IBRAHIM YUSUF

Security Engineer

Email: ibrahim.a.yusuf741@gmail.com | GitHub: https://github.com/KoredeSec | Linktree: https://linktr.ee/KoredeSec

PROFESSIONAL SUMMARY

Security engineer with hands-on experience across the full security lifecycle from penetration testing and detection engineering to cloud infrastructure hardening and governance. Completed two structured training programmes (Cyblack SOC Academy and AWS re/Start) and a six-sprint security internship spanning threat intelligence, cloud security, GRC, and SOC operations. Delivered multiple independent projects across AWS, Azure Sentinel, Docker, and Python, all with working deployments. Graduated with a B.Sc. in Cybersecurity, Osun State University, 2026.

EDUCATION

B.Sc. in Cybersecurity — Osun State University, Osogbo, Nigeria **2022 - 2026**

- Served as President, Nigeria Association of Cybersecurity Students (NACSS-UNIOSUN) — 500+ member community
- Organised ISC2 CC bootcamps and hands-on security labs for student cohorts
- Bridged academic curriculum and industry practice through structured learning programs and external partnerships

TRAINING & EXPERIENCE

Security Engineering Intern, Cyblack Internship – Remote | January - April 2026

- Conducted a full penetration test on a live vulnerable banking application (VulnBank) using Burp Suite, independently discovering and exploiting 7 vulnerabilities (SQL injection, JWT manipulation, mass assignment, race condition, IDOR, XSS, SSRF) and mapping the attack chain to the Cyber Kill Chain
- Authored 8 KQL Scheduled Query Rules in Microsoft Sentinel covering credential stuffing, phishing payloads, WannaCry C2, XWorm persistence, and AsyncRAT communications, each mapped to MITRE ATT&CK with entity mappings for automatic incident enrichment
- Led Team 7's cloud security sprint, deploying Microsoft Defender for Servers with JIT VM access and a Logic App playbook for automated incident escalation
- Authored a Privileged Account Policy (P7S-PAP-01) aligned to ISO/IEC 27002:2022, NYDFS 23 NYCRR 500.07, and PCI-DSS, with MFA enforcement, bastion host access, and a dual-approval Break-Glass procedure
- Profiled three government-sector threat actors in OpenCTI using the Diamond Model; extracted and categorised 60+ IOCs from WannaCry, XWorm, and AsyncRAT malware samples

SOC Analyst Intern, Cyblack SOC Academy – Remote | September - December 2025

- Performed malware triage on 30+ samples using VirusTotal hash scanning and OSINT enrichment, producing written IOC reports
- Ran credentialed Nessus scans across lab environments, triaged findings by CVSS score, and drafted remediation recommendations
- Automated patch deployment for common CVEs using Ansible playbooks, cutting manual remediation steps
- Investigated simulated security incidents using SIEM log analysis and threat intelligence feeds (OTX, AbuseIPDB)

Cloud Engineering Trainee, AWS re/Start Program – Remote | August - November 2025

- Completed 40+ hands-on labs covering EC2, VPC, S3, CloudTrail, KMS, SNS, and EventBridge
- Built and documented cloud architecture patterns around least-privilege IAM and audit logging
- Developed proficiency in CI/CD fundamentals, infrastructure automation, and AWS Well-Architected Framework principles

PROJECTS

Microsoft Sentinel Home SOC Lab · *Stack: Azure VM · Microsoft Sentinel · KQL · Logic Apps · Honeypot* → View on GitHub

- Deployed an Azure VM as a honeypot, forwarded live attack logs to Sentinel, and built a real-time attack map visualisation
- Created automated incident response workflows using Logic Apps alerts fired within minutes of detected events
- Wrote KQL rules targeting failed RDP logins (Event ID 4625), enriched attacker IPs with GeoIP watchlist data, and automated metadata logging to a custom Sentinel table via Logic App

Threat-Intel Aggregator · *Stack: Python · Flask · OTX · AbuseIPDB · VirusTotal · Slack API* → View on GitHub

- Built a Python tool that pulls IOCs from OTX, FeodoTracker, AbuseIPDB, and VirusTotal, deduplicates across feeds, and geolocates threats on an interactive map
- Integrated Slack and email alerting — live IOC notifications delivered to a test channel with zero manual intervention
- Reduced IOC review time by consolidating 4 separate threat feeds into a single normalised dashboard

StackDeployer · *Stack: Bash · Docker · Nginx · SSH · Git* → View on GitHub

- Production-grade Bash script that fully automates Dockerised app deployment on remote Linux servers. It does repo pull, Docker setup, Nginx reverse proxy config, and secure SSH handshake in a single command
- Eliminated an estimated 15+ minutes of manual deployment steps per release cycle

Risk Assessment Model for Cloud-Based LLM · *Stack: AWS Bedrock · EC2 · OpenSearch · Flask · LangChain · IAM · CloudTrail* → View on GitHub

- Deployed a RAG chatbot on AWS Bedrock (Llama 3.1 8B) and built a 35-test-case security framework across LLM, RAG, and cloud layers
- Shipped 14 hardening controls, raising the Security Posture Score from 67.09% to 89.60% with 100% vulnerability remediation

Linux VPC Builder · *Stack: Python · Linux Networking · Docker · iptables · iproute2* → View on GitHub

- Built a production-ready CLI tool that recreates cloud VPC functionality entirely on Linux using container networking primitives such as subnets, routing tables, and security groups with no cloud dependency
- Implements subnet isolation, custom routing tables, and iptables-based security group rules mirroring AWS VPC behaviour without a cloud account

SKILLS

Cloud & Infrastructure: AWS (EC2, VPC, S3, CloudTrail, KMS, SNS, EventBridge, IAM, Bedrock, OpenSearch), Azure (VMs, Sentinel, Logic Apps), Docker, Nginx, Apache2, SSH/SCP, Git

Security & SOC: Threat Intelligence (OTX, FeodoTracker, AbuseIPDB, VirusTotal), SIEM (Microsoft Sentinel), Microsoft Defender for Cloud, KQL, Burp Suite, OpenCTI, MITRE ATT&CK, Nessus, Ansible, Incident Response, Log Analysis, Honeypot Deployment

Languages & Scripting: Python (Flask, LangChain, automation, threat intelligence tooling), Bash, SQL, YAML, JSON, HTML/CSS

GRC & Compliance: ISO/IEC 27002, NYDFS 23 NYCRR 500.07, PCI-DSS, Privileged Access Management, Policy Authoring, WCAG 2.1, NIST SP 800-30

CERTIFICATIONS

- Microsoft SC-200: Security Operations Analyst · *2025*
- Google Cybersecurity Professional Certificate · *2025*
- AWS Certified Cloud Practitioner · *2026*