

JASON HENRY

Augusta, GA • (762) 333-5369 • jason@jhenry.io • jhenry.io

SUMMARY

Cybersecurity training leader with 10+ years across program design, curriculum development, and direct team leadership. Built training pipelines and outcome metrics for 60+ direct reports (25% reduction in Time to Train) before scaling into end-to-end curriculum ownership for DoD cyber forces. Built Praxis, a multi-agent AI platform that auto-generates incident-response training scenarios from threat intelligence — proof that AI-assisted tooling can accelerate content development without sacrificing rigor. Practitioner background in SOC operations, incident response, and security architecture lends immediate credibility with technical teams. GIAC- and CompTIA-certified; active TS/SCI clearance with CI Polygraph.

EXPERIENCE

U.S. Army Cyber School

Cybersecurity Course Instructor & Curriculum Developer

Fort Gordon, GA

July 2021 – Present

- **Own end-to-end training program lifecycle** for 400+ cybersecurity professionals across 4 training cohorts annually — needs analysis with mission partners, curriculum design, content development, instruction, and outcome assessment.
- **Translate operational performance gaps** identified by leadership and mission partners into structured, prioritized learning initiatives; maintain a living curriculum backlog so programs reflect current adversary tradecraft rather than static content.
- **Partner with subject matter experts** across Army, Marine Corps, Air Force, and Navy cyber communities to develop technically accurate content, structuring the design work so SMEs contribute expertise without carrying the instructional design burden.
- **Design assessment frameworks** aligned to DoD JQR/JQS standards that validate practitioner readiness against operational tasks — measuring qualification outcomes, not just course completion.
- **Mentor junior instructors and cadre members** through co-teaching, scenario reviews, and curriculum development partnerships, growing their ownership of program content over time.
- **Anchor curriculum in operational reality** by planning and executing 400+ hours of exercises annually against live DoD networks, using Splunk SIEM workflows, MITRE ATT&CK-mapped TTPs, and realistic SOC scenarios.

U.S. Army Cyber Protection Brigade

Computer Network Defense Analyst

Fort Gordon, GA

October 2020 – July 2021

- Performed SOC-style analysis within an EUCOM/NATO cyber defense mission — incident response, host and network investigation, and threat characterization across Windows and Linux enterprise environments.
- Investigated suspicious activity and potential intrusions; analyzed application behavior and network traffic patterns to identify malicious indicators; documented IOCs aligned to known threat actor TTPs.
- Conducted vulnerability assessments, prioritized remediation actions, and performed digital forensics and malware artifact triage (static/dynamic fundamentals) to support attribution.

782nd Military Intelligence Battalion, 106 CMT

Enlisted Team Lead

Fort Gordon, GA

July 2015 – June 2019

- **Designed training pipelines and progress-tracking metrics** for 60+ team members across 7 work roles, reducing Time to Train by 25% and accelerating mission readiness.
- **Led and mentored 60+ direct reports**, coordinating training development, administrative, and operational requirements across 3 mission elements conducting offensive cyberspace operations.

- Coordinated with higher headquarters for operational and administrative deconfliction, improving cross-leadership communication and program execution efficiency.
- Performed SIGINT/DNEA target development, translation, and analysis of language-specific technical data supporting priority operational missions.

SELECTED PROJECTS

Praxis - AI-Driven Cybersecurity Training Platform

github.com/jhenrysec/praxis

- Designed and built a multi-agent AI platform that ingests adversary whitepapers and auto-generates incident-response training scenarios, demonstrating AI as a force multiplier for instructional design at scale.
- Architecture composes specialized agents — intelligence ingestion, infrastructure provisioning, content generation, security validation, and orchestration — converting raw threat reporting into ready-to-deliver training environments without manual scenario authoring.
- Authored Terraform, Packer, Ansible, and Docker automation to provision isolated multi-VM training ranges on demand, enabling rapid curriculum iteration; delivered iteratively in agile phased rollouts with Git-versioned configurations.

EDUCATION

SANS Technology Institute

North Bethesda, MD

M.S., Information Security Engineering

Expected 2028

Post University

Waterbury, CT

B.S., Business Administration

2019

Cochise College

Sierra Vista, AZ

A.A.S., Intelligence Operations Studies

2019

CERTIFICATIONS & TECHNICAL SKILLS

- **Certifications:** GIAC GDSA, GSTRT, GCIH, GSEC; CompTIA Pentest+, CySA+
- **Training & Enablement:** Curriculum design and lifecycle ownership; needs analysis; assessment framework design (DoD JQR/JQS); SME collaboration; AI-assisted content development
- **Cybersecurity Operations:** SOC workflows, incident response, Splunk SIEM, MITRE ATT&CK, vulnerability assessment, digital forensics, network defense
- **Infrastructure & Automation:** Terraform, Packer, Ansible, Docker; Proxmox VE, VMware; Git/GitHub
- **Scripting (10+ yrs):** Python, Bash, PowerShell, Go; Windows and Linux administration; application behavior and network traffic analysis