ZACHARY NICHOLAS

Hubert, NC · 910-320-1369 · zachary.nicholas@outlook.com
GitHub: github.com/Toast-stack | LinkedIn: linkedin.com/in/zachary-nicholas1341

Professional Summary

Security-certified analyst with a Bachelor of Science in Computer Science and DoD 8570 IAT II compliance. Experienced in investigating security incidents, tuning SIEM alerts, and documenting response logic in alignment with frameworks such as NIST 800-53 and MITRE ATT&CK. Built and maintained custom threat detection environments using Splunk to simulate enterprise-scale triage, remediation, and escalation. Skilled in endpoint diagnostics, multi-threaded scripting, secure access workflows, and collaborative threat intelligence development. Driven by a commitment to cybersecurity hygiene, operational readiness, and precision problem-solving.

Technical Skills

Security Operations & Investigation: SIEM (Splunk Lab), Phishing Detection, IOC Tracking, MITRE ATT&CK Alignment, Vulnerability Remediation, Endpoint Diagnostics, Security Incident Analysis
Security Frameworks & Compliance: NIST SP 800-53, RMF Concepts, FISMA (Lab-Simulated), HIPAA (Simulated), DoD 8570 Compliance, Risk Documentation, ATO Workflow Familiarity
Scripting & Tool Development: Python, PowerShell, Bash, Flask, REST APIs, Log Parsing, JSON/CSV Transformation, CLI & Dashboard Design, Certificate Handling, Encryption (SHA-256)
Systems & Network Knowledge: Linux/Windows Audit Scripts, TCP/IP, DHCP, SSH, Role-Based Access Control, IDS/IPS Concepts, Firewall Rule Simulation
Collaboration & Workflow Tools: GitHub, GitLab, JIRA (Conceptual), Markdown Documentation, Version Control, Technical Writing, Team Coordination

Certifications

- CompTIA A+, Network+, Security+, CySA+ (Valid through Apr 2028)

Education

Bachelor of Science in Computer Science

Southern New Hampshire University · Graduated Dec 2024 · GPA: 3.797

Experience

Technical Development & Security Labs

Academic & Homelab Experience · Jan 2020 – Present

- Built Splunk SIEM dashboards to simulate alert triage, IOC mapping, and incident lifecycle tracking
- Developed modular CLI tools in Python and PowerShell for system scanning, log parsing, and misconfiguration detection
- Investigated simulated phishing and malware indicators, integrating basic GeoIP logic and suppression rules
- Explored RMF and NIST control mapping through mock ATO documentation, risk registry simulations, and control summaries
- Wrote markdown-based technical documentation, code guides, and usage notes for security-focused projects

Heavy Equipment Mechanic

United States Marine Corps · May 2017 – Aug 2021

- Diagnosed electronic systems under pressure using structured fault isolation
- Created technical maintenance documentation aligned with operational readiness goals
- Operated under DoD asset tracking protocols (GCSS-MC) and secure logistics workflows
- Trained junior personnel in systematic troubleshooting and diagnostics

Technical Projects

SecureStack Toolkit: Modular CLI suite for vulnerability scanning, endpoint health checks, and log analysis across Linux and Windows environments.
SecOps-Lab: Simulated cloud threat monitoring and intelligence ingestion with Flask dashboards, alert workflows, and automated response logic.
SSHLogAnalyzer: Python tool to detect brute-force attacks by analyzing SSH logs and flagging suspicious activity.
Flight Tracker App: Flask-based backend with PostgreSQL and Folium map integration; visualized real-time flight data from public APIs using secure web architecture.
Password Security Toolkit: Python-based password validator and breach checker with strength analysis, entropy scoring, and dynamic generation logic.