Zachary Nicholas

CYBERSECURITY ANALYST

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 a proven track record in threat detection, incident response, and vulnerability management. Leveraging industry-recognized certifications (CompTIA Security+, CySA+, and ISC2 Certified in Cybersecurity) and hands-on experience with SIEM tools, cloud security, and compliance frameworks, I aim to safeguard systems, mitigate risks, and enhance organizational resilience.

Certifications

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

Skills & abilities

- **Cybersecurity:** Threat Detection, Incident Response, Vulnerability Assessment, Risk Management, SIEM Tools (Splunk), Microsoft Defender
- **Network Security:** Proficient in SIEM tools (e.g., Splunk), VPNs, firewalls, IDS/IPS, and network protocols (TCP/IP, DHCP, DNS).
- **Cloud Security:** Familiarity with AWS and Azure, including virtual machine setup, hardening, and monitoring.
- **Programming & Automation:** Skilled in Python, PowerShell, Bash, and SQL for scripting, log analysis, and secure application development.
- **Incident Management:** Hands-on experience aligning workflows with the NIST Cybersecurity Framework and OWASP guidelines.
- **System Administration:** Proficient in Windows, Linux, and Active Directory environments, including secure configuration and optimization.
- **Compliance Frameworks:** Knowledge of NIST, ISO 27001, GDPR, HIPAA, and implementation of security policies and audits.

Soft Skills:

Critical Thinking, Problem-Solving, Communication, Team Collaboration, Attention to Detail, & Adaptability

Experience

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

- Delivered custom hardware solutions tailored to client needs, balancing cost-efficiency and performance.

- Designed and maintained a home lab server infrastructure, showcasing advanced networking proficiency.
- Collaborated with clients to test and debug applications, improving end-user experiences and system functionality.
- Conducted technical troubleshooting and performance tuning using tools like HWinfo64 and NetData.

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

- Diagnosed and maintained mission-critical machinery, ensuring operational readiness and adherence to safety standards.
- Supervised and trained personnel, fostering teamwork and technical proficiency.
- Managed inventory with GCSS and Excel, streamlining parts management processes.

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

Python Vulnerability Scanner

- This project demonstrates your ability to identify network and website vulnerabilities, showcasing critical skills in threat analysis and cybersecurity tools.

Splunk-SIEM Environment

- SIEM configuration and real-time threat monitoring are essential for SOC Analyst roles. This project highlights your ability to detect and respond to threats using industry-standard tools.

SSH Log Analyzer

- Parsing SSH logs and identifying brute force attacks align directly with SOC workflows, showcasing practical experience in incident response.

Password Security Toolkit

- This project reflects your expertise in strengthening authentication measures and leveraging APIs, which are valuable for safeguarding systems.

CS-305: Software Security

- Conducting vulnerability assessments and applying NIST standards demonstrates your understanding of secure coding practices and compliance, essential for cybersecurity roles.