

ELIJAH EBENEZER ARMAH JNR

Information Security Operations Manager & Full-Stack Cyber Architect

☎ 0594032521

✉ Available Upon Request

📍 Accra, Ghana

EXECUTIVE SUMMARY

Information Security Operations Center (SOC) Manager & Full-Stack Cyber Architect with over a decade of technical and strategic cybersecurity experience across Ghana's financial sector. Unique hybrid background combining 24/7 SOC leadership (QRadar, Sentinel, Defender EDR), Application Security (OWASP, VAPT, Secure SDLC), Cloud Architecture (Azure/AWS), UI/UX Product Design (Figma, Design Systems, A11y), and Full-Stack Web Development (React, Next.js, Node.js, PHP, REST APIs) with Security-by-Design.

CORE TECHNICAL, DESIGN & SECURITY SKILLS

🛡️ Cybersecurity & SOC Operations

SOC Operations Management, 24/7 Planning, Threat Monitoring, Incident Response, Incident Triage, SOC Playbooks, Threat Intelligence, Security Metrics & KPIs.

🎨 UI/UX Product Design

Figma, Adobe XD, Wireframing, Interactive Prototypes, Design Systems, User Flow, SaaS Dashboard Design, Admin Portals, Web Accessibility (a11y/WCAG).

🔍 SIEM & Threat Monitoring

IBM QRadar SIEM, Microsoft Sentinel, Log Analytics, KQL, Detection Engineering, Alert Tuning, Threat Hunting, Logstash, Elastic Stack, Kibana.

🌐 Web & Full-Stack Development

HTML5, CSS3, JavaScript, TypeScript, React, Next.js, Node.js, PHP, REST APIs, JSON, SQL, MySQL, Git/GitHub, Docker, Full-Stack Architecture.

🦟 Endpoint Security & EDR

Microsoft Defender for Endpoint / EDR, Kaspersky EDR, EDR Policy Development, Secure Score Optimization, Endpoint Hardening, SCCM & Ansible.

🔒 Secure Web Dev & DevSecOps

Security-by-Design, OWASP Top 10 Mitigation, Secure API Development, Input Validation, Secure Session Management, DevSecOps Automation.

🌐 Network & WAF Security

Imperva WAF, F5 BIG-IP, NGINX Security, Azure WAF, Azure Application Gateway, IBM DataPower, DDoS Protection, Network Segmentation.

📋 Compliance & Governance

PCI DSS, ISO/IEC 27001, NIST CSF, Bank of Ghana Cybersecurity Requirements, Ghana Cybersecurity Act, Risk Assessment & Auditing.

KEY SHOWCASE PROJECTS

1. Microsoft Defender EDR Migration

Led enterprise migration from Kaspersky to Defender EDR across Windows and Linux server fleets using Ansible & SCCM automation.

2. SOC Transformation & Operations

Architected 24/7 SOC monitoring, incident response escalation protocols, threat detection engineering, and SOC KPI dashboards.

3. SIEM Evaluation & Implementation

Evaluated and implemented enterprise IBM QRadar and Microsoft Sentinel SIEM platforms with custom KQL detection rules.

4. WAF & DDoS Protection Architecture

Designed WAF and DDoS protection using Imperva, F5/NGINX, and Azure WAF for core internet banking portals and APIs.

5. Application & API Security Program

Managed vulnerability assessments (VAPT) across web banking applications, mobile APKs, and REST APIs adhering to OWASP standards.

6. Imperva Database Activity Monitoring

Implemented Imperva DAM across core database clusters to monitor privileged activity and satisfy Bank of Ghana regulatory audits.

PROFESSIONAL EXPERIENCE

Information Security Operations Manager • Fidelity Bank Ghana 2024 – Present

- **Authoritative Leadership:** Complete management of SOC operations, incident response, and threat detection workloads across banking infrastructure.
- **Executive Briefings:** Escalating critical security threats to the Head of SOC and C-suite leadership.
- **Technical Head of Monitoring:** Technical authority for SIEM, EDR, and enterprise security monitoring services.

Team Lead Application Security Engineer • Universal Merchant Bank 2019 – 2023

- Directed application security reviews, secure SDLC integration, and penetration testing (VAPT) for all digital banking portals and REST APIs.
- Enforced OWASP Top 10 and PCI DSS security controls across web, mobile APK, and core payment systems.

Ag. SOC Manager • Universal Merchant Bank 2021 – 2023

- Supervised 24/7 SOC threat detection, incident containment, and alert triage.
- Mentored SOC analysts, developed threat hunting playbooks, and refined SIEM alert correlation rules.

Azure Cloud Solution Architect • Universal Merchant Bank 2019 – 2021

- Led cloud architecture teams in designing secure Azure hybrid cloud migrations, Azure WAF, and identity protection.

Information Security Consultant • CAL BANK GHANA 2020 – 2021

- Designed and deployed CalBank's SOC room layout, Microsoft Sentinel ingestion pipelines, and SIEM monitoring.

CERTIFICATIONS & ACADEMIC DEGREES

ISACA CISM – Certified Information Security Manager

ISACA CRISC – Certified in Risk and Information Systems

MSc MSc. Cyber Security & Forensics (KNUST)

BSc BSc. Information Technology (Valley View)

EXPERT Certified SOC Manager

EC-COUNCIL CEH v10 – Certified Ethical Hacker

SECURITY WAPT – Web Application Penetration Tester

AZURE Azure Solutions Architect Expert

KPMG PCI DSS Trained Specialist

ELASTIC Elastic Certified Engineer