Zachary Nicholas

Hubert, NC | 910-320-1369 | zachary.nicholas@outlook.com

Technical Projects: github.com/Toast-stack | LinkedIn: linkedin.com/in/zachary-nicholas1341

Professional Summary

Cybersecurity professional specializing in threat detection, vulnerability management, and secure systems administration with a strong technical and operational background from military service. Experienced in SIEM tools (Splunk, Microsoft Defender), network security, and automation scripting (Python, PowerShell, Bash) to enhance security operations. Skilled in incident response, compliance enforcement (NIST, ISO 27001, HIPAA), structured diagnostics, risk mitigation, and technical documentation control. Proven expertise in multi-system troubleshooting, inventory management, cross-functional coordination, and environmental compliance, ensuring mission-critical readiness and data security integrity.

Experience

Independent IT Consultant | Self Employed **Jan 2020 – Present**

- Conducted threat analysis and vulnerability management, identifying risks and implementing remediation strategies.
- Developed automation scripts (Python, PowerShell, Bash) to streamline security monitoring and reduce operational overhead.
- Managed SIEM-based threat detection (Splunk, Microsoft Defender) to proactively respond to security incidents.
- Assisted in network security optimization, implementing firewall rules, IDS/IPS configurations, and system hardening practices.
- Advised on compliance frameworks (NIST, ISO 27001, HIPAA), supporting organizations in achieving cybersecurity alignment.

Heavy Equipment Mechanic | United States Marine Corps **May 2017- Aug 2021**

- Cross-trained extensively across multiple technical disciplines, including electrical systems, refrigeration, automotive diagnostics, water support systems, and structured troubleshooting methodologies, ensuring adaptability in high-demand environments.
- Led maintenance operations and system diagnostics for mission-critical assets using GCSS-MC, ensuring seamless operational readiness and efficient resource management.
- Managed technical documentation and compliance tracking, overseeing PLMS 3 publication control and structured maintenance workflows via IETMs, MIMs, and MRCs.
- Conducted structured troubleshooting and risk mitigation, applying electrical, hydraulic, and mechanical diagnostics to sustain system reliability and security resilience.
- Oversaw environmental compliance, ensuring proper handling of MSDS-tracked hazardous materials, used oil disposal, and safety enforcement protocols.

- Provided high-level reporting to unit leadership, delivering readiness briefings and operational assessments that informed decision-making across command levels.
- Supervised and mentored junior personnel, reinforcing best practices in troubleshooting, maintenance workflows, compliance enforcement, and structured operational coordination.

Skills & abilities

Threat Detection & Incident Response – SIEM event monitoring (Splunk, Microsoft Defender) for proactive risk mitigation.

Network & Cloud Security – Secure system configurations, VPN, firewall, IDS/IPS management, and AWS security policies.

Security Automation & Scripting – Python, PowerShell, Bash for automated security workflows and anomaly detection.

Compliance & Risk Management – Knowledge of NIST, ISO 27001, HIPAA, ensuring structured policy enforcement and security auditing.

Technical Documentation & Process Optimization – Security reporting, audit documentation, compliance tracking, and operational risk analysis.

Logistics & Multi-System Coordination – Inventory control, cross-disciplinary technical expertise, structured diagnostics, and readiness reporting.

Education

B.S. in Computer Science **Oct 2021 - Dec 2024**

Southern New Hampshire University | GPA: 3.797

Cyber Warrior Program **Jan 2025 - Apr 2025**

My Computer Career

Certifications

- CompTIA A+, Network+, Security+, & CySA+ Expires: April 2028
- Certified in Cybersecurity (ISC2) Expires: March 2028

References Available Upon Request