ALAYO MICHAEL

Cybersecurity Engineer | SOC Operations | Threat Detection & Incident Response
Lagos, Nigeria | +234 703 683 5824 | alayomichaeladetola@gmail.com | linkedin.com/in/alayomichael

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in security operations, threat detection, and incident response. Currently embedded within a live enterprise SOC at DataSixth Consulting, working with Elastic SIEM and ArcSight to monitor, correlate, and investigate real-world security events. Skilled in log analysis, MITRE ATT&CK; mapping, vulnerability assessment, and security documentation. Complementary background in offensive security through structured penetration testing training covering web application security, reconnaissance, and exploitation methodology. ISC2 Certified in Cybersecurity (CC). Actively developing expertise in cloud security and compliance frameworks.

CORE COMPETENCIES

SIEM & Detection Elastic SIEM, ArcSight, Wazuh — event correlation, detection rule development, alert triage

Threat Intelligence MITRE ATT&CK; mapping, IOC analysis, VirusTotal, threat actor behaviour profiling

Network Security Wireshark, packet capture analysis, network forensics, pcap investigation, traffic anomaly detection

Incident Response Alert triage, incident escalation, log analysis, IOC extraction, security documentation

Vulnerability Mgmt Nessus, OpenVAS, vulnerability scanning, risk assessment, remediation tracking

Offensive Security Burp Suite Pro, Kali Linux, Nmap, Metasploit, OWASP Top 10, web app penetration testing

Frameworks NIST CSF, MITRE ATT&CK;, OWASP, SOC 2 & GDPR (studying), identity & access management principles

Scripting & Tools Python (basic), KQL queries, MobaXterm, GCP, cloud security fundamentals

WORK EXPERIENCE

SOC Analyst Intern

DataSixth Consulting · Lagos, Nigeria · On-site | Apr 2026 – Present

- Monitor and correlate security events across Elastic SIEM and ArcSight in a live enterprise SOC environment
- Apply MITRE ATT&CK; framework to map adversary behaviour patterns and support structured threat intelligence analysis during active investigations
- Perform log analysis across network and endpoint data sources to identify anomalous activity and indicators of compromise (IOCs)
- Conduct network forensics investigations using Wireshark — extracted infected host identity, user credentials, C2 infrastructure, and malware delivery domains from raw packet captures
- Collaborate directly with senior SOC analysts on onsite investigations, building real-world incident response workflows
- Produce formal incident response reports documenting findings, evidence, and remediation recommendations

Cybersecurity Tutor (Contract)

Gurugeeks Royalty · Lagos, Nigeria · Remote/Hybrid | Apr 2026 – Aug 2026

- Delivered structured cybersecurity training covering SOC operations, threat detection, SIEM monitoring, and incident response
- Developed curriculum and hands-on lab exercises for aspiring cybersecurity professionals
- Taught MITRE ATT&CK; framework application, defensive security concepts, and SOC analyst workflows
- Mentored students through practical cybersecurity projects and provided personalised feedback on assessments

Ethical Hacker (Internship)

The Victor Akinode Initiatives · Remote | Nov 2025 – Mar 2026

- Performed web application security assessments using Burp Suite Pro — intercepting HTTP/S traffic, manipulating requests, and validating injection and access control vulnerabilities against OWASP Top 10

- Executed advanced reconnaissance using Shodan, OSINT frameworks, DNS enumeration (nslookup, dig), and WHOIS analysis to map attack surfaces
- Completed PortSwigger Academy labs covering authentication flaws, IDOR, SQL injection, and XSS with documented methodology and remediation writeups
- Researched CVE and CWE databases to identify exploitation paths and assess real-world applicability of discovered vulnerabilities

Cybersecurity Coach

HGSC2 Digital Skills Academy · Remote | 2025 – Present

- Developed and maintained training documentation, assessment criteria, and compliance tracking for student progress
- Guided learners through hands-on labs covering log analysis, network scanning, and vulnerability identification
- Supported students in understanding MITRE ATT&CK; techniques, defensive security concepts, and SOC analyst workflows

SOC Analyst Intern

CyBorts · Nigeria | 2025

- Assisted with real-time threat monitoring and incident analysis in a SOC-style environment
- Supported vulnerability assessments, risk identification, and tracked security findings through remediation to closure
- Maintained security documentation including incident logs and response procedures

Ethical Hacker (Junior Role)

Kinplus Technologies · Nigeria | 2023 – 2024

- Conducted vulnerability scanning and security assessments in controlled environments using industry-standard tools
- Practiced reconnaissance, scanning, exploitation, and reporting techniques across penetration testing methodology

SECURITY PROJECTS

Network Forensics Investigation — Malvertising Campaign (2026)

- Performed full pcap analysis in Wireshark to investigate a malicious Google Authenticator download incident on an enterprise network
- Identified infected host, MAC address, hostname, and logged-in user account through ARP, NBNS, and Kerberos packet analysis
- Traced initial access vector to a typosquatted domain registered 2 days before the attack; mapped three C2 servers across Iceland, Panama, and Lithuania
- Corroborated all IOCs using VirusTotal and WHOIS; produced formal incident response report with documented evidence and remediation recommendations

Home Security Lab — Wazuh SIEM Environment

- Built security monitoring environment using Wazuh SIEM; created detection rules for common attack patterns mapped to MITRE ATT&CK;
- Practiced incident investigation and documentation workflows in a self-managed lab environment

Web Application Security Assessment — PortSwigger Labs

- Identified and exploited broken access control vulnerabilities using Burp Suite; demonstrated horizontal privilege escalation and credential disclosure through parameter manipulation
- Conducted SQL injection testing on DVWA and completed labs covering authentication bypass, XSS, and IDOR

Cloud Security Implementation — GCP (2026)

- Deployed secure cloud infrastructure with logging, monitoring, and access controls on Google Cloud Platform
- Implemented security best practices for identity and access management; documented security architecture and configuration standards

CERTIFICATIONS & TRAINING

- ISC2 Certified in Cybersecurity (CC)
- Google Cybersecurity Professional Certificate

- Cisco Introduction to Cybersecurity
- Udacity Next Generation Tech Booster — Cybersecurity
- TryHackMe — Hands-on labs and learning paths
- Actively pursuing: AWS Certified Security Specialty, SOC 2 & GDPR compliance training

EDUCATION

B.Ed Human Kinetics & Health Education 2020 – 2024

Ekiti State University, Ado-Ekiti