psLens

PeopleSoft Operations & Security Intelligence

pslens.com
chris.malek@cedarhillsgroup.com

psLens is a read-only web console for PeopleSoft. It searches every PeopleSoft object type (records, pages, components, permission lists, and more), runs security audit reports, and monitors Process Scheduler and Integration Broker across all connected databases — from a browser, without App Designer or SQL access.

30+	16	14	<1s
PeopleSoft object types browsable	real-time alert types	on-demand audit reports	object search response

HOW IT CONNECTS

psLens never opens a connection to your database. It queries PeopleSoft through the **SWS framework**, a REST layer delivered as a standard App Designer project (roughly 100 objects under the `CHG_/C_` prefixes, two service operations, two roles) that you migrate through your normal change process. All traffic arrives through the Integration Broker REST endpoint as ordinary service operation requests, visible in your existing IB monitoring.

SECURITY POSTURE

- **Read-only by design.** psLens has no code path that writes to PeopleSoft.
- **Bounded query surface.** SWS answers queries only against a whitelist of PeopleTools metadata tables, enforced on the PeopleSoft side. You review and can narrow the whitelist before approving it.
- **No database credentials.** Users never connect to the database; DB passwords stay in PeopleSoft.
- **No business data stored.** psLens stores alert history and report output (90 days). It does not copy employee, financial, or HR data.
- **No browser storage.** Pages render server-side; nothing is written to LocalStorage, SessionStorage, or IndexedDB.
- **Secrets encrypted at rest.** The one stored credential (the SWS service account) is encrypted with AES-256-GCM.

DEPLOYMENT

- **Dedicated instance per customer** — no shared multi-tenant backend.
- Managed hosting (fly.io region of your choice), self-hosted (Docker, systemd, Kubernetes), or air-gapped.
- Single Go binary; 1 vCPU / 512 MB RAM minimum footprint.
- **Egress:** HTTPS to your SWS endpoint, plus SMTPS only if magic-link sign-in is enabled. No telemetry, no update checks, no callbacks.
- Structured logs to stderr — your runtime and SIEM own retention.

AUTHENTICATION

Email magic-link, or front psLens with your reverse-proxy SSO (OIDC, Cloudflare Access, oauth2-proxy) to enforce your IdP policy including MFA. Native OIDC is on the roadmap.

WHAT IT'S USED FOR

- Security audits: overly broad permission lists, stale passwords, node authentication gaps, web-service access.
- Operational alerting: failed and long-running processes, stalled IB messages, locked operator accounts.
- Metadata research without granting App Designer to non-developers.
- Markdown export of any object or report for documentation and AI-assisted analysis.

EVALUATING PSLENS

Demos run against a live PeopleSoft environment: 30 minutes, no preparation, no commitment. Full security documentation — data handling, what SWS installs, sub-processors, business continuity — is published at **pslens.com/security**. Security questions answered in writing: **security@cedarhillsgroup.com**.