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

Security-certified SOC Analyst with a B.S. in Computer Science and DoD 8570 IAT II compliance. Skilled in SIEM monitoring, log analysis, and incident response through academic and homelab experience. Familiar with MITRE ATT&CK, threat intelligence feeds, and structured escalation workflows. Known for disciplined troubleshooting, documentation habits, and a mission-driven mindset. Ready to contribute to real-time threat detection and security investigations in a collaborative SOC environment.

Core Competencies

SIEM Monitoring (Splunk) | Log Analysis & Correlation | Threat Detection | Incident Response Support | Escalation Workflows | MITRE ATT&CK Familiarity | Threat Intelligence Feeds | Detection Rule Tuning (Lab-Based) | IOC Investigation | Vulnerability Assessment | Endpoint Diagnostics | Windows & Linux Systems | Technical Documentation | Security Reporting | PowerShell Scripting | Compliance Frameworks (NIST, HIPAA) | Root Cause Analysis | Team Collaboration

Certifications

CompTIA A+, Network+, Security+, & CySA+ (Expires: Apr 2028) | Certified in Cybersecurity (ISC2, Expires: Mar 2028)

Experience

Technical Development & Cybersecurity Projects | Academic & Personal Experience **Jan 2020 – Present**

- Built and maintained a custom Splunk lab to simulate SOC workflows including alert triage, threat hunting, and log correlation
- Engineered a homegrown log aggregation pipeline to replicate SIEM telemetry ingestion and parsing logic
- Practiced incident response steps using MITRE ATT&CK mapping and investigation of indicators of compromise (IOCs)
- Explored DNS filtering concepts and threat intelligence feeds through lab-based research
- Studied Palo Alto firewall logic and network segmentation principles as part of certification preparation
- Created structured documentation including troubleshooting guides and escalation procedures for repeatable lab tasks
- Applied PowerShell scripting to automate health checks, parse logs, and validate endpoint remediation
- Contributed to simulated security reporting aligned with NIST 800-53 and HIPAA compliance practices

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

- Diagnosed and repaired mission-critical electronic systems under operational and security constraints
- Conducted structured reporting to senior leadership on equipment readiness and operational status
- Created technical documentation and SOPs to train junior Marines in troubleshooting and escalation logic
- Maintained provisioning records and ensured compliance with DoD operational standards
- Operated under SAAR authorization and background clearance protocols in secure environments

TECHNICAL PROJECTS

Splunk Lab: Alert Triage & Threat Investigation: Designed and deployed a custom Splunk instance to simulate EDR workflows. Practiced log correlation, threat hunting, and post-event documentation aligned with MITRE ATT&CK.

Custom Log Aggregation & SIEM Simulation: Engineered a self-built telemetry ingestion workflow using Splunk and parsing scripts to emulate production-level SIEM operations without commercial orchestration tools.

DNS Security & Network Hardening Research: Explored DNS filtering techniques, threat intelligence integration, and network segmentation concepts to reinforce secure infrastructure design and incident containment strategies.

Education

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

Southern New Hampshire University | GPA: 3.797

- Focus: Secure systems administration, scripting, infrastructure development
- Projects include cloud labs, homelab environments, and compliance-aligned documentation