

Joshua Whitney

Offensive Security Engineer | AI Engineering | Red Team Operations

 Knoxville, TN  Military Veteran  joshwhitney.com  <https://www.linkedin.com/in/joshmwhitney>

PROFILE

Senior Cyber Security Engineer specializing in offensive security, red team operations, AI engineering, and security automation. Experienced in independently leading complex security assessments, architecting custom tools and infrastructure, and developing AI-driven solutions to enhance operational efficiency. Proven technical leader with expertise in mentoring security professionals, optimizing assessment workflows, and translating emerging technologies into innovative cybersecurity services.

CERTIFICATIONS

- CPTS (Certified Penetration Testing Specialist)
- MCRTE (Microsoft Certified Red Team Expert)
- CRTO (Certified Red Team Operator)
- CRTP (Certified Red Team Professional)
- CRTE (Certified Red Team Expert)
- PNPT (Practical Network Penetration Tester)

TECHNICAL SKILLS

- Offensive Security: Internal/External Penetration Testing, Red Team Operations, Social Engineering, Cloud Security Assessments
- AI Engineering: AI-Assisted Security Testing, LLM Integration, Claude SDK, OpenRouter, Dreadnode
- Development: Python, TypeScript, React, FastAPI, PostgreSQL, REST APIs
- Infrastructure & Security: Docker, Cloudflare, Garage S3, Google OAuth, Argon2, Security Automation

PROFESSIONAL EXPERIENCE

11/2024 – Present
Remote, U.S

- Senior Cyber Security Engineer**, Hacket Cyber
- Independently lead end-to-end offensive security engagements, including internal and external penetration testing, red team operations, social engineering, and cloud security assessments across AWS, Azure, and GCP.
 - Architect, deploy, and maintain red team, social engineering, and supporting business infrastructure while developing custom security tools, scripts, and automation to improve assessment execution and operational efficiency.
 - Solely architected and developed **ODIN**, a comprehensive penetration testing management platform currently in internal beta testing, integrating engagement scoping, client management, secure communications, file sharing, reporting, and invoicing into a centralized workflow.
 - Spearheaded the introduction of a commercial AI-assisted penetration testing service, contributing to the development of custom capabilities within the Dreadnode platform and researching emerging AI technologies for offensive security applications.
 - Drive operational improvements through custom reporting solutions, automated workflows, standardized pre-engagement data collection, and streamlined client communications.

- Provide technical leadership through employee onboarding, hands-on training, ongoing mentorship, and collaborative project oversight, supporting the professional development and operational effectiveness of fellow security engineers.
- Independently manage client engagements from initial planning and scoping through technical execution, reporting, and remediation guidance, while advising clients and supporting sales teams in identifying appropriate security assessments and emerging service opportunities.

2022 – 2024
Remote, U.S.

Help Desk Manager - LXGE, Omni Interactions

- Led a team of 600 help desk technicians, overseeing technical operations, employee training, performance management, and service delivery.
- Improved support resolution times by 30% through standardized procedures and reduced repetitive support requests by 80% through the implementation of an AI-powered knowledge base.

2021 – 2022
Remote, U.S.

Help Desk Tier 2 - SME, Arise

- Served as a technical subject matter expert, resolving complex IT issues, mentoring support personnel, and collaborating with engineering teams to improve system reliability and operational efficiency.

2006 – 2021
Remote, U.S.

Owner / Operator, JLM Consulting

- Provided IT consulting and technology advisory services, developing strategic roadmaps and recommending infrastructure improvements, process automation, and cloud solutions to improve client operations.

2002 – 2006
Hawaii, U.S.

Air and Missile Defense Command, U.S. Army

- Operated, maintained, and troubleshoot mission-critical military technology, including radar, command-and-control systems, and network infrastructure, while collaborating with military leadership to support operational readiness.

PROJECTS

ODIN | Founder, Architect & Lead Developer, Penetration Testing Management & Automation Platform — Internal Beta

- Independently designed, architected, and developed a full-stack cybersecurity platform managing the entire penetration testing lifecycle, from client onboarding, scoping, and rules of engagement through assessment execution, reporting, and invoicing.
- Engineered secure client portals, role-based access controls, authentication and password hashing, encrypted file sharing, automated document generation, and centralized engagement workflows using modern application frameworks and cloud infrastructure.
- Integrated AI services and LLM capabilities into a modular architecture designed to automate operational tasks, streamline reporting, enhance client collaboration, and support future AI-driven security assessment workflows.

Technologies: Python, TypeScript, React, FastAPI, PostgreSQL, Docker, Cloudflare, Argon2, Google OAuth, Garage S3, SuperDoc, Resend, OpenRouter, Anthropic Claude SDK.

EDUCATION

Remote, U.S.

Full Sail University, Mobile Application Design & Development

Davie, FL, U.S.

Nova SouthEastern, Computer Networking

Remote, U.S.

Capella University, Criminal Justice / Security Management