ADJEI YAW OSEI

adjeiyawosei@gmail.com | +233201240821| My Portfolio | LinkedIn | GitHub

PROFILE

Cybersecurity enthusiast with exposure to basic SOC operations, log analysis, and scripting to support incident response. Familiar with Splunk, Wireshark, and scripting in Python, Bash, and PowerShell. Currently pursuing CompTIA Security+ and eager to contribute to a SOC team while gaining hands-on experience in real-world defense operations. Open to learning new tools and technologies across cybersecurity and related areas.

EDUCATION

BSc. Computer Science **Expected Graduation: November 2027**
Kwame Nkrumah University of Science and Technology (KNUST), Kumasi Ghana

PROFESSIONAL TRAINING/ CERTIFICATION

- Google Cybersecurity Professional Certificate – Google (2024)
- ISO/IEC 27001 – Mastermind (2025)
- CCNA – Cisco (2025)
- ISC2 Certified in Cybersecurity (CC) – ISC2 (2025)
-CyberOps Associate – Cisco (2025)
- IBM Cybersecurity Analyst – IBM (2025)

SKILLS & COMPETENCIES

• Tools: Splunk, Wireshark, Microsoft Defender
• Operating Systems: Windows, Linux (Ubuntu)
• Scripting: Python, Bash, PowerShell, KQL
• Frameworks: ISO 27001, OWASP Top 10
• Other: Packet inspection, log correlation, threat detection, basic SIEM automation

WORK EXPERIENCE

SOC Intern, Ideation Axis, Greater Accra **Sept 2024 – Dec 2024**

- Analyzed 50+ daily security events in Splunk, escalating 20+ confirmed threats to senior analysts
- Parsed logs from Windows and Linux systems using Python scripts, reducing triage time from ~8–10 minutes to under 5 minutes per alert.
- Detected IOCs in packet captures using Wireshark, contributing to threat identification and escalation

Security Analyst Intern, Center for Cyber Security Studies & Research, Remote **May 2024 – July 2024**

- Developed basic IR playbooks for phishing and malware scenarios, standardizing response steps
- Monitored lab networks for phishing/malware campaigns using log analysis and sandbox testing

PROJECTS & RESEARCH EXPERIENCE

Investigating Automated Detection and Response for Phishing & Business Email Compromise Threats **May 2025 - Present**
- The study will investigate and mitigate advanced phishing and business email compromise attacks in real time using Splunk, Python scripting and ML.

SIEM Automation with Wazuh (IBM CAS + KNUST) **March 2025 – Present**
- Building a Wazuh-based SOC lab with intrusion simulation, REST API agents, and SOAR workflows using Docker and n8n, in collaboration with IBM, to improve automated threat detection and response

Traffic Anomaly Detection System (Team Project) | [GitHub] **Jan 2025 – April 2025**
- Designed an alerting system using statistical thresholds to detect unusual activity in large network traffic datasets.
- Integrated Slack/email notifications for faster team response during simulation drills.

Custom Network Packet Sniffer | [GitHub] **Sept 2024 – Jan 2025**
- Built a Python-based sniffer to capture and filter 5,000+ packets per session.
- Detected ARP spoofing, SYN flood attacks and port scans in a controlled lab setting.

LEADERSHIP & VOLUNTARY EXPERIENCE

- Mentor, CSS-KNUST – Guided 5+ freshmen in academic planning and study
- Workshop Facilitator, KNUST Cybersecurity Club – Taught basic Python automation and basic SOC concepts
- Outreach Speaker – Delivered cybersecurity awareness to basic & high school students

REFEREES

References available upon request.