

Lans Hung

Staff Platform Engineer — Product & Supply-Chain Security

San Francisco Bay Area | [lans-h.cc](#) | lansoulot@gmail.com | github.com/amdslancelot

SUMMARY OF QUALIFICATIONS

Staff platform engineer, 10+ years in distributed systems, site reliability and open-source software security. Owned the vulnerability lifecycle and secure release pipelines behind a commercially supported Linux distribution — CSAF/VEX/OVAL advisories at 3,500+/year, CVE backporting across 50+ packages, artifact distribution at ~23M downloads/month. Since leaving Oracle, I converted a decade of platform engineering into **security-owned systems I run in production**: a multi-tenant Kubernetes platform where tenant isolation, signed delivery and certificate lifecycle are the design, and two open-source Claude Code plugins that constrain autonomous agents — permission boundaries, execution separated from verification, per-call cost telemetry — the basis for reasoning about **AI risk in a product and in an engineering process**.

SKILLS

Languages: Python, Java, Go (module/vendoring toolchain), Shell/Bash, SQL

Product & Supply-Chain Security: CSAF/VEX/OVAL advisories, CVE backporting, applicability triage (OVAL/OpenSCAP), package & repository integrity (SHA-256 chains, GPG signature model, gpgcheck), air-gapped dependency vendoring

Application Security: multi-tenant data isolation & least privilege, threat modeling, encryption-at-rest (Kubernetes Secrets/etcd) with data-layer verification, TLS/PKI & ACME DNS-01 lifecycle, HMAC request signing, OAuth 2.0/OIDC, zero-trust production access (bastion, SSH-CA short-lived certificates, hardware token), SELinux, secrets rotation

Cloud/Infra & Automation: OCI (AWS/GCP), Kubernetes, Docker/Podman, Terraform, Ansible/AWX, IaC, CI/CD, RPM/dnf/yum, Bare-Metal/VM provisioning, Apache/Nginx, Grafana

Data: PostgreSQL, Oracle DB, Cassandra, MongoDB, Redis, Solr, MySQL

Agentic AI: Claude Code plugins/skills/hooks, subagent orchestration & permission boundaries, LLM evaluation, token/cost instrumentation

SELECTED PROJECTS

Platform lans-h.cc — Multi-tenant Kubernetes platform running a four-app fleet 2025 – present

- Designed and operate the shared infrastructure four independent apps run on, with **tenant isolation as the organizing constraint**: one database and one LOGIN-only least-privilege role per app, CONNECT revoked from PUBLIC, provisioned by an idempotent script that ends by verifying it — own database reachable, a peer's refused.
- Delivery is signed, not trusted**: deploys arrive over an HMAC-verified webhook behind per-app CI gates with read-only credentials; a wildcard ACME DNS-01 certificate is the ingress default, so no app handles key material. Omitted controls — Postgres without TLS — are recorded with their rationale.

Stack: Kubernetes, Traefik, cert-manager (ACME DNS-01), PostgreSQL role/grant isolation, HMAC webhooks, Kustomize, GitHub Actions

Upward Mobility — Agent operating controls + LLM evaluation methodology 2025 – present

- Published two Claude Code plugins: `upward`, which **constrains how autonomous agents run** — a single executing context with read-only sub-agents (delegation reversed on measurement), verification performed by an actor other than the one that did the work, an explicit model-tier escalation ladder — and `upward-stats`, a hook-based token accountant supplying the telemetry to audit what an agent did.
- Benchmarking exposed the harder problem: **LLM-on-LLM evaluation invalidates itself** — a drifting subject, a reviewer generating its own criteria, a scaffold overfitting to prior rounds — and autonomy raises verification cost rather than lowering it. Execution scales inside bounded specifications; scope, acceptance and pivot decisions remain human.

Stack: Claude Code plugin/skill/hook APIs, headless agent orchestration, LLM evaluation methodology, token/cost instrumentation

Snoopy Home — Household AI assistant chatbot | Live on Discord 2025 – present

- Gemini-powered Discord assistant, and the cluster used to validate platform controls: enabled AES-CBC

encryption-at-rest for Kubernetes Secrets and **verified it at the data layer, not at the flag** — marker absent from etcd's raw store, `k8s:enc:aescbc:` prefix present — then automated against regression.

- Rejected encrypted per-tenant service-account keys in the credential threat model: an operator-held master key leaves the trust boundary unchanged; per-household OAuth allows independent revocation.

Stack: Python, Google Gemini API (native function calling), discord.py, PostgreSQL/asyncpg, APScheduler, Google Calendar API

Transigen — Boiler Room style AI automix web app | Live at transigen.lans-h.cc 2025 – present

- DJ automix web app: cached YouTube/Spotify ingestion, beat-mapped transitions, self-hosted Postgres + Auth.js.

Stack: Next.js 15, React 19, TypeScript, PostgreSQL (LISTEN/NOTIFY-to-SSE), Google OAuth, YouTube IFrame API, beat-analysis worker

Gelp — A better way to find Google Maps saved places | Live at gelp.lans-h.cc 2025 – present

- Google Takeout export turned into a list/place/map browser. **No credential reaches the browser:** the Places key stays server-side and the map layer is keyless OpenStreetMap tiles.

Stack: Next.js 15 (App Router), TypeScript, NextAuth v5, PostgreSQL (Drizzle ORM), Leaflet/OpenStreetMap, Google Places & Drive APIs

PROFESSIONAL EXPERIENCE

Staff Platform Engineer

10/2023 – 09/2025

Oracle Linux Services, *Remote*

- Architected the machine-readable **security advisory (CSAF/VEX/OVAL) pipeline** publishing 3,500+ advisories/year, and closed detection gaps upstream OVAL auditing missed by redesigning package module-stream support.
- Fielded **vulnerability applicability triage** for customers and internal scan findings — mapped CVEs onto errata and proved backported fixes with OVAL/OpenSCAP and package changelogs.
- Owned the dual API surfaces — customer-facing yum-client (registration, subscription, dependency resolution, errata/CVE queries) and the internal operator pipeline (channel lifecycle, errata publishing, advisory generation).
- Operated the yum-channel release pipelines (1M+ packages / ~57M monthly downloads) and the OCI and Oracle official image registry mirrors (22 geo-distributed endpoints, ~23M monthly downloads).
- Containerized Open Source Software platform to run on OL9 and executed a zero-downtime x86-to-ARM migration with ~90% **automated provisioning** via Ansible (23 roles), reducing deploy cost to 10%.

Staff Product Engineer

08/2022 – 10/2023

Oracle Automation Platform, *Remote*

- Delivered **0-to-1** of an Ansible CI/CD Automation platform (AWX based) as tech lead (research, architect, workflow, product delivery) of a cross-functional team of ~6 (2 engineers, 2 QA, technical writer, PM) + support team.
- Containerized job execution runtime with libraries/SDK dependencies based on job types, to decouple job scaling issues between playbooks, softwares, and Ansible runtime as task complexity increases.
- Integrated OCI natively (credential type + toolchain in the execution image), enabling direct OCI resource management from job templates.

Senior Software Engineer

12/2015 – 08/2022

Oracle Linux Release Engineering, *Redwood Shores*

- Maintained and code-reviewed 50+ Oracle Linux packages across OL6/7/8 (Python, curl, PowerShell) — backported upstream CVE patches through the full patch-review-build-release lifecycle for production Errata.
- Built `go_vendor_gen` to automate third-party Go dependency vendoring (Terraform / rclone / packer modules) for Oracle Linux's air-gapped RPM build system.
- Built BugDB-CLI (batch field updates + CI/CD comment detection for status updates automation), unblocking the Linux team's Bugzilla-to-BugDB migration.
- Built a Grafana release-tracking dashboard for package and errata shipment status across OL6/7/8.

Software Engineer

04/2014 – 10/2015

Fuhu, Inc, *Milpitas*

- Backend engineer on the NabiPass Catalog API (Java Spring + Cassandra); built Apache Solr text search.

Analytics Engineer

08/2012 – 01/2014

Kixeye Inc, *San Francisco*

- Built an analytics dashboard (Hadoop/Hive, MongoDB, MySQL) driving in-game event logging.

EDUCATION

M.S. Computer Science,

University of Southern California (USC)