Jonathan R. Reed

Security Engineering | AI Security | IT Infrastructure | Secure Deployment

contact@jonathanrreed.com | Dallas, TX | JonathanRReed.com | github.com/JonathanRReed | linkedin.com/in/jonathanrreed0

Security-minded technical operator working across IT infrastructure, access control, AI red teaming, secure deployment, and workflow hardening. Strong fit for security engineering, application security, AI security, customer security, and infrastructure roles that value practical implementation, user support, and risk reduction.

Experience

Reed & Terry, L.L.P. | IT & Security Lead | Jun 2023 - Present

- Own IT/security operations for a confidentiality-sensitive law firm, including servers, networks, endpoints, cloud services, backups, permissions, and support workflows.
- Implemented MFA, least-privilege access, patching, endpoint standards, access reviews, and recovery planning, reducing avoidable access and endpoint risk by 25%.
- Deployed secure on-prem and cloud AI retrieval/drafting workflows with data-boundary controls, human review, permissions discipline, and maintainable runbooks.
- Harden document handling, collaboration, backup, and recovery workflows while keeping attorney and staff productivity intact.

Hello.World Consulting | Founder & AI Security Consultant | Jul 2022 - Present

- Lead AI red teaming, architecture review, and hardening work for LLM/RAG systems, focusing on prompt injection, data leakage, unsafe tool use, and rollout failure modes.
- Build private RAG and local LLM workflows with access controls, logging boundaries, retrieval tuning, and documentation for cleaner handoff.
- Reduced exploit success and policy bypasses by 35% in tested systems and cut third-party inference exposure through local/private-cloud deployments.
- Translate findings into prioritized remediation plans that teams can implement, retest, and maintain.

Podium Education | Team Lead, AI Programs | Dec 2025 - Present

- Teach risk-aware AI use, prompt hygiene, and data handling to 400+ students while supporting AI integrations and program operations.
- Created feedback methods that reduced grading turnaround by 31% and improved rubric clarity across student projects.

Methodist Dallas Medical Center | EMT-B, Emergency Department Intern | Aug 2024 - Dec 2024

- Worked repeated 12+ hour ER and ambulance shifts, strengthening risk triage, documentation discipline, and high-pressure communication.

Selected Projects

RAGFuzz | AI security testing | GitHub: github.com/JonathanRReed/RAGFuzz

- Testing project for probing RAG behavior, prompt injection risk, and retrieval failure cases before deployment.

PoliBench | Astro, React, Bun, Convex | GitHub: github.com/JonathanRReed/Poli-bench

- Model-behavior benchmark with answer receipts, official-run gates, parse quality, refusal behavior, policy posture, and audit artifacts.

TRACED | Astro | Live: traced.jonathanrreed.com | GitHub: github.com/JonathanRReed/traced

- Security archive and password-exposure tool built around public breach data, privacy-preserving checks, and clearer incident context.

Prompt Info | Next.js, TypeScript | Live: prompt-info.helloworldfirm.com | GitHub: github.com/JonathanRReed/prompt-info

- Prompt inspection tool for token, payload, and cost review before model execution.

Education

The University of Texas at Dallas, B.A. Sociology, Expected 2027 | EMT-B Certificate, UT Dallas/UEMR, Grade A | Wharton County Junior College, Core Curriculum, GPA 3.35

Selected Certifications & Recognition

Google Cybersecurity coursework (Python automation, detection/response, Linux/SQL, network security, assets/threats/vulnerabilities); Cybrary Penetration Testing Professional; Microsoft Security Essentials.

IBM AI Engineering Professional Certificate; Red Teaming for Generative AI; Docker Foundations; GitHub Career Essentials; Multi-time Gray Swan Arena top-five.

Skills

Threat modeling; prompt-injection testing; IAM; least privilege; vulnerability testing; red teaming; detection and response; network security; cloud security; Python; Linux; SQL; Docker; backups/recovery; incident response; AI/LLM security.