AROMOLARAN EMMANUEL

(+234) 902-578-7239 · sopearomolaran@gmail.com · linkedin.com/in/emmie-aromolaran · Lagos, Nigeria

PROFESSIONAL SUMMARY

Cybersecurity professional with 3+ years of experience in SOC operations, vulnerability management, and penetration testing. Skilled in AWS security tools (GuardDuty, CloudTrail, Security Hub), SIEM (Splunk, Wazuh), and penetration testing frameworks. Proven track record of reducing organizational risk and translating technical findings into business impact for executive stakeholders.

CORE SKILLS

Security Operations	SIEM (Splunk, Wazuh), Incident Triage, Log Analysis, Alert Escalation
Cloud Security	AWS GuardDuty, CloudTrail, Security Hub, EC2 Security Groups, IAM
Penetration Testing	Nmap, Metasploit, OWASP ZAP, Burp Suite, Dirbuster
Vulnerability Mgmt	Nessus, CVSS Scoring, Remediation Reporting
Frameworks	NIST, MITRE ATT&CK, ISO 27001
Scripting	Python, Bash, Terminal

WORK EXPERIENCE

Cybersecurity Instructor — PluralCode Institute (Remote)

June 2024 – August 2026

– Train 100+ adult learners in threat detection, network security, and AWS cloud security.
– Facilitated hands-on labs: GuardDuty configuration, CloudTrail investigation, Security Group hardening.
– Reduced student misconfigurations by 25%; achieved 85% internship placement rate for graduates.

Penetration Tester — Freelance

2023 – June 2026

– Tested web applications and networks for 10+ clients, discovering 15+ critical vulnerabilities.
– Reduced client risk exposure by 35%; delivered executive-level reports mapping technical findings to business risk.

SOC / Vulnerability Analyst (Internship) — Cardify Africa

2022 – 2023

– Assessed 50+ systems daily using CVSS scoring; reduced remediation time by 20% via clear vulnerability reporting.
– Monitored Splunk alerts, escalated confirmed threats to Tier 2, and trained 30+ staff on security best practices.

SOC Analyst / Threat Hunter — TrendMicro (Remote)

2021 – 2022

– Threat hunting with Wazuh and Splunk; escalated 10+ simulated attacks, improving MTTD by 18%.
– Mapped incidents to MITRE ATT&CK; for structured risk communication.

PROJECTS

AWS Security Operations Lab: Built end-to-end AWS SOC lab simulating brute force investigation. Configured GuardDuty, CloudTrail, and Security Hub; demonstrated full Tier 1 workflow: Alert → Investigate → Remediate → Document.

Threat Intelligence Lab: Analyzed Lazarus Group campaign; identified IOCs including proxy execution binaries and mapped findings to MITRE ATT&CK.

CERTIFICATIONS & EDUCATION

Certifications

– Certified SOC Analyst — TrendMicro (2023)
– NaijaSecCon 2019 — First Runner-Up (SQLi, XSS, Wireshark, Cryptography)

Education

– B.Tech in Cybersecurity — Federal University of Technology, Akure (2023)
– Second Class Upper (2:1)

KEY IMPACT METRICS

25% reduction in misconfigurations · 35% client risk reduction · 20% faster remediation · 18% improved MTTD · 85% client/placement satisfaction

ADDITIONAL INFORMATION

Languages: English (Fluent), Yoruba (Native) · **Tools:** Slack, Zoom, Microsoft Teams, Notion · **Availability:** Immediate — remote/hybrid · **References:** Available upon request