Adam Van Nostrand

Columbia, SC | (423) 383-0123 | adamvannostrand@gmail.com
linkedin.com/in/adam-van-nostrand-5a603424b/ | github.com/advannostrand

PROFESSIONAL SUMMARY

IT engineer and final security escalation point across 74 client organizations and 600+ endpoints. Detected and contained a live ScreenConnect RAT intrusion, documenting 349 credential-harvest events the $30K incumbent MDR missed. CompTIA trifecta (A+, Network+, Security+) plus a DoD cyber internship at USAFRICOM. Builds production AI tooling through AI-accelerated development: architect, direct, and verify, never ship unverified code.

TECHNICAL SKILLS

Security: Detection engineering, incident response, digital forensics (KAPE), vulnerability management, NIST RMF, HIPAA security, MITRE ATT&CK

Systems & Identity: Microsoft 365, Entra ID, Intune, ThreatLocker, Defender for Endpoint, ConnectWise Manage, NinjaOne, PowerShell, RMM platforms

AI & Automation: RAG pipelines, LangGraph, Ollama, pgvector, FastAPI, Docker, Whisper, LLM evaluation, AI-assisted development

EXPERIENCE

Blencowe IT (Lyra Technology Group)

IT Engineer | Sep 2025 - Present | Columbia, SC

- Detected, investigated, and contained a live ScreenConnect RAT intrusion, documenting 349 credential-harvest events with KAPE and PowerShell; the investigation outperformed the incumbent $30K/year Sophos MDR.
- Final escalation point for every security event across 74 client organizations and 600+ endpoints in a 9-technician MSP: detection engineering over alert triage.
- Own the identity and endpoint security stack: Entra ID, Intune, ThreatLocker, and Defender for Endpoint; drove the RMM platform migration.
- Authored the AI governance framework (NIST AI RMF, EU AI Act) adopted by Colliers International SC; wrote four security policies (encryption, DLP, network security, backup and retention) accepted by Truist Bank as vendor compliance evidence.
- Operate a ConnectWise MCP server and the "cwadmin" dashboard in daily production use across the technician team.

Digital Technology Partners

Systems Administrator | Oct 2023 - Sep 2025 | Columbia, SC

- One of the final escalation points for 500+ HIPAA-regulated dental offices across the Southeast.
- Wrote PowerShell automation and standardized RMM tooling that cut repeat tickets and kept the fleet within HIPAA compliance baselines.
- Investigated endpoint and identity incidents with real regulatory stakes, building the IR fundamentals carried into the Blencowe role.

Aug 2022 - Oct 2023: Relocated from Stuttgart, Germany to the United States; worked part-time while studying for CompTIA certifications and transitioning into full-time IT work.

USAFRICOM J62 / SOCAFRICA

Cybersecurity Intern (Volunteer, 800+ hours) | Aug 2021 - Aug 2022 | Stuttgart, Germany

- Ran facility walkthroughs verifying device separation and hunting unauthorized devices; one finding formally reported to the Stuttgart field office.
- Key member of the IG inspection preparation: emanations screening across hundreds of endpoints plus color-coded compliance labeling of systems.
- Completed HBSS training and privileged-user training for SIPRNet systems; performance led the supervisor to pursue a GS-12 federal position for continued service.

INDEPENDENT PROJECTS

Mitsumeru

- Self-hosted, local-first RAG for MSP support (FastAPI, LangGraph, pgvector, Ollama, Docker). Built solo in 9 business days and evaluated against 98,000+ production support tickets. MIT-licensed: github.com/advannostrand/Mitsumeru.

Nine-Model LLM Benchmark

- One-shot evaluation of 9 frontier models building a real-time 3D physics engine; every result graded pass/fail against objective criteria and written up as a 29-page paper. Repository starred by researchers at MIT, Johns Hopkins, UCLouvain, and the Czech Academy of Sciences.

THE WIRE

- Automated video pipeline where chat-spike detection gates an LLM scoring pass, Whisper transcription is metered against per-channel spend caps, and a two-pass ffmpeg render produces finished vertical video. Runs across two hosts under supervisor with a dashboard and cost breakers, at about $18/month per channel.

Hermes

- Personal AI operations agent that runs pipelines overnight and reports over Signal; built on a pay-per-call model with judgment about what is worth waking a human for.

CERTIFICATIONS

- CompTIA A+, Network+, Security+ (all active)
- In progress: Microsoft SC-300 (Identity and Access Administrator), AZ-500 (Azure Security Engineer)