Prince Richard Osaro

📍 Lagos Mainland, Nigeria | 📧 princerichard547@gmail.com | 📞 +234-807-891-0382

🔗 LinkedIn | 💻 GitHub | 📰 Medium | 🌐 Portfolio

🎯 Professional Summary

Mission-driven Cybersecurity & SOC Analyst with a passion for building intelligent, resilient defenses. Certified by ISC2 (Certified in Cybersecurity – CC) and Google (Cybersecurity + Python Automation), with practical experience in threat detection, cloud security, and automation. Hands-on skills with SIEM tools (Splunk, ELK), network analysis (Wireshark, Sysmon), and Python scripting. Currently pursuing Cybersecurity Mastery & Ethical Hacking and preparing for CompTIA Security+. Blending cybersecurity expertise with a full stack web development background and a DevSecOps mindset.

🎓 Education

University of Benin — B.Sc. Accounting
Graduated: 2021 | Second Class Upper (2:1)

Torilo Academy — Cybersecurity Mastery & Ethical Hacking (In Progress)

Global Tech Academy — Full Stack Web Development (Completed 2024)

📜 Certifications

- ISC2 Certified in Cybersecurity (CC)

- Google Cybersecurity Professional Certificate

- Google IT Automation with Python

- Google IT Support Certificate

- CompTIA Security+ (In Progress)

💼 Work Experience

Cybersecurity Intern (SOC Track) – Torillo Academy
Jan 2025 – May 2025

- Monitored alerts using ELK Stack, performed triage, and escalated incidents.
- Investigated brute-force attempts and phishing simulations using log analysis and SIEM tools.
- Documented response workflows and collaborated on detection rules to reduce false positives.

Full Stack Developer Intern – Global Tech Academy
July 2024 – Dec 2024

- Developed responsive UI components using HTML, CSS, and JavaScript.
- Contributed to Laravel and React-based apps and collaborated on backend API security.
- Applied secure coding practices and built reusable components in cross-functional teams.

🛠️ Projects

- SOC Lab (Personal Project): Simulated enterprise SOC with Splunk, Sysmon, and ELK for threat detection practice.

- SSH Log Analyzer: Python + Bash script to detect brute-force SSH login patterns in system logs.

- Fintech IR Playbook: Created a simulated incident response guide for phishing and lateral movement scenarios.

🔧 Core Skills

- SIEM Tools: Splunk, ELK Stack | Log & Alert Analysis | MITRE ATT&CK

- Cloud Security: AWS (IAM, S3), Azure | IAM Policies | Workload Protection

- Security Automation: Python, Bash | Threat Hunting | AI in Cyber Defense

- Network Analysis: Wireshark, Sysmon, Suricata | Event Log Correlation

- DevSecOps: HTML, CSS, JS, React, Laravel | API Security | Secure SDLC