Joseph Gharbieh

Oceanside, CA | (442) 500-4816 | jgharbieh42@gmail.com | linkedin.com/in/joseph-gharbieh | github.com/jgharbieh | joseph-gharbieh.com

SUMMARY

Application Security & AI Systems Engineer with hands-on experience across authorization architecture (RBAC/IDOR/BOLA remediation), AI-directed development at production scale, and full-stack engineering (React/Next.js, Node.js, TypeScript). Background spans hiring/operations leadership to security hardening, giving direct visibility into how the work actually gets used. Open to full-time and contract roles.

SKILLS

Application Security

RBAC design, enforcement & propagation; authorization enforcement & privilege context analysis; trust boundary & data classification design; default deny & secure failure modes; identity & access management (Google Workspace, M365); broken access control (IDOR/BOLA, privilege escalation, authz bypass); multi-tenant isolation & cross-tenant leak remediation; authentication & session architecture; row-level security (RLS) patterns; XSS, open redirect & input validation; OWASP Top 10 & CVSS v3.1 scoring; networking, protocols & infrastructure (CompTIA Network+)

AI Engineering & Enablement

AI-directed development at production scale; prompt engineering; AI enablement tooling; agent sandboxing & parallel execution; LLM API integration (Anthropic, OpenAI); conversational AI & AI-powered application development; MCP client development, hosting & access control; browser automation & CDP

Engineering

Root cause debugging & performance profiling; browser DevTools & client-side debugging; TypeScript/JavaScript; React/Next.js (App Router); Convex; Node.js/Express; SQL & schema design; REST & webhook integration; front-end implementation & UX; Electron

Automation & Pipeline Design

GoHighLevel pipeline & workflow design; workflow automation (Make.com); Twilio, telephony & SMS systems; A2P 10DLC registration & carrier compliance

Data & Knowledge Systems

Enterprise knowledge base architecture; RAG (retrieval augmented generation) system design; data repatriation from vendor systems; operational data analysis & closed-loop feedback

Systems & Delivery

Docker & containerized environments; Git/version control; cloud cost optimization; Cloudflare, Google Cloud, Vercel; CI/CD design & automated deploy pipelines; Linux

Platforms

Google Workspace administration; Microsoft 365 administration & support (Excel, Word, tenant ops); Tekmetric, ClickUp, Slack, Discord

EXPERIENCE

MTS Moose Tech Solutions L.L.C. — Oceanside, CA **Jun 2023 – Present**

Application Security & AI Systems Engineer *Jan 2026 – Present*

- Identify and remediate broken access control in production: broken object level authorization (IDOR/BOLA), vertical and horizontal privilege escalation, cross-tenant data exposure, and authorization bypass through call paths the enforcement layer never sees.
- Trace privilege context across the call graph, including confused deputy conditions where a privileged service identity acts for a lower-privileged caller and skips the gate entirely.
- Score findings against the OWASP Top 10 and CVSS v3.1, and defend every metric in the vector.
- Design RBAC models that stay consistent across every enforcement point they touch — data layer gates, API routes, client state, and isolated operator surfaces — from a centralized policy store with event-driven propagation.
- Harden identity end to end: authentication, authorization, session architecture, user provisioning, invitation and account claim flows, and the identity lifecycle around them.
- Enforce default deny: row-level security, secure failure modes, attack surface reduction, and explicit error handling in place of silent failure.
- Diagnose client-side and application performance to root cause in application logic and query patterns rather than infrastructure spend.
- Ship front-end: UI implementation, client state, and the authorization gating that decides what a user is permitted to see.
- Direct agentic development workflows across parallel isolated environments on a fixed budget, and verify output rather than trust it.

Technical Recruiter *Jun 2023 – Jan 2026*

- Executed full lifecycle staffing: sourcing, screening, resume redesign, job posting creation, interview coordination, and onboarding support.
- Sourced and screened more than 300 candidates across IT, cybersecurity, and administrative roles.
- Redesigned 120+ resumes to meet vendor and client submission requirements.
- Coordinated over 80 interviews and supported 25+ successful placements from intake to start date.
- Improved candidate quality by refining screening and submission processes, reducing unqualified pipeline volume by 40 percent.
- Increased candidate engagement and response rates through structured communication and follow-up methods.

Oceanside Motorsports, Inc — Oceanside, CA **Dec 2025 – Present**

IT & AI Systems *Dec 2025 – Present*

- Architected the enterprise knowledge base and agent policy layer behind the staff AI assistant, with every process documented, one live source of truth, and answers returned with citations.
- Deployed a self-hosted MCP client inside the company's own cloud tenancy, connecting AI tooling to the CRM and knowledge base with no data leaving to third-party infrastructure.
- Centralized authorization in a single policy store across every AI surface with event-driven propagation, governing self-service capability requests through review.
- Rebuilt the talent acquisition pipeline end to end: stood up the company's own candidate database, developed the talent bench from nothing, and cut time spent on screening and interview coordination through automation.
- Redesigned the careers front-end and social presence, raising inbound applicant volume on every open role.

- Instrumented a closed-loop voice-of-customer program: built the database behind post-service follow-up calls, and routed that data into an AI training corpus wired to the knowledge base.
- Consolidated learning management into a single system for courses, software guides, and process training.
- Automated employee onboarding and recurring HR operations, and wired social content distribution directly into the sales pipeline.
- Administer the Google Workspace tenant (provisioning, groups, access management) on cloud-native, free-tier infrastructure at zero recurring cost.
- Identified and remediated a critical unauthenticated privilege escalation vulnerability: privileged backend functions (set any user's role, strip 2FA, purge any user) were exposed on the public API with no login required. Removed from the public surface and enforced least-privilege default provisioning. CVSS 9.8.
- Identified and remediated an unauthenticated PII exposure: 134 lead records returned from a request with no login, caused by a tenant helper treating "no identity" as "server identity." Replaced with a member-gated check and swept the pattern across the app. CVSS 7.5.
- Identified and remediated a privilege escalation vulnerability allowing any viewer to grant themselves full system permissions via a writable shared policy store and a service-identity bypass on enforcement routes. Locked the store and restored role checks. CVSS 8.8.
- Results: closed the year at $1.2M revenue, projecting $1.8M. Automated four processes that previously required a dedicated person — hiring pipeline, employee onboarding, post-service customer follow-up, and social-to-sales distribution.

PROJECTS

- **Legion Warden** (private, walkthrough on request) — Desktop application controlling the runtime environment AI coding agents live in. Agents deploy into local Docker containers instead of cloud VMs; sessions seed from real browser cookies for authenticated automation; flows recorded once and replayed on demand; per-environment configuration for any provider, model, or target.
- **agent-pods** (github.com/jgharbieh/agent-pods) — Containerized browser isolation for parallel AI coding agents: isolated Chromium container per agent, own CDP port, noVNC window for live observation, and cookie injection for authenticated flows.
- **inTrack** — CI/CD verification pipeline for AI-generated pull requests: builds and boots the app in a pinned container, probes declared endpoints, replays a recorded UI baseline and diffs it, optionally runs a budget-capped AI agent against the live app, and posts pass/fail findings on the PR. Includes a config-gated OWASP Top 10 security scanner with a baseline/ratchet system. Personal project, pre-hardening.
- **oceansidemotorsports.com** (in progress) — Full rebuild of the shop's site: animated landing page, React components, version-controlled with an automated deploy pipeline and a non-technical content editing interface.

EDUCATION & CERTIFICATIONS

CompTIA Network+ — Certified (Networking, Protocols, Infrastructure)

Germanna Community College — Associate Degree, Cybersecurity (Jan 2023 – May 2025)

Culpeper Technical Education Center — Two-year Cybersecurity program, Computer & Information Systems Security / Information Assurance (Aug 2021 – Dec 2023)