Security Sweep — lumiscare.com Public Landing — MC #107301 (2026-08-18)

lumiscare.com Security Sweep — MC #107301

Overall verdict: PARTIAL
Public marketing domain: PASS
Repository credential/key posture: BLOCKED — external rotation/owner decisions required
Date: 2026-08-18

Scope and privacy boundary

Only public `lumiscare.com`, tracked `landing/`, repository metadata/history scans and deployment configuration were examined. No authentication, patient/carer/tenant data, PHI, clinical API, portal workflow, account or form submission was accessed. Both AzDO and GitHub repositories are PRIVATE.

Public-domain findings and remediation

1. **P1 — false 200 fallback:** `navigationFallback` rewrote every unknown/source/sensitive path to the homepage with HTTP 200.
   - Removed SPA fallback (the marketing site has no client router).
   - Added `404.html` and SWA `responseOverrides.404` preserving HTTP 404.
2. **P2 — unnecessary CSP privilege:** a scriptless/formless static site allowed inline/eval scripts, broad Microsoft/Azure/ALAI connections, blob and arbitrary HTTPS images.
   - CSP now uses `script-src 'none'`, `connect-src 'none'`, `form-action 'none'`, `object-src 'none'`, `frame-ancestors 'none'`, explicit Google Fonts styles/fonts and self/data images only.
   - Added COOP/CORP and expanded Permissions-Policy denial.

3. **P2 — missing regression gate:** added `scripts/check-public-landing.py` and blocking Azure CI job for exact asset allowlist, no scripts/forms/symlinks, strict CSP and true 404.
4. **P1 process safety — clinical blast radius:** ordinary manual runs deploy backend and all clinical portals.
   - Added typed `ciOnly` and `publicLandingOnly` runtime parameters.
   - Build #1141 proved a queue variable was ineffective and was cancelled before any backend build/deploy job.
   - Build #1145 proved backend-only guarding still allowed frontend stage entry and was cancelled before any SWA deploy job.
   - Build #1148 PASS: only `Gate: Public landing security` ran; every build/deploy/PI2/prod stage was machine-verified SKIPPED.
5. **Credential hygiene:** removed RUNBOOK instructions that extracted a PAT from a git remote. The expired credential-bearing local `azdo` URL was replaced by credential-free canonical HTTPS; current vault askpass was validated. No credential value appears in evidence.

Public verification

- Local preflight PASS; Azure SWA emulator: root/legal 200, source/config/unknown paths true 404, restrictive headers live.
- Landing Gitleaks 0; landing Semgrep 0 findings / 0 errors.
- Preview SWA `mc107301`: Playwright **4/4 PASS**, desktop/mobile screenshots, zero data entry.
- AzDO PR #357 merged to `dev` as `e7560a32bd78a0f3e862a5a2852ce52b73575ffe` with explicit `[skip ci]`; no automatic clinical pipeline was created.
- Production deployed manually to only `lumiscare-landing`; no backend/backoffice/admin/family deployment.
- Production Playwright **4/4 PASS**.
- Final exact probes: **13/13 HTTP 404**; homepage hash exactly matches merged `landing/index.html`; TLS and all required headers live.
- Preview deleted; only SWA environment `default` remains Ready.

Repository blockers — not silently closed

Redacted full scan found 35 current-tree and 76 reachable-history Gitleaks records. They include documented legacy/test candidates but also previously confirmed security findings that this public-domain task cannot safely rotate or rewrite:

- **MC #10065 (paused, owner decision):** tracked RSA private-key files; revoke/replace/history treatment requires owner authorization.

- **MC #103380 (open):** legacy external-tenant Azure service-principal secret; external tenant admin must rotate/delete and audit RBAC. No value was printed.
- **MC #103765 (open):** Azure DevOps PAT class in historical/current build material; rotation and repository-wide cleanup remain owned by that task.

Current-tree removal alone would not revoke credentials or purge reachable history. Those actions cross client/legacy-tenant boundaries and are therefore a real blocker, not a process excuse. Consequently the repository cannot receive a zero-secret PASS under MC #107301.

Residual accepted items

- `style-src 'unsafe-inline'` remains because the canonical landing embeds CSS in HTML; scripts are fully disabled.
- Google Fonts remain external and explicitly scoped in CSP.
- Marketing/feature claims were not validated as clinical capabilities in this security task.

Evidence anchors

- `final-live-security-summary.json`
- `production-playwright-report.json`
- `build-1148-timeline.json`
- `azdo-build-1148.json`
- `azdo-pr-completed.json`
- `preview-cleanup.json`
- `repository-visibility.json`
- `baseline/gitleaks-tree.json` and `baseline/gitleaks-history.json` (redacted, mode 0600)
- `remediation-local/`

Revision #1
Created 2026-08-18 13:01:28 UTC by John
Updated 2026-08-18 13:01:28 UTC by John