LumisCare CI — Snyk + Lighthouse for deployed packages (MC #102842) — 2026-06-03

Summary

MC #102842 re-adds **Snyk** (dependency scan) and **Lighthouse** (performance) CI jobs to `.github/workflows/ci.yml` for the **deployed** pnpm packages, replacing the placeholder TODOs left by MC #102817 (which removed the old jobs that scanned the dead `frontend/web/` tree).

- **Repo:** github.com/johnatbasicas/vivacare — branch `ci/snyk-lighthouse-packages-102842` → **PR #43** (base `dev`)
- **Fix commit:** `1ed9f107`

What was added

`security` job (Snyk)

- Scans deployed packages: `frontend/packages/{backoffice,admin,family-portal}/package.json`
- Auth via `${{ secrets.SNYK_TOKEN }}` only — **never hardcoded**
- `--severity-threshold=high`
- **Advisory / non-blocking** (`continue-on-error: true`); NOT in the blocking `quality-gate` `needs:`
- **Graceful degrade:** a guard step checks the token; if absent it emits a `::warning::` and skips the scans (job stays success) rather than hard-failing

`lighthouse` job

- Runs `lhci collect` against the **live** SWA URLs — `app.lumiscare.com`, `admin.lumiscare.com`, `family.lumiscare.com`
- Does **not** build the dead `frontend/web/` tree
- Advisory / non-blocking

Defect caught + fixed before close

First CI run (`26888003662`) the Snyk job died at `pnpm install --frozen-lockfile` with `ERR_PNPM_IGNORED_BUILDS` (exit 1) — `pnpm/action-setup@v4 version: latest` resolved to pnpm v10, which treats ignored build scripts as a hard error. `deploy.yml` pins `PNPM_VERSION: "9"` (warn only). **Fix:** pin pnpm 9 + add pnpm cache, mirroring `deploy.yml`.

Verification

- FINAL CI run **26888884509** = `completed/success`; all 5 jobs success (backend-test, security, lighthouse, code-scan, quality-gate REQUIRED).
- Snyk install step success (641 pkgs); guard fired (`skip=true`, token absent); scans skipped; job success.
- Independent verifier subagent: **13/13** atomic claims PASS.
- Company Mesh P2P pre-verifier (eval/Proveo): **PASS** — `mesh-thr-105cdec0-7dd4-4370-adb0-271547da635a`.
- til-done verdict: **DONE** — receipt `/tmp/til-done/102842-20260603T135849Z.json`.

Standing CEO action

Add **`SNYK_TOKEN`** to the `johnatbasicas/vivacare` repo secrets (Settings → Secrets → Actions) to activate real Snyk scanning. Until then the job skips cleanly with a warning. (John's PAT lacks `secrets:write` — HTTP 403.)

Revision #1
Created 2026-06-03 14:02:15 UTC by John
Updated 2026-06-03 14:02:15 UTC by John