ISMAIL OLANREWAJU

Cybersecurity Analyst | Defensive Security Specialist
ismailolanrewaju0@gmail.com | cyberismail.com | linkedin.com/in/ismail-olanrewaju-093a6a221

PROFILE

Cybersecurity Analyst with 4+ years across SOC operations, threat detection, incident response, and IT security. Daily experience with Splunk SIEM, vulnerability management, and multi-source intelligence analysis in regulated environments. Strong at translating complex security findings into clear, actionable reports for technical and non-technical stakeholders. Hands-on builder — from Splunk dashboards in production to offensive/defensive lab environments at home.

CORE SKILLS

SIEM & Detection: Splunk (SPL, dashboards, alerting, correlation rules), log management, event correlation, detection engineering, security monitoring
Threat Intelligence: MITRE ATT&CK, Cyber Kill Chain, OSINT, IoC/TTP analysis, threat hunting, CTI, VirusTotal API
Incident Response & DFIR: Full IR lifecycle, FTK Imager, Volatility, malware analysis, playbook development
Vulnerability Management: Nessus, Qualys, OpenVAS, risk-based prioritisation, remediation reporting
Network & Endpoint: TCP/IP, firewalls, IDS/IPS, Active Directory, IAM, Windows/macOS/Linux, Wireshark, endpoint hardening
Frameworks & GRC: NIST CSF, ISO 27001, MITRE ATT&CK, ITIL V3, GDPR awareness, change control, security policy
Scripting & Tools: Python, PowerShell, Bash, JavaScript, Microsoft 365, structured reporting

CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ITIL V3 Foundation

EXPERIENCE

SOC Analyst
Sep 2025 – Present
Amdari

- Perform real-time security monitoring and threat detection across customer infrastructure using Splunk SIEM, correlating log data from endpoints, network devices, firewalls, and OSINT feeds to maintain situational awareness and identify indicators of compromise (IoCs).
- Investigate and triage security incidents through the full lifecycle — detection, analysis, containment, eradication, and post-incident review — classifying events against the MITRE ATT&CK kill chain and maintaining audit-ready case documentation against SLAs.
- Conduct proactive threat hunting across enterprise environments, analysing threat actor tactics, techniques, and procedures (TTPs) to identify gaps in detection coverage and develop new use cases for SIEM correlation rules.
- Tuned SIEM detection content, correlation rules, and alert thresholds to reduce false positive rates by ~30%, improving signal-to-noise ratio and freeing analyst capacity for higher-priority threat investigations.
- Built and deployed a real-time Splunk Cloud dashboard with automated threshold-based alerting for SSH brute force activity. It caught threats the previous detection setup missed and became a standard SOC monitoring tool used daily across the team.
- Conducted vulnerability assessments using Nessus, Qualys, and OpenVAS; produced risk-rated findings with prioritised remediation recommendations communicated to both technical teams and non-technical stakeholders.
- Authored analytical playbooks, incident response procedures, and SOC process documentation adopted team-wide, standardising triage workflows, escalation paths, and the quality of intelligence outputs.
- Identified an emerging SSH brute force campaign through proactive cyber threat intelligence (CTI) monitoring before it triggered any existing alerts. Developed new detection rules, validated them against live traffic, and delivered a targeted threat briefing to senior management.
- Collaborate with senior analysts and cross-functional security teams to investigate active threats, applying MITRE ATT&CK, NIST CSF, and Cyber Kill Chain frameworks to guide analysis and recommend follow-up actions to stakeholders.

IT Systems & Security Analyst
Apr 2022 – Dec 2022
United Bank of Africa (UBA)

- Built incident and asset reporting frameworks from scratch across 200+ endpoints in a multi-branch banking environment — gave management their first data-driven view of system health, security posture, and operational risk. Reports directly informed risk prioritisation and IT spending decisions.
- Investigated suspicious account activity, unauthorised access attempts, and anomalous behaviour across the network; conducted root cause analysis, documented findings with risk assessments, and escalated confirmed security incidents with clear remediation recommendations.

- Administered endpoint security controls, user access management (Active Directory), and security policy enforcement across Windows, macOS, and Linux environments, ensuring compliance with internal security standards.
- Triaged and resolved IT and security incidents in line with ITIL procedures and SLA targets, improving average resolution time through better documentation, knowledge sharing, and structured escalation paths across branches.
- Led a Trust-wide OS upgrade and hardening programme to address legacy system vulnerabilities — reduced downtime by ~20%, eliminated a class of recurring incidents, and strengthened the organisation's overall security posture.

Technical IT Support Analyst *Oct 2020 – Mar 2022*

Essence of Greenfield

- Built and maintained a WordPress e-commerce site end-to-end: hosting, SSL, DNS, payment integration, WooCommerce inventory, and email infrastructure. The site became the primary revenue channel for the business.
- Provided daily IT support across hardware, software, and network issues; achieved 70% first-contact resolution rate and reduced repeat incidents through structured troubleshooting documentation.
- Set up Google Analytics and Facebook Pixel tracking, giving management actionable data on customer behaviour, traffic sources, and campaign performance for the first time.
- Performed regular backups, plugin updates, security patches, and malware scans to keep the site secure and reduce vulnerability exposure.
- Documented IT processes and built an internal knowledge base that empowered non-technical staff to handle routine issues independently.

EDUCATION

MSc Cyber Security (Merit) | University of Chester *2023 – 2024*
Risk Management, Digital Forensics & IR, Penetration Testing, ISO 27001

BSc Information Technology (First Class) | Pratap University *2017 – 2020*

HOMELAB & PROJECTS

Cybersecurity Home Lab — Threat Detection & Offensive Security

- Built a virtualised security lab in VirtualBox simulating enterprise network segments. Deployed Splunk as the SIEM for log ingestion, correlation, and alerting. Configured Kali Linux against vulnerable targets (Metasploitable, DVWA) for penetration testing and exploitation practice. Integrated log forwarding from target VMs into Splunk to develop and validate custom detection rules against live attack traffic — bridging offensive testing with defensive monitoring.

Threat Intelligence — Spear Phishing Investigation

- Analysed a targeted phishing campaign using email header forensics (SPF/DKIM/DMARC), traced source attribution, validated IoCs via AbuseIPDB and VirusTotal, and produced a defensive assessment with remediation recommendations.

Digital Forensics — Windows Breach Investigation

- Conducted full DFIR on a simulated breach: disk/memory imaging (FTK Imager, DumpIt), RAM analysis (Volatility), static and dynamic malware analysis. Delivered a professional remediation report.

Penetration Testing — WordPress/Linux

- Ran a structured vulnerability assessment using Nmap, Nessus, WPScan, Metasploit, and Hydra. Identified 6 vulnerabilities across 3 severity tiers with exploitation evidence and prioritised remediation.

Social Engineering Awareness Tool

- Built a web-based security awareness training tool with interactive phishing simulations and real-time scoring (JavaScript, HTML, CSS), focused on human-layer threat reduction and measurable awareness improvement.

ADDITIONAL

Founder | Meldcrew — B2B platform connecting business owners for brand partnerships across African markets. Built end-to-end from market research and competitor analysis through to technical deployment and stakeholder outreach.

Founder | Staticish — automated web-design service: a Node.js / Python pipeline that generates, deploys and markets client websites. Designed, built and shipped live hotel sites end-to-end (React, Netlify).

Student Experience Representative — Gathered and analysed student feedback through surveys and direct engagement, presented consolidated findings to academic staff in formal meetings, and influenced departmental decision-making on course and facility improvements.