Robert Wevamwo

Security Operations | Security Engineering | Security Architecture

Location: Accra, Ghana

Links: wevbert.pages.dev | linkedin.com/in/wevbert

Summary

Senior cybersecurity analyst with over five years of experience in cybersecurity and financial services technology. Lead an eight-member SOC, combining incident response, SIEM/EDR engineering and vulnerability management with security architecture. CISSP, CCSP and Certified SOC Analyst, with experience deploying enterprise security technologies, developing MITRE ATT&CK-aligned detections and reporting operational performance.

Work Experience

Feb 2023–Present

Senior Cybersecurity Analyst at **Access Bank (Ghana) Plc**

Lead an eight-person SOC delivering 24/7 security operations across Ghana and West African subsidiaries, coordinating incident handling, vendors and operational resilience.

Led CrowdStrike Falcon deployment across approximately 1,359 endpoints, improving endpoint visibility, malware prevention, incident response and audit readiness.

Led implementation of Seceon aiSIEM and CimTrak file-integrity monitoring. Managed log ingestion and normalisation for 300+ assets, sustaining over 99% availability for monitoring and forensic use.

Engineered 45+ SIEM correlation rules mapped to MITRE ATT&CK tactics, reducing false-positive alert volume by approximately 30% and mean time to detect by approximately 25%.

Led response to high-severity incidents, covering containment, forensic investigation with FTK and Autopsy, recovery coordination and post-incident improvements to SOC playbooks.

Ran quarterly vulnerability assessments across 200+ systems using Nessus and Qualys, achieving approximately 85% closure of critical and high findings within agreed SLAs.

Led Infoblox DNS security and Zero Networks microsegmentation deployments to counter malicious domains and lateral movement. Designed an Enterprise Security Architecture Framework being adopted across the bank.

Report incidents, SOC performance and remediation to executives and the board. Support ISO/IEC 27001, PCI DSS, SWIFT CSP and Bank of Ghana control assurance.

soc-operations | siem/edr | incident-response | zero-trust

Aug 2022–Feb 2023

Security Operations Center Analyst at **Access Bank (Ghana) Plc**

Investigated more than 1,000 security alerts monthly, assessed vulnerabilities across over 200 systems, and coordinated incident response and remediation with technology stakeholders.

security-monitoring | alert-triage | vulnerability-management

Earlier Experience

Jul 2021–Aug 2022	**Digital Project Analyst** Access Bank (Ghana) Plc	Coordinated mobile-app development and quality assurance across business, technology, compliance and vendors; contributed to 20% user-adoption growth within three months of launch.
Sep 2020–Jun 2021	**IT Support Analyst** Ghana Data Protection Commission	Provided hardware, software and network support. Implemented access controls, backup procedures and system hardening, and maintained documentation across more than 50 workstations and servers.

Technical Profile

Operations:	Security monitoring, alert triage, incident analysis, containment coordination, detection engineering, forensic investigation, SOC playbooks and performance reporting
SIEM & Endpoint:	Seceon aiSIEM, ArcSight, Securonix, CrowdStrike Falcon, Microsoft Defender and CimTrak file-integrity monitoring
Network & Data:	Forescout NAC, Symantec DLP/SWG, Infoblox DNS security, Zero Networks microsegmentation and Zero Trust
Cloud & Identity:	Google Cloud IAM, cloud logging and monitoring, Active Directory, security architecture review and control design
Assessment:	Nessus, Qualys, CVSS prioritisation, FTK and Autopsy
Frameworks:	MITRE ATT&CK, ISO/IEC 27001, PCI DSS, SWIFT CSP, Bank of Ghana CISD and Ghana's Data Protection Act
Systems:	Windows Server, Linux, PowerShell and Bash
Languages:	English; Akan Twi; Kasem; Spanish (beginner)

Certifications

Security:	CISSP; SSCP; Certified in Cybersecurity (CC) — ISC2
Operations:	EC-Council Certified SOC Analyst; CompTIA Security+
Cloud:	CCSP; Google Cloud Professional Security Engineer
Governance:	PECB ISO/IEC 27001:2022 Lead Implementer; PCI DSS Certified Lead Implementer
AI:	Certified AI Leader, Google Cloud

Education

Expected Mar 2027	**MSc Cyber Security & Digital Forensics** Kwame Nkrumah University of Science & Technology. Completed; formal award expected March 2027.
2016–2020	**BSc Telecommunication Engineering (Honors)** Ghana Communication Technology University. Gold Fields Ghana Foundation Scholar.
2022	**School of Banking Excellence** Access Bank, The Learning Institute, Lagos. Completed with Distinction; Associate Chartered Banker (ACIB), Chartered Institute of Bankers, Nigeria.