OBIOMA FELICITY UZOH

Cybersecurity Analyst | SOC & Blue Team Specialist

Gmail: obiomafelicityuzoh@gmail.com | LinkedIn: https://www.linkedin.com/in/felicityuzoh | Portfolio: https://techounik.github.io/techounik/

PROFESSIONAL SUMMARY

Performance-driven **Cybersecurity Analyst** with appreciable experience in **Information Assurance**, **Security Operations**, and **Continuous Monitoring**. Currently ranked **#1 in Nigeria on Hackviser**, with a dedicated focus on **SOC workflows**, **Incident Response**, and **FISMA/NIST compliance frameworks**. Proven ability to mitigate high-risk technical challenges, successfully managed 100% delivery of enterprise-level lab requirements during critical hardware failures by applying asset prioritization and risk management principles. Expert at translating complex **Information Security policies** into actionable technical training

---

TECHNICAL SKILLS

- **Security Technologies:** SIEM (Splunk), EDR (Qualys), IDS/IPS (Snort, Suricata), Firewalls, Wireshark (Traffic Analysis), Nessus, OWASP ZAP.
- **Standards & Frameworks:** NIST-CSF, ISO 27001, SOC 2 (Type 1 & 2), PCI DSS, GDPR, CIS Critical Security Controls, OWASP Top 10.
- **Domains & Platforms:** Vulnerability Management, RBAC (Role-Based Access Control), Configuration & Patch Management, Identity & Access Management (IAM), Active Directory, Cloud Security (Qualys Cloud), Digital Forensics.
- **Methodologies:** SDLC (Secure Systems Development Life Cycle), Agile/Scrum, Technical Report Writing, Incident Response Playbook Development

---

INTENSIVE TRAINING & PROJECTS

Project 20 Next Gen (Cohort 1) | 8-Week Intensive Program

- **Security Assurance Testing:** Performed rigorous testing of security controls and their operating effectiveness across 40+ labs.

- **Threat Intelligence:** Identified threat vectors and developed **use cases for security monitoring** using the **Unified Kill Chain** and **Pyramid of Pain**.
- **Network Security:** Achieved network security objectives by deploying and administering **Firewalls** and **IDS/IPS tools** for virtualized servers.
- **Vulnerability Management:** Scheduled and executed vulnerability assessments leveraging **Qualys** and **Nmap**, followed by coordinated **security remediation**.
- **Incident Response:** Established **Incident Response Playbooks** in alignment with industry-standard response plans (NIST).

BlueTeam_Kit | Award-Winning Forensic Triage Framework

- Developed a custom Python-based CLI tool that won a 2026 Cybersecurity Challenge for its efficiency in automating the analysis of Windows Event Logs (.evtx).
- Programmed detection logic to identify critical persistence mechanisms (Event 4720) and anti-forensic activities (Event 1102).
- Implemented image metadata scanning functionality to detect hidden malware payloads via steganography.

Final Year Project: Insider Threat Detection | Miva Open University

- Developing an ML-based system for **Continuous Monitoring** of behavioral rhythm anomalies to detect **Insider Threats**.

PROFESSIONAL EXPERIENCE

Cybersecurity Tutor | Tech Region Africa

March 2026 – Present

- Responsible for the **creation, maintenance, and delivery** of technical cybersecurity training programs focused on network defense and incident response.
- Lead students in **engineering virtualized security lab environments** using VirtualBox to host Kali Linux and Metasploitable targets for defensive testing.
- Administer and monitor network traffic through **Wireshark** to identify threat vectors and demonstrate security-related incidents on the wire.
- Instruct on the implementation of **isolated network routing protocols** and infrastructure design to ensure secure and controlled testing environments.
- Ensure curriculum and student performance **align with industry-standard KPIs** to meet managed SOC service expectations.

Student Ambassador | Hackviser (Oct 2025 – Present) and Cowrywise (Feb 2026 - Present)

- Launched **"Club Cyber,"** a LinkedIn educational series that uses relatable analogies to simplify complex SOC concepts such as SIEM monitoring and privilege escalation for a growing professional audience.
- Actively promotes ethical hacking best practices and provides feedback on platform usability to improve the training experience for peers.

Cybersecurity Job Simulations | Forage (Mastercard & Commonwealth Bank) (Dec 2025)

- **SOC & Incident Response:** Engineered Splunk dashboards for fraud detection and analyzed phishing data to identify high-risk social engineering targets.
- **Security Assessment:** Performed web application penetration tests, identified vulnerabilities, and authored professional remediation reports.
- **Governance:** Designed security awareness infographics based on Australian Cybersecurity Centre standards to bridge training gaps.

EDUCATION & CERTIFICATIONS

- **B.Sc. Cybersecurity** | *(Expected Aug, 2026)*
- **Certified Associate Penetration Tester (CAPT)** | Hackviser London | *Dec, 2025*
- **Google Cybersecurity Professional Certificate** | Coursera | *Nov, 2025*
- **Certified Web Security Expert (CWSE)** | Hackviser London | *Dec, 2025*
- **Introduction to cybersecurity** | Cisco | *Jan, 2025*
- **Talk2Luke Academy Canada - Cybersecurity Training Program** | *Feb, 2026*
- **Training Completed: ISC2 Certified in Cybersecurity (CC) |** *Mar 2026*