escalation".
- docs/security-event-investigation-policy.md — The investigation policy (triage, evidence collection, escalation). Please highlight the triage, evidence collection and escalation sections.
- docs/code-backend-updates-policy.md — Patch management and vulnerability remediation policy (shows scan cadence and remediation steps). Highlight the Process and Evidence sections.
- evidence/npm-audit.json — Raw `npm audit --json` output (server-side dependency scan). This file contains the exact scan output and metadata including vulnerability counts and severities.
- evidence/npm-deps.json — Raw `npm ls --all --json` output (dependency tree). This file shows the exact packages scanned and the dependency paths.
- evidence/dependency-scan-report.txt — Human-readable summary report produced at the same time as the raw scan. Contains the scan timestamp and a short advisory summary.
- evidence/dependency-vulns.csv — CSV extract of the vulnerabilities (columns: package,severity,range,fixAvailable,advisories).
- evidence/automated-alert.md — A redacted, reviewer-friendly ticket/alert generated by our automated process that references the scan output and creates a tracking ticket (redacted placeholders used where appropriate).
- evidence/sample-admin-audit-log.csv — A redacted sample of admin audit log entries that shows timestamps, event types and actor placeholders (REDACTED) so you can verify audit log collection.
- evidence/sample-alert.txt — A redacted example alert/ticket text file showing automated monitoring triggering an investigation/ticket.
What these files demonstrate
- Audit logs are collected and contain timestamps and event types: `sample-admin-audit-log.csv` shows the required fields (timestamps, event_type, actor, resource, details). The policy files explain retention, review cadence and escalation.
- Automated scanning is executed and produces server-side scan artifacts: `npm-audit.json` and `npm-deps.json` are the raw outputs from running `npm audit --json` and `npm ls --all --json` respectively. The human-readable report and CSV (`dependency-scan-report.txt`, `dependency-vulns.csv`) summarize results for easy review.
- Automated evidence-to-ticket flow: `automated-alert.md` demonstrates that the scan is integrated into our process and creates an actionable ticket referencing attached evidence.
Commands & methodology used to generate the scan
- Command run (exact):
  - npm audit --json
  - npm ls --all --json
- Script used (runs the commands above and packages the results): `scripts/generate-evidence.ps1`
- Scan timestamp: 2025-10-24T17:29:00Z (UTC). Evidence files in `evidence/` were created at this time.
Redaction note
- All uploaded artifacts intended for external review have been redacted to remove personally identifiable information (user IDs, emails, IP addresses, tokens). Where real examples are required, replace values with the literal string REDACTED while keeping event types and timestamps intact.
Suggested highlights for reviewers
- In `docs/audit-logs-collection-review-policy.md` highlight:
  - "Review frequency & process" (weekly review cadence)
  - "What we log (minimum required)" (lists unsuccessful login attempts, admin privilege changes, deletion of audit logs, etc.)
  - "Escalation" (steps when a security event is confirmed)
- In `docs/security-event-investigation-policy.md` highlight:
  - The investigation steps (Triage, Containment, Evidence collection, Root cause, Remediation, Post-incident)
- For the dependency scan evidence, review `dependency-scan-report.txt` first (summary), then inspect `npm-audit.json` and `dependency-vulns.csv` for details.
If you need any additional formats

- I can produce a redacted PDF version of the report or a ZIP bundle containing only the files you request. I can also provide short screencapture PNGs (redacted) showing alerts or dashboard entries if required.

Contact

- If reviewers need clarification, please direct questions to the Security Owner listed in the policy documents (security@example.com) and reference Ticket ID shown in `evidence/automated-alert.md`.

Thank you for reviewing — we are available to provide additional redacted screenshots or CI logs on request.