Christopher W. Nowak

Security Engineer — Vulnerability Assessment & Cloud Identity Security

(704) 806-1807 | chris@nowaksolutions.com | linkedin.com/in/christopher-nowak-71a351162 | nowaksolutions.com

Security-focused technology professional with a U.S. Marine Corps background, pursuing an M.S. in Information Security Engineering and building toward vulnerability research and security engineering roles. Fully DoD 8570/8140 baseline qualified, alongside GSEC, CySA+, PenTest+, and SecurityX (CASP+ CE). Investigates and remediates identity, access, and endpoint security issues across Microsoft cloud environments, and runs a self-hosted lab performing vulnerability assessments, log analysis, and adversary-simulation exercises, including a Kubernetes/Docker honeypot for attacker behavior analysis.

CORE SKILLS

Vulnerability Assessment & Management • Security Testing & Analysis (CySA+, PenTest+, SecurityX) • Identity & Access Security (Azure AD/Entra ID, IAM) • SIEM & Log Analysis • Incident Investigation & Response • Container & Cloud Security (Kubernetes, Docker, Azure) • Network Security (TCP/IP, VPN, Firewall, IPsec/SSL) • PowerShell & Scripting (Fundamentals) • Infrastructure as Code (Familiar) • NIST-Aligned Practices • DoD 8570/8140 Compliance

PROFESSIONAL EXPERIENCE

Service Desk Analyst — Summit 7 Systems (Remote)

May 2026 – Present

- Investigate and remediate identity, access, and endpoint security issues across Azure AD (Entra ID), Microsoft 365, and Intune in a Microsoft-focused MSP environment
- Support Azure Virtual Desktop (AVD) infrastructure and Exchange Online, troubleshooting connectivity, access, and configuration issues within SLA targets
- Enforce least-privilege access controls and safeguard Controlled Unclassified Information (CUI) across Microsoft cloud and endpoint systems

Technical Support Analyst I — PAR Technology (Remote)

Jan 2026 – May 2026

- Performed structured incident analysis on POS and enterprise systems, identifying root cause and enforcing least-privilege access across user accounts
- Troubleshot hardware, software, and network issues across POS and enterprise systems while ensuring secure handling of customer data

Compliance & Systems Operations Manager — CarrierIQ Freight LLC (Nashville, TN · Hybrid)

Aug 2024 – Dec 2025

- Audited compliance and fleet management systems, identifying data integrity issues and enforcing regulatory controls across cloud platforms
- Managed the Tenstreet LMS platform, auditing electronic logs and coordinating secure training content delivery

Maintenance Operations Manager & Training Specialist — U.S. Marine Corps (Japan & U.S.)

Dec 2018 – Dec 2024

- Applied structured, methodical troubleshooting to mechanical and electronic systems, developing corrective action plans and audit-ready documentation
- Developed technical documentation and training materials to support data-driven decisions and consistent audit readiness

PROJECTS (SEE GITHUB)

Container Honeypot (Kubernetes/Docker): Deployed and monitored a honeypot on Kubernetes/Docker to capture and analyze attacker behavior, reinforcing container security and threat detection skills

Project Archon (Home Lab): Segmented, enterprise-style infrastructure lab spanning Active Directory, virtualization, managed switching, NAS storage, and firewall/SIEM, used for vulnerability assessments and NIST-aligned log analysis

EDUCATION & CERTIFICATIONS

B.S., Cybersecurity & Information Assurance: Western Governors University, 2026

M.S., Information Security Engineering: SANS Technology Institute (In Progress)

DoD 8570/8140 Baseline Qualified: IAT Level III, IAM Level II, CSSP Analyst, CSSP Incident Responder, CSSP Auditor (via SecurityX, CySA+, PenTest+)

GIAC: GSEC: Security Essentials

CompTIA: CySA+, PenTest+, SecurityX (formerly CASP+/CAS-005), Security+, Linux+, Network+, A+, Project+, Data+

Microsoft: AZ-900: Azure Fundamentals • MD-102: Endpoint Administrator Associate • SC-200: Security Operations Analyst Associate

Other: LPI Linux Essentials, ITIL v4