

Joseph Gharbieh

Application Security & AI Systems Engineer

🏠 Oceanside, CA

📞 (540) 729-8609

✉️ jgharbieh32@gmail.com

🏠 Oceanside, CA 📞 (540) 729-8609 ✉️ jgharbieh32@gmail.com 🔗 [linkedin.com/in/joseph-gharbieh](https://www.linkedin.com/in/joseph-gharbieh) 🐙 github.com/jgharbieh

ABOUT ME

I build technology that gives people their time back and hands them capability they did not have yesterday. That is the work I care about, and I bring real energy to it, because watching a team suddenly move faster because of something I made is the part that never gets old.

I have hired for companies, run their operations, and hardened their software against the attacks nobody else was watching for. So when I build, I am not guessing at how the work actually gets done. I walked that experience, and I put it behind every system I ship.

AI just raised the ceiling on what a small team can do, and most companies have not reached it yet. I want to be the one who brings them there the right way: fast, secure, and owned by the people using it. Give me a problem and I will find the way through, and leave everyone around it stronger than I found them.

Open to full time and contract-based roles.

EDUCATION & CREDENTIALS

CompTIA Network+

Certified
NETWORKING, PROTOCOLS,
INFRASTRUCTURE

Germanna Community College

Associate Degree, Cybersecurity
JAN 2023 to MAY 2025

Culpeper Technical Education Center

Two-year Cybersecurity program.
Computer & Information Systems Security
/ Information Assurance
AUG 2021 to DEC 2023

EXPERIENCE

MTS Moose Tech Solutions L.L.C.

JUN 2023 TO PRESENT · OCEANSIDE, CA

Application Security & AI Systems Engineer

JAN 2026 to 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 role-based access control (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.
 - ◇ Role hierarchy enforcement, permission sets, and the propagation logic that keeps one policy change meaning the same thing everywhere.
- ◆ **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 the output rather than trust it.

Technical Recruiter

JUN 2023 to 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

DEC 2025 TO PRESENT · OCEANSIDE, CA

IT & AI Systems

DEC 2025 to PRESENT

- ◆ **Deliver AI enablement** in the most digestible, user friendly form the staff will actually use, with professional grade functionality underneath it.
 - ◇ Architected the enterprise knowledge base and the agent policy layer behind the staff AI assistant: every process documented, one live source of truth, 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, and governed self-service on top of it: staff request a capability, it goes through review, it lands access scoped for everyone.
- ◆ **Rebuilt the talent acquisition pipeline** end to end.
 - ◇ Stood up the company's own candidate database and developed the talent bench from nothing.
 - ◇ 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.**
 - ◇ Post-service follow-up calls capture customer feedback. Built the database behind them and improved it systematically.
 - ◇ Routed that data into an AI training corpus wired to the knowledge base, turning real customer feedback into technician training material.
- ◆ **Consolidated learning management** into a single system: courses, software guides, and process training staff actually use.
- ◆ **Modernizing the public site** on version control with an automated deploy pipeline and a non-technical content editing interface. (*in progress*)
- ◆ **Automated employee onboarding** and recurring HR operations, and wired social content distribution directly into the sales pipeline.
- ◆ **Administer the Google Workspace tenant:** provisioning, groups, and access management. Entire platform runs cloud native on free tier infrastructure at zero recurring cost.

RESULTS

- ◆ **Anyone on the internet could have made themselves an admin.** Privileged backend functions were sitting on the public API with no login required: set any user's role, strip any account's 2FA, purge any user. Pulled them off the public surface and cut default provisioning to least privilege. CVSS 9.8
- ◆ **134 lead records with PII came back to a request with no login on it.** A tenant helper read "no identity" as "this is the server." Replaced it with a member gated check and swept the pattern across the app. CVSS 7.5
- ◆ **A viewer could grant their own role every permission in the system.** The policy store both enforcement layers read was writable by any member, and API routes calling under a privileged service identity skipped the gate entirely. Locked the store, restored role checks on the routes that were bypassing. CVSS 8.8
- ◆ **Closed the year at \$1.2M and projecting \$1.8M.** Increased operational efficiency, reduced new-hire training time, improved processes, and systematically drawing in more customers.
- ◆ **Four processes that used to need a person now run unattended.** Hiring pipeline, employee onboarding, post-service customer follow-up, and social to sales distribution.
- ◆ **Nobody has to find the right person to get an answer anymore.** Staff ask, and it comes back cited, in seconds.

PROJECTS

Legion Warden

PRIVATE · WALKTHROUGH ON REQUEST

- ◆ A desktop application that controls the runtime environment AI coding agents live in. Isolated, focused, and configurable to any target domain.
- ◆ **Run long-running agents without standing up a VM.** Agents deploy into your own Docker image instead of a cloud machine, light enough to run on hardware you already have, so an agent working for hours costs nothing but the tokens.
- ◆ **Hand an agent a real session and let it do real work.** Cookies seed in from your actual browser, so the agent operates as the authenticated user rather than as a bot fighting its way in, inside a sandbox that cannot reach your real browser.
- ◆ **Get repeatable automation without writing a script.** A flow driven once is recorded and replays on demand, so production runs stop paying an agent to rediscover a path it already knows. Script-first automation, without building a single script.
- ◆ Configuration is per environment: any provider, any model, any target. Secrets live in a store the agent references but never reads.
- ◆ Runs on **agent-pods** (below), which supplies the isolated browser containers underneath it.

agent-pods

[GITHUB.COM/JGHARBIEH/AGENT-PODS](https://github.com/JGHARBIEH/AGENT-PODS)

- ◆ Containerized browser isolation for parallel AI coding agents. Agents sharing one browser corrupt each other's sessions. agent-pods gives each an isolated Chromium container, its own CDP port, a noVNC window for live observation, and cookie injection for authenticated flows. Git worktrees isolate the code. This isolates the browser.

- Rebuilding the shop's site from the ground up: an animated landing page, React components, and an immersive experience built to actually hold a visitor. Shipping on version control with an automated deploy pipeline and an editing interface the staff can use without me.

SKILLS

AI ENGINEERING & ENABLEMENT	LEVEL
AI-directed development at production scale	PROFESSIONAL
Prompt engineering	PROFESSIONAL
AI enablement tooling	PROFESSIONAL
Agent sandboxing & parallel execution	PROFESSIONAL
LLM API integration (Anthropic, OpenAI)	PROFESSIONAL
Conversational AI & AI-powered application development	INTERMEDIATE
MCP client development, hosting & access control	PROFESSIONAL
Browser automation & CDP	INTERMEDIATE
AUTOMATION & PIPELINE DESIGN	LEVEL
GoHighLevel pipeline & workflow design	PROFESSIONAL
Workflow automation (Make.com)	ADVANCED
Twilio, telephony & SMS systems	INTERMEDIATE
A2P 10DLC registration & carrier compliance	INTERMEDIATE
DATA & KNOWLEDGE SYSTEMS	LEVEL
Enterprise knowledge base architecture	PROFESSIONAL
RAG (retrieval augmented generation) system design	INTERMEDIATE
Data repatriation from vendor systems	INTERMEDIATE
Operational data analysis & closed-loop feedback	INTERMEDIATE
APPLICATION SECURITY	LEVEL
RBAC design, enforcement & propagation	PROFESSIONAL
Authorization enforcement & privilege context analysis	PROFESSIONAL
Trust boundary & data classification design	PROFESSIONAL
Default deny & secure failure modes	PROFESSIONAL
Identity & access management (Google Workspace, M365)	PROFESSIONAL
Broken access control (IDOR/BOLA, privilege escalation, authz bypass)	INTERMEDIATE
Multi-tenant isolation & cross-tenant leak remediation	INTERMEDIATE
Authentication & session architecture	INTERMEDIATE
Row level scoping / RLS patterns	INTERMEDIATE
XSS, open redirect & input validation	INTERMEDIATE
OWASP Top 10 & CVSS v3.1 scoring	INTERMEDIATE
Networking, protocols & infrastructure (Network+)	INTERMEDIATE
ENGINEERING	LEVEL
Root cause debugging & performance profiling	PROFESSIONAL
Browser DevTools & client-side debugging	INTERMEDIATE
TypeScript / JavaScript	INTERMEDIATE
React / Next.js (App Router)	INTERMEDIATE
Convex	INTERMEDIATE
Node.js / Express	INTERMEDIATE
SQL & schema design	INTERMEDIATE
REST & webhook integration	INTERMEDIATE
Front-end implementation & UX	INTERMEDIATE
Electron	INTERMEDIATE
SYSTEMS & DELIVERY	LEVEL
Docker & containerized environments	INTERMEDIATE
Git / version control	INTERMEDIATE
Cloud cost optimization	INTERMEDIATE
Cloudflare, Google Cloud, Vercel	INTERMEDIATE
CI/CD design & automated deploy pipelines	INTERMEDIATE
Linux	INTERMEDIATE
PLATFORMS	LEVEL
Google Workspace administration	PROFESSIONAL
Google Workspace & Microsoft Office suites	PROFESSIONAL
Microsoft 365 administration & support (Excel, Word, tenant ops)	ADVANCED
Tekmetric, ClickUp, Slack, Discord	PROFESSIONAL