Zachary Nicholas

CYBERSECURITY PROFESSIONAL *THREAT DETECTION & SYSTEM SECURITY*

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

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

Objective

Results-driven cybersecurity professional with expertise in threat detection, vulnerability management, and security operations. Skilled in network security, secure system configurations, and structured incident response workflows. Adept at analyzing security events, mitigating risks, and enforcing compliance standards, with a strong foundation in SIEM tools, cloud security, and automation scripting.

Certifications

- CompTIA A+, Network+, Security+, & CySA+
- Certified in Cybersecurity (ISC2)

Skills & abilities

Cybersecurity & Threat Detection

- Monitoring security events and analyzing vulnerabilities using SIEM tools (Splunk, Microsoft Defender)
- Conducting security audits and risk assessments to ensure system integrity
- Implementing structured security frameworks aligned with industry standards

Network Security & Incident Response

- Configuring VPNs, firewalls, and IDS/IPS for secure network environments
- Investigating security anomalies and applying structured remediation strategies
- Enhancing compliance tracking through structured documentation and security reporting

Cloud Security & Secure System Configuration

- Managing cloud security policies and hardening AWS/Azure environments
- Implementing encryption protocols and secure authentication workflows
- Supporting cybersecurity policies aligned with ISO 27001 and NIST standards

Programming & Automation

- Developing security automation scripts using Python, Bash, PowerShell, and SQL
- Parsing security logs to detect anomalies and enhance structured incident response
- Optimizing security workflows with automated event correlation tools

Technical Documentation & Compliance Tracking

- Creating structured security documentation for audits and policy enforcement
- Refining structured risk analysis reports for cybersecurity governance
- Providing security awareness training to improve team-based security strategies

Experience

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

- Conducted cybersecurity assessments and vulnerability analysis to improve system defenses.
- Assisted clients with SIEM monitoring, firewall policy enforcement, and secure authentication configurations.
- Developed structured security documentation, compliance reports, and incident response guidelines.

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

- Managed technical troubleshooting workflows and structured documentation tracking.
- Conducted data-driven assessments to refine operational security tracking methodologies.
- Led problem-solving initiatives in structured technical environments focused on risk mitigation.

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

Technical Projects

Splunk-SIEM Threat Monitoring

- Configured real-time event tracking to analyze security incidents and improve threat detection

Python Vulnerability Scanner

- Developed a custom security script to automate network and web vulnerability analysis

SSH Log Analyzer

- Parsed SSH logs to identify brute-force attack patterns and enhance security monitoring

Home Lab Security Optimization

- Designed and maintained a secure home lab environment for testing network security configurations