

RICHMOND NSIAH DUAH

IT & CYBERSECURITY ANALYST

work.nsiahduah@gmail.com

SUMMARY

Cybersecurity professional with hands-on experience in security monitoring, vulnerability assessment, incident response, and IT system protection. Skilled in analyzing logs, detecting threats, and strengthening network security through both real-world IT roles and a dedicated home lab SOC environment. CompTIA Security+ certified, with strong analytical skills and a proactive approach to identifying vulnerabilities and improving security posture.

CORE SKILLS

- Security Monitoring: SIEM (Splunk), log analysis, alert triage, IDS/IPS basics (Snort, Suricata).
- Threat Detection & Analysis: Network traffic analysis, malware behavior basics, packet capture (Wireshark), endpoint security.
- Vulnerability Assessment: Nmap, GVM/Nessus Essentials, system hardening, configuration review.
- Incident Response: Evidence collection, root-cause analysis, containment & recovery strategies, documentation.
- Cybersecurity Frameworks: NIST CSF, ISO 27001, PCI-DSS, GDPR fundamentals.
- IT & Network Support: System administration, user access management, network security, software troubleshooting.
- Security Awareness & Policy Enforcement: Staff training, safe internet practices, data protection compliance.

PROJECTS

Home Lab SOC & Cybersecurity Environment

- Deployed a virtual network using VirtualBox with Windows, Linux, and Kali nodes.
- Configured a mini SOC environment using Splunk and ELK to simulate SIEM monitoring, log analysis, and alert triage.
- Simulated attacks and defensive strategies, including brute force attempts, privilege escalation, and log correlation.
- Conducted basic malware analysis in an isolated environment.

Mastercard Cybersecurity Virtual Experience Program on Forage

November 2025

- Completed a job simulation where I served as an analyst on Mastercard's Security Awareness Team.
- Helped identify and report security threats such as phishing.
- Analyzed and identified which areas of the business needed more robust security training and implemented training courses and procedures for those teams.

Tata Cybersecurity Security Analyst Job Simulation on Forage

November 2025

- Completed a job simulation involving identity and access management (IAM) for Tata Consultancy Services, collaborating with a Cybersecurity Consulting team.
- Acquired expertise in IAM principles, cybersecurity best practices, and strategic alignment with business objectives.
- Delivered comprehensive documentation and presentations, showcasing the ability to communicate complex technical concepts effectively.

Datacom Cybersecurity Job Simulation on Forage

November 2025

- Completed a simulation focused on how Datacom's cybersecurity team helps protect its clients
- Investigated a cyberattack and produced a comprehensive report documenting findings and outlining key recommendations to improve a client's cybersecurity posture
- Conducted a comprehensive risk assessment

Forage Academy Data Labeling Job Simulation on Forage

November 2025

- Completed a job simulation where I worked as a Data Labeling Analyst for a hypothetical AI company, reviewing real customer support messages
- Practiced classifying messages for Intent, Sentiment, and PII (personally identifiable information) using a consistent labeling schema
- Evaluated tricky or ambiguous edge cases, and wrote short rationales justifying final label decisions
- Reviewed labeling work done by others, identified inconsistencies, and suggested one improvement to the team's labeling guidelines
- Strengthened my ability to apply clear definitions, follow ethical privacy practices, and maintain consistency across data
- Gained hands-on experience in human-AI collaboration, foundational to roles in AI ops, trust & safety, and machine learning support

TOOLS & TECHNOLOGIES

Security

Splunk, ELK Stack, Suricata, Snort, Nmap, Wireshark, GVM, Nessus Essentials.

Systems

Windows Server, Linux (Kali, CentOS), VirtualBox, VMware.

Networking

Firewalls, VLANs, TCP/IP, DNS, DHCP.

Other

Python (basic scripting), Git, Bash, PowerShell.

CERTIFICATION

CompTIA Security+ (SY0-701) — Issued 2025

Validated knowledge of Security operations & monitoring, Incident response & digital forensics fundamentals, Network defense & access control, and Risk management & security architecture.

EDUCATION

BSc Information Technology

Knutsford University College, Accra (2019–2023)

FGPA: 3.54

- Relevant coursework in Computer Crime, Forensics & Auditing, Network Security, Database Management, IT Project Management.

PROFESSIONAL EXPERIENCE

Technical Staff & Assistant Video Editor | Ghana Broadcasting

November 2023 - October 2024

Corporation – Garden City TV

- Monitored and maintained broadcast & IT systems, ensuring uptime and system integrity.
- Applied cybersecurity hygiene, including secure file transfers and access control.
- Supported system upgrades, software troubleshooting, and workflow security.
- Ensured systems complied with internal policies and safe data handling procedures.

IT Consultant | Kumasi Roman Catholic Girls' JHS

January 2022 - November 2023

- Conducted security checks on school IT systems and enforced data protection practices.
- Implemented secure user access management procedures.
- Provided staff training on cybersecurity best practices and safe internet usage.
- Managed network security controls and responded to security-related issues.

ADDITIONAL INFORMATION

- **Languages:** English, Twi.
- **Interests:** Interested in SOC analysis, threat detection, incident response, and security engineering paths.
- Passionate about continuous learning in cybersecurity.