

Abdulmuiz Annafi

AI Security & Threat Intelligence Engineer

oladipupoabdulmuiz@gmail.com | +234 902 0676 314 | linkedin.com/in/annafiabdulmuiz | github.com/Abdulmuiz635

PROFESSIONAL SUMMARY

AI Security and Threat Intelligence Engineer. I build pipelines and AI tooling that modern threat operations run on, moving raw threat and vulnerability data through ingestion, ECS normalization, CTI enrichment, Sigma detection, and MITRE ATT&CK mapping, then layering models on top that analyze cases, validate findings, and drive response. Every layer is measured on whether its output holds up when a real decision is on the line. ISC2, AWS, and Microsoft certified, with a B.Sc. in Cybersecurity.

TECHNICAL SKILLS

AI & MLSecOps: TensorFlow, Scikit-Learn, Keras, Vertex AI, LLM & MCP Integration, Anomaly Detection, Model Evaluation & Benchmarking, MLSecOps

Threat Intelligence & Detection: CTI Lifecycle, MITRE ATT&CK, Sigma Detection, ECS Normalization, OSINT, MISP, VirusTotal, NVD / CISA KEV / EPSS, Threat Hunting, Incident Response

Security Engineering: Penetration Testing, Vulnerability Management, SIEM, Tenable (Nessus), Burp Suite, Wireshark, CrowdStrike, Wiz, Cortex (XDR/SOAR), TLS/PKI, Zero-Trust

Languages & Backend: Python, Go, JavaScript/TypeScript (Node.js), SQL, FastAPI, Flask, Express, REST APIs, Async Microservices, WebSockets

Cloud & Data: Google Cloud Platform, AWS, Azure, Docker, Docker Swarm, CI/CD, BigQuery, Firebase, PostgreSQL, MySQL, MongoDB, OpenSearch

PROFESSIONAL EXPERIENCE

Cyber Threat Intelligence Analyst – CyberSOC Africa

Jan 2026 – Present | Lagos, Nigeria

- Design and build AI-augmented security tooling in the R&D division that automates threat detection and triage pipelines, with rubric-based scoring to measure the reliability and explainability of AI-driven detection.
- Work the end-to-end CTI lifecycle, combining manual analysis with automated workflows to identify, track, and mitigate emerging threats across the African threat landscape.
- Built automation and web scrapers that continuously surface impersonation and negative mentions of client VIPs across the open web, triggering real-time alerts for rapid takedown.

Site Reliability & Platform Security Engineer – ZerOPaper OU (Contract)

Apr 2026 - Jul 2026 | Remote, Estonia

- Built and secured the infrastructure layer of a multi-tenant PaaS that deploys customer workloads from Git to Docker Swarm on Hetzner.
- Engineered hardened multi-tenant isolation across the cluster, enforcing network segmentation, secrets management, and least privilege access on shared infrastructure.
- Designed the Git-to-deploy pipeline with automated builds, private container registries, and reproducible rollouts, enabling self-service customer onboarding.

MLSecOps Engineer – IRIS-SOC

Feb 2025 - Jan 2026 | Remote, Nigeria

- Built the intelligence pipeline of an AI-native SOC platform, from ingestion and ECS normalization through CTI enrichment, Sigma detection, and MITRE ATT&CK mapping.
- Integrated Vertex AI and a custom security model that analyzes cases and drives automated response, backed by BigQuery log storage and case lifecycle management.
- Established evaluation pipelines and scoring rubrics for model outputs, keeping automated security decisions reliable and explainable.

Cybersecurity Intern – Access Bank Plc (Information & Cybersecurity Group)

Apr 2024 - Oct 2024 | Lagos, Nigeria

- Supported SOC operations across incident response, threat monitoring, and threat hunting with enterprise SIEM tooling, alongside senior analysts.
- Performed penetration testing and vulnerability analysis with Tenable Nessus to detect exposures and strengthen the bank's security posture.

PROJECTS

SideDoor - Session Hijack Detection Lab

Built a Python detection engine and custom Sigma rules that catch MFA-bypass session replay by comparing the context a session was issued under against its later use, using multi-signal correlation and false-positive tuning validated by automated tests.

Technologies: *Python, Sigma, OpenSearch, TLS/JA4 fingerprinting*

AI-Augmented Security Advisory Pipeline

Deployed, client-facing pipeline that ingests NVD, CISA KEV, and GitHub Advisory data, vets each CVE against a client's tech stack, prioritizes by exploited status and severity, and generates formatted monthly advisory reports with a human-review checkpoint, replacing a manual analyst workflow.

Technologies: *Python, NVD API, CISA KEV, GitHub Advisory*

External Attack Surface Management (EASM) Platform

Multi-client platform that continuously discovers an organization's external footprint (subdomains, exposed IPs, ports, services, TLS certificates) and correlates it against live NVD, CISA KEV, and EPSS data to surface prioritized, exploitable vulnerabilities through an analytics dashboard.

Technologies: *React, FastAPI, Python, MongoDB*

Email Impersonation Detection Tool

OSINT-driven engine that generates email variants via systematic name-mangling and validates each through DNS/MX resolution and SMTP probing to expose live impersonation infrastructure, with VIP management, WebSocket progress streaming, and automated alerting.

Technologies: *FastAPI, Python, OSINT, DNS/SMTP*

Hybrid Network Intrusion Detection System

Hybrid IDS fusing rule-based signature detection with deep-learning neural networks for anomaly detection, reducing false positives while improving detection precision.

Technologies: *Python, Deep Learning, Scikit-Learn*

AI Incident Response & Vulnerability Agent (Visa Harness)

Built an IR and vulnerability agent on Visa's open vulnerability harness that does not just generate findings, it validates them. It runs adversarial verification to confirm a finding is exploitable, requires multiple agents to agree before a result is kept, and grades proposed fixes through a review panel, so only triage an analyst can act on reaches a human.

Technologies: *Python, LLM Agents, Visa Vulnerability Harness, Adversarial Verification*

EDUCATION

B.Sc. Cybersecurity - Al-Hikmah University

Second Class Honours (Upper Division), CGPA 4.25 / 5.0

CERTIFICATIONS

- Certified in Cybersecurity (CC) - ISC2
- AWS Certified Cloud Practitioner - Amazon Web Services
- Microsoft Certified: Data & AI Security Engineer - Microsoft
- Google Cybersecurity Professional Certificate - Google
- Certified LLM Security Professional (CLLMSP) - Red Team Leaders
- Cisco Certified Network Associate (CCNA) - Cisco
- Model Context Protocol, Introduction + Advanced Topics - Anthropic

COMMUNITY

General Secretary, Robotics & AI Nigeria (RAIN), 2024-25 | Technical Team Lead, Google DSC, 2023-24 | Volunteer, Okapi Children Cancer Foundation, 2023-present