OLABANJI OKUNOLA

Cybersecurity Engineer · Detection, Threat Analysis & Offensive Security

EU Blue Card Eligible | IT Specialist Visa §19c Ready | Relocation: Germany · UK · Canada · UAE · US

banjhi001@gmail.com +2348077609209 linkedin.com/in/thebanjioflagos github.com/thebanjioflagos
thebanjioflagos.vercel.app

PROFESSIONAL PROFILE

Cybersecurity Engineer with 5+ years of experience in detection engineering, security operations, and offensive security. I build systems that find threats in real time — and break systems to find weaknesses before attackers do.

25%	**200+**	**90%**
Reduction in MTTD/MTTR via engineered IDS deployment	Vulnerabilities found across 65+ engagements incl. CVSS 8–9	Critical/high vulnerability remediation closure rate within SLA

Combines offensive security expertise with defensive engineering — enabling proactive threat detection rather than reactive firefighting. Available immediately. Zero immigration cost to employer under Germany's IT Specialist Visa §19c and EU Blue Card framework.

CORE COMPETENCIES

Detection & SIEM	ELK Stack (Logstash, Elasticsearch, Kibana) · Splunk · Sigma Rules · MITRE ATT&CK · Sysmon · Windows Event Logging · Threat Hunting · Alert Triage · Incident Response · MTTD/MTTR Optimisation
Offensive Security	Web, API, Network & Mobile Pen Testing · OWASP Top 10 · Auth Bypass · Privilege Escalation · Burp Suite · Metasploit · Nmap · SQLmap · Hydra · Nessus · Kali Linux · Black/Grey/White-box Testing
Security Eng.	IDS Development (Python) · Bash · Linux Hardening · Secure Architecture · Fernet · bcrypt · RBAC · Secure File Storage
Network & Server	CCNP/CCNA-Level Networking · VPN & Firewall Hardening · Network Protocol Security · Server Administration · Secure Remote Access
Cloud & DevSecOps	AWS & Azure (Foundations) · Docker Security · CI/CD Pipeline Security · Git · Jenkins · IAM / Identity & Access Control
Compliance	ISO 27001 · NIST CSF · GDPR · CVSS Scoring · Security Audit Reporting · Remediation Planning
Programming	Python · Bash · JavaScript · Flask · Node.js · React · Solidity / Smart Contract Auditing · MongoDB · PostgreSQL · MySQL

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst & Penetration Tester

Kani Technologies Limited (Nigerian cybersecurity consultancy serving financial services & enterprise clients) — Lagos, Nigeria | *September 2023 – Present*

The challenge: no structured threat detection pipeline existed — the organisation relied entirely on reactive incident response. Tasked with building detection capability from zero while simultaneously running offensive assessments.

- Conducted 50+ penetration tests across web applications, APIs, and internal network infrastructure — uncovering 120+ vulnerabilities including 18 critical findings (CVSS 8–9): IDOR, authentication bypass, and privilege escalation. Remediation closure rate: ~90% of critical/high findings resolved within SLA.
- Engineered a Python-based IDS from scratch ingesting live network traffic and system logs, detecting ARP spoofing, DDoS patterns, and SQL injection in real time — reducing MTTD/MTTR by 25% within the first quarter of deployment.
- Built detection logic aligned to MITRE ATT&CK techniques (T1110 brute force, T1021 lateral movement, T1059 command execution), improving threat visibility and enabling faster analyst triage.
- Developed a machine learning phishing detection system using URL feature extraction and NLP classification — achieving 92% detection accuracy and reducing internal phishing incidents by 40%.
- Delivered technical and executive security reports with CVSS scoring, PoC evidence, and prioritised remediation roadmaps — accelerating patch cycles by an average of 30%.
- Implemented ISO 27001 and NIST CSF-aligned security controls, reducing audit non-conformities by 45% and positioning clients for compliance certification.

Freelance Cybersecurity Consultant

Upwork — Remote (Clients: US, UK, Africa) | *May 2022 – January 2023*

International security consultancy across 15+ engagements for SaaS platforms, fintech applications, and cloud-hosted systems. Following conclusion of Upwork engagements, dedicated Q1–Q3 2023 to independent security research, home lab development (SIEM/IDS architecture), and preparation for advanced certifications — culminating in appointment at Kani Technologies.

- Identified 80+ vulnerabilities across authentication systems, APIs, and cloud misconfigurations — including 12 critical findings. Achieved ~85% remediation rate within 30 days through actionable, business-contextualised reporting.
- Conducted black-box and grey-box penetration tests simulating real-world attack scenarios: brute force, credential stuffing, session hijacking, and targeted phishing vectors.
- Designed and deployed encrypted file storage systems using Fernet encryption, bcrypt password hashing, and RBAC — reducing client data exposure risk by 50%.
- Translated technical vulnerability findings into business risk language for non-technical stakeholders, enabling leadership to prioritise and fund remediation efforts effectively.

Network & IT Support Engineer

Total Shield Inc. (IT infrastructure & managed services provider) — Remote | *March 2020 – January 2022*

Infrastructure security and network operations for a distributed remote organisation. Primary focus on hardening, automation, and documentation.

- Configured and hardened VPNs, firewalls, and secure remote access infrastructure, enforcing zero-trust access principles across the organisation.
- Reduced incident and ticket resolution time by 60% through automation of repetitive helpdesk workflows — freeing engineering capacity for higher-value security tasks.
- Investigated and resolved network and endpoint security incidents; performed root cause analysis and implemented controls to reduce recurrence rates and improve uptime.
- Managed server infrastructure, network topology, and security configuration documentation — maintaining audit-ready operational records aligned with ISO continuity planning standards.

KEY PROJECTS — PORTFOLIO EVIDENCE

SIEM-Based Intrusion Detection & Threat Monitoring System

- Built a production-grade ELK Stack SIEM pipeline ingesting Sysmon logs and live network traffic. Implemented Sigma detection rules for brute force (T1110), privilege escalation (T1068), and anomalous network activity. Simulated attacks using Metasploit, Hydra, and Nmap.
- Result: 30% reduction in detection latency. Full attack-to-detection-to-response workflow documented end-to-end. github.com/thebanjioflagos/SIEM-SOC-Portfolio

Machine Learning Phishing Detection System

- Developed a phishing URL classifier using URL feature extraction and NLP techniques. Achieved 92% detection accuracy. Integrated into a simulated email gateway for real-time alerting and analyst triage workflows.
- Result: 40% reduction in simulated internal phishing incidents. Precision/recall metrics documented. github.com/thebanjioflagos/PhishGuard-ML

Real-Time Network Security Monitoring Dashboard

- Built using Python Dash with live packet capture backend. Displays active connections, threat event feeds, and anomaly scores. Designed for SOC-style single-screen monitoring.
- Result: 50% reduction in manual log analysis effort. Screenshots and architecture docs in portfolio. github.com/thebanjioflagos/NetSentinel-Dash

CERTIFICATIONS

Cisco CCNP — Enterprise Networking	2017
Cisco CCNA	2015
CompTIA Security+	2024
Google IT Support Professional Certificate	2020
Computer Professionals Registration Council of Nigeria (CPN)	2016
OSCP — Offensive Security Certified Professional	***In Progress***

EDUCATION

B.Sc. Computer Science | University of Lagos, Nigeria | Completed: 2016

Programme included a structured industry placement period and final-year research focus on network security architecture, extending the standard programme duration. No academic interruptions.

ADDITIONAL CONTEXT FOR INTERNATIONAL APPLICATIONS

Visa Status	Germany & EU: Eligible for IT Specialist Visa §19c and EU Blue Card — zero employer immigration cost beyond standard employment letter. US: Open to H-1B sponsorship (employer-sponsored) or O-1A Extraordinary Ability visa pathway supported by published security research and public portfolio. UK/Canada/UAE: No sponsorship complexity for skilled worker routes.
Language	English — Professional working language across all international client engagements.

Remote Track	3+ years international remote delivery across US, UK, and African markets. Comfortable with async workflows, European timezone overlap, and cross-cultural teams.
Availability	Immediate. Notice period: 4 weeks.

References available on request · Portfolio: thebanjioflagos.vercel.app · GitHub: github.com/thebanjioflagos