YAW OSEI AHENKRO

Address: Queen's Park House, Coventry, CV1 3GX, United Kingdom
Email: ahenkroyawosei@gmail.com
LinkedIn Profile: https://linkedin.com/in/yaw-osei-ahenkro
Phone: 07946610246

PERSONAL PROFILE

A Cyber Security Analyst with hands-on experience in threat detection, incident response, and security operations across Windows and Linux environments. Skilled in network traffic analysis, log review, and vulnerability assessment using tools such as Wireshark, Zeek, Splunk, Kali Linux, etc. Experienced in analysing suspicious activity, simulating common attack vectors, and supporting incident investigations through packet inspection and basic digital forensics. Knowledgeable in SIEM workflows, firewall rule analysis, intrusion detection techniques, and access control models. Comfortable working in command-line environments and applying structured, methodical approaches to identifying and mitigating security threats within SOC and enterprise settings.

SKILLS

Technical Skills

- Threat detection and incident response
- Vulnerability identification and OWASP Top 10 familiarity
- Access control models and system hardening practices
- Malware behaviour analysis and digital forensics techniques
- Comfortable in Linux (Kali, Ubuntu) and Windows environments
- Network configuration, subnetting, port scanning, and routing basics
- Log analysis (system logs, firewall logs, and SIEM workflows, eg, Splunk)
- Wireshark for packet analysis and protocol inspection
- Risk management, VMware, Metasploit
- Hydra password brute-forcing and service login testing
- Kali Linux - penetration testing and reconnaissance workflows

Soft Skills

- Analytical mindset with attention to detail
- Eager to learn, adapt, and work collaboratively within security teams
- Strong written and verbal communication for documentation and reporting

EXPERIENCE

Cybersecurity Analyst Intern, Amdari, London, United Kingdom, Dec 2025 - Present
Key Achievements & Impact:

- Implemented and optimised SIEM solutions, enhancing real-time threat detection and reducing cyber incidents by 40%, while accelerating incident response time by 50% through automated alerts and streamlined remediation workflows.
- Identified and remediated security vulnerabilities, reducing attack surfaces by 85% through proactive risk assessments, penetration testing, and automated patch management.
- Enhanced cloud security infrastructure, implementing robust IAM policies, encryption standards, and Zero Trust principles, leading to a 30% decrease in cloud-based security breaches.
- Designed and delivered cybersecurity awareness programs, increasing phishing detection and employee security awareness by 60%, significantly reducing social engineering risks across the organisation.

Cyber Security Lab Work, Coventry University, Jan 2025 – Dec 2025

- Troubleshot virtual machine setup issues in Kali Linux environments with a 75% success rate as part of cybersecurity coursework.
- Used command-line tools, e.g., CMD, bash, and shell, to analyse logs and simulate basic penetration tests of 5 virtual machines.
- Collaborated with classmates on simulated IT support of 10 cases involving password resets, user access control, and patch updates
- Performed 10 labs on network configurations using Cisco Packet Tracer, such as IP addressing, Access Control Lists, Routing, RIP, VLANS, etc.

ACADEMIC PROJECTS

Network Traffic Forensics for detecting and analysing IoT botnets and DDoS Attacks – TShark, Zeek, Splunk (Dissertation), Coventry **University, Sept 2025 – Dec 2025**

- Analysed 67M+ network events from IoT traffic to detect botnet-driven DDoS attacks, using Zeek, Splunk, Wireshark, and TShark in a controlled lab environment.
- Identified Mirai-like attack behaviour (SYN floods, UDP floods, HTTP floods, beaconing, command injection) through metadata correlation and packet-level validation.
- Built a reproducible network forensics workflow that converts raw PCAPs into SIEM-ready intelligence, supporting faster threat identification and incident investigation.
  Tools: Zeek, Splunk, Wireshark, TShark, Python, Linux, VMware
  Techniques: Network forensics, DDoS analysis, botnet detection, SIEM analysis

PixelForge Nexus Management System – Academic Software Development Project
Coventry University, May 2025 – Aug 2025.
Link: https://github.com/ahenkroyawosei/PixelForge-Nexus.git

- Developed a role-based project management system supporting Admin, Project Lead, and Developer roles, ensuring proper access control and data security.
- Implemented secure authentication, including bcrypt password hashing and optional Multi-Factor Authentication (MFA) for enhanced account protection.
- Enforced role-based access control (RBAC) to ensure users only accessed functions and data aligned with their privileges.

EDUCATION

MSc Cybersecurity, **Coventry University, Coventry, UK**
Jan 2025 – Dec 2025)

- Core Modules: Network Security, Digital Forensics, Secure System Design, Ethical Hacking, etc.
- Developed and delivered multiple technical reports and case study-based projects

BSc (Hons) Information Technology, Valley View University
Aug 2020 – Dec 2023 (First Class)

CERTIFICATIONS

Google Foundations of Cybersecurity via Coursera, Issued on Jan 9, 2023
Verify at: https://coursera.org/verify/8RWKQQGXZHSR

REFERENCES

Available upon request