King Awhaetoma
(765) 354 8822 | linkedin.com/in/king-awhaetoma | github.com/Kingawhaetoma

SUMMARY Entry-level Cybersecurity graduate with hands-on experience in security monitoring, alert triage, vulnerability analysis, and incident documentation through coursework, labs, and security projects. Strong foundation in network traffic analysis, SIEM operations (Splunk), and incident response, with a clear goal of growing into a SOC analyst role.

Education Ball State University | Muncie, IN BSc in Applied Cybersecurity, Minor Music Production | GPA 3.9 Coursework: Network Security, Ethical Hacking, Defensive Security, Digital Forensics, System Administration, Shell Scripting, Programming.
Certifications: CompTIA Security+, CompTIA CySA+, Palo Alto Certified Cybersecurity Practitioner, Splunk Core Certified User

TECHNICAL SKILLS

- **Security Tools**: Wireshark, pfSense, Nmap, Burp Suite, Metasploit,
- **Threat Intelligence:** IOC analysis, TTP identification, threat actor profiling
- **Networking:** TCP/IP, DNS, DHCP, VLANs, VPN configuration, Firewall rules (pfSense),
- **Programming**: Python, Bash, Java,
- **Risk & Compliance**: NIST CSF, NIST 800-53, ISO 27001, SOC 2
- **Digital Forensic:** Magnet Axiom, FTK Imager, Eraser,
- **Incident Response:** Alert triage, phishing analysis, log analysis, threat hunting, SIEM monitoring (Splunk, Defender)

WORK EXPERIENCE

Security Analyst (Project-Based) – Innovation Connect (InnC) **October 2025 – Present (Remote)**

- Conducted **security assessments** on production WordPress environments, identifying **15+ vulnerabilities** including misconfigurations, outdated plugins, weak authentication, and missing HTTPS
- Reduced risk of unauthorized access by auditing user roles, removing inactive accounts, and enforcing multi-factor authentication (MFA)
- Collaborated with a 5-member security team to deliver a **Security Audit Report and Incident Response Plan** for executive leadership
- Documented findings clearly for **non-technical stakeholders**, aligning recommendations with **NIST security principles**

PROJECT EXPERIENCE

Security Operations & Monitoring (SOC Capstone Project) January 2026 – Present

- Deploying and configuring a simulated Security Operations Center (SOC) environment using **Wazuh SIEM** for centralized log collection and security monitoring
- Monitoring security events and alerts across Linux and Windows systems to detect anomalous activity, failed authentication attempts, and potential intrusions
- Supporting **file integrity monitoring (FIM)** and vulnerability detection to identify unauthorized system changes
- Conducted user account reviews and cleanup exercises to reduce unauthorized access risk.
- Documenting incidents, findings, and response actions using SOC-style workflows and reporting practices

Enterprise Network Security & Assessment Lab August 2025 – Present

- Designed and implemented a secure 7-floor enterprise network (168 users, 5 servers, 6 printers) using Cisco Packet Tracer.
- Configured IP addressing, Implemented **VLAN segmentation,** trunking, **routing, firewall rules (pfSense), IDS/IPS, and access controls**
- Delivered a full bill of materials, cost estimates, and a working Packet Tracer simulation to demonstrate enterprise- ready deployment.
- Conducted a full **vulnerability assessment**, documenting findings with CVSS scoring
- Used Wireshark to analyze network traffic and identify anomalies.
- Produced security documentation aligned with NIST CSF and SOC-style controls