Jose Hernandez

josehernandez.dev | github.com/jhern603 | Austin, TX

jhern603@gmail.com | +1 786-357-8107

Open to Relocation

Summary

AI Security Engineer with experience securing AI platforms, agentic systems, and developer tooling. Designed and shipped a production Model Context Protocol (MCP) service enforcing permission-based LLM access and data-boundary controls across multiple enterprise knowledge sources. Defined security standards and guardrails for agentic tooling as technical lead on a enterprise wide AI adoption program. Rearchitected enterprise Data Loss Prevention (DLP) platform into a modular, policy-based system.

Technical Skills

AI Security: Agentic AI Security, LLM Access Governance, Model Context Protocol (MCP) Security, AI Guardrails, Prompt Injection Mitigation, RAG Security, LLM Evaluation Frameworks

Security Engineering: Data Loss Prevention (DLP), Role-Based Access Control (RBAC), Data-Boundary Enforcement

Languages: Python, Java, Go, Bash, Oracle SQL/PL-SQL, JavaScript

Cloud & Infrastructure: Oracle Cloud Infrastructure (OCI), Kubernetes, Terraform, Docker, Linux/Unix

Observability & Detection: Prometheus, Grafana, OCI Logging, Log Mining, Monitoring

Experience

Deloitte Austin, TX

Software Engineer II | Secret Clearance *October 2026 – Current*

- Delivered a Salesforce-style outreach platform for medical plan eligibility in GPS, meeting core requirements for multichannel communication across email, SMS, and phone.
- Reviewed AI-generated code, tests and documentation for accuracy and completeness against requirements before merge, keeping quality high.
- Built and deployed AWS infrastructure with Terraform, supporting repeatable, reliable releases across Agile sprints with engineering, QA and product teams.

Oracle — Oracle Cloud Infrastructure Austin, TX

Software Engineer *July 2024 – March 2026*

- Designed and shipped production Model Context Protocol (MCP) service enforcing permission-based LLM access across multiple enterprise knowledge sources, with data-boundary enforcement and access controls that prevented unauthorized data exposure through AI interfaces.
- Served as technical lead on a corporate-wide AI Adoption program; partnered with security architects to define security standards and guardrails for agentic tooling, embedding safe-use controls into internal developer workflows.
- Rearchitected monolithic PL/SQL Data Loss Prevention (DLP) platform into a modular, policy-based, fully automated system which simplifies policy management and enabling faster, safer iteration on data-protection rules.
- Designed a Unified MCP Gateway centralizing governed access to enterprise knowledge behind a single policy-enforced interface, reducing access-control complexity and configuration risk for product teams.

– **Impacted by large scale reduction in force**

Software Engineer Intern *May 2023 – August 2023*

- Reduced CI/CD build times from several hours to under 10 minutes by parallelizing test execution and optimizing dependency resolution, accelerating production release cycles.
- Built mock OCI service integrations to simulate real user requests against OCI Kubernetes Engine (OKE) operations, enabling full prerelease validation without live infrastructure changes.

Florida International University Miami, FL

Junior Webmaster *February 2024 – June 2024*

- Deployed an LLM-powered support ticket summarization tool using prompt engineering and generative AI APIs, reducing manual ticket review time for the IT team and improving triage throughput.
- Maintained and extended the CS department website using PHP and WordPress.

Student IT Assistant *March 2022 – February 2024*

- Conducted regular security testing via pentesting to ensure website and onsite infrastructure is secure and resilient against cybersecurity incidents.
- Overhauled the campus monitoring solution to simplify log ingestion and significantly reduce mean time to diagnosis across the KFSCIS network.

Military Experience

US Army

Biomedical Equipment Technician | Secret Clearance *May 2017 – May 2023*

- Managed accountability and audit of over $2M in medical and non-medical equipment across multiple operational contexts.
- Trained 100+ personnel at an overseas combat support hospital in equipment operation, care, and maintenance protocols under operational conditions.