Kyle Nehman

kyle@nehman.dev | (410) 758-7196 | Pittsburgh, PA | nehman.dev

SKILLS

Languages: Rust, C, C++, Python, x64/PPC Assembly, JavaScript, TypeScript, Java, Groovy

Security: Reverse Engineering, Malware Analysis, IDS/IPS, Protocol Analysis, Ghidra, Binary Ninja

Infrastructure: AWS, GCP, Docker, Kubernetes (K8s), Data Center Operations, CI/CD

Systems: Windows Kernel (WDK), Linux Kernel Modules, Embedded, Win32 API, OS Development

Full-Stack: React, WebRTC, REST APIs, Mobile (iOS/Android), NLP, MongoDB Sharding

EXPERIENCE

Cyber Crucible
December 2016 – October 2025

Co-Founder & CTO

- Co-founded endpoint security company; architected and built complete product from zero to market
- Developed Windows kernel driver using WDK in C/C++ (no CRT) for endpoint security solution
- Built ML-powered network IDS that automatically reverse engineers and decrypts malware C2 traffic in real-time
- Developed custom 10Gbps PF_RING Linux kernel driver for high-performance packet capture
- Led malware reverse engineering across x64, PPC, and ARM architectures using WinDbg and custom tools
- Architected and executed infrastructure migrations from AWS/GCP to physical data center colocation

Squire Solutions
Jan 2018 – Nov 2021, May 2024 – Sept 2025

Original Systems Developer & Technical Consultant

- Created original software systems in Rust: full-stack web app, backend services, distributed systems, custom NLP pipeline
- Developed SMF (abstracted messaging framework) with P2P protocol; implemented WASM and Android/ARM bindings
- Built Android application with ATAK integration for tactical communications

ECS Federal
August 2025 – October 2025

Contracted Data Scientist & AI Consultant

- Built AIGINT custom AI engine for intelligence analysis with async multitenant governance platform featuring custom algorithms, LORA fine-tuning, and RAG systems

PERSONAL PROJECTS

Custom Game Engine: Low-level C++ and Jai with OpenGL. Custom physics, entity systems, audio, input handling.

SSBM Triples Mod: Reverse engineered PPC GameCube rendering and OOP. Shellcode injection for character select, hitboxes, player 5/6 support.

Endpoint Management & Task System: Multi-endpoint patch/software management. Windows kernel driver, userspace service, shared memory IPC, WebSocket/REST backend.

Bare-Metal Raspberry Pi OS: Zero deps OS. Multicore, TTY over UART, scheduler, storage, monokernel, bootloader. Linux/NT hybrid architecture.

EDUCATION

University of Maryland, Baltimore County (UMBC) - Bachelor of Science in Computer Science

PATENTS

- **Systems and Methods for Ransomware Detection and Mitigation** - US PCT/US20/42924 (2020)
- **System and Method for Highly Efficient Information Flow Using NLP and Speech Recognition** - US 62/901259 (2019)
- **Systems And Methods For Ransomware Detection And Mitigation** - US 62/877748 (2019)