OLUWATOBI AWOLUDE

SOC Analyst | IT Security Engineer | Cloud Engineer

Newcastle, United Kingdom | +44 7727 111 482 | oluwatobi.awolude@outlook.com | oluwatobiawolude.co.uk

PROFILE

SOC Analyst and Cloud-capable IT Security professional with 5+ years running enterprise security, cloud, and network operations across Microsoft Sentinel, Defender XDR, Azure, and Entra ID. Operates a global Tier 2 / Tier 3 SOC single-handed with zero supervision, closing 20+ tickets a day at a 30-minute MTTR while handling daily phishing cases for a worldwide user base. Authors KQL detections, drives Tenable-led vulnerability remediation in line with ISO 27001 and GDPR, and brings a strong cloud engineering foundation with hands-on Terraform, Azure DevOps, Docker, and CI/CD. Looking for a Cybersecurity, IT Security, or Cloud Engineer role where proactive detection and automation have direct business impact.

KEY ACHIEVEMENTS

- Closes 20+ SOC tickets per day at a 30-minute MTTR across Sentinel, Defender XDR, Zscaler, and BeyondTrust, owning every alert from triage to post-incident review.
- Handles daily phishing cases for a globally distributed user base, containing credential and payload-based attacks within the same shift they are reported.
- Engineered custom KQL detections and hunt queries in Sentinel that surfaced threats default rules missed and lifted overall detection fidelity.
- Keeps the estate audit-ready against ISO 27001 and GDPR by driving Tenable Nessus scans, remediation tracking, and fix validation with asset owners.
- Supported 5,000+ BT and EE users across UK sites while meeting SLAs on VPN, Windows 10/11, Intune, and Active Directory.
- Bridges security and cloud engineering: trained in Terraform, Docker, Jenkins, and Azure DevOps Pipelines (AppMigro 2024 to 2025) and applies security-as-code to detection content.

CORE SKILLS

- **Security Operations:** SOC Tier 2 / Tier 3, incident response, threat hunting, triage, chain-of-custody documentation
- **SIEM and Detection:** Microsoft Sentinel, KQL, log correlation, detection engineering, SOAR playbooks
- **Endpoint and Network Security:** Microsoft Defender XDR and for Endpoint, Zscaler, BeyondTrust, Aternity, phishing triage
- **Vulnerability Management:** Tenable Nessus, patch and compliance reporting, remediation tracking
- **Cloud and Identity:** Microsoft Azure, Entra ID, Conditional Access, Intune, Autopilot, SC-900 aligned
- **Cloud Engineering:** Azure App Services, Terraform, Azure DevOps Pipelines, Docker, Jenkins, Git, CI/CD, IaC
- **Networking:** TCP/IP, routing and switching, VLANs, VPN, DNS, DHCP, NOC monitoring, MTTR management
- **Systems and Platforms:** Windows Server 2012 to 2019, Active Directory, Group Policy, SCCM, Citrix, Microsoft 365
- **Compliance and Frameworks:** ISO 27001, GDPR, NIST-aligned controls, ITIL v4 service management
- **Scripting and Automation:** PowerShell, Bash, KQL, YAML for pipelines

PROFESSIONAL EXPERIENCE

IT Analyst, Security (SOC Analyst) | Mott MacDonald *Jan 2025 to Present*

Newcastle, UK (Hybrid)

- Close 20+ tickets per day at a 30-minute MTTR as an independent Tier 2 / Tier 3 analyst across Sentinel, Defender XDR, and Zscaler, owning every alert from triage to review.
- Respond to daily phishing cases for the global user base: analyse headers and payloads, extract IoCs, purge mailboxes, and harden detections to stop repeat campaigns.
- Engineer custom KQL detections and hunt packs that surface threats default rules miss, raising detection quality across identity, endpoint, and network telemetry.
- Drive vulnerability management in Tenable Nessus: scope scans, track remediation with asset owners, and validate fixes to keep the risk register clean.
- Tighten identity and privileged access through Entra ID Conditional Access and BeyondTrust session monitoring, reducing standing privilege exposure.
- Produce control evidence for ISO 27001 and GDPR, mapping SOC activity to audit requirements.
- Treat detection content as code: version-controlled in Git and deployed through Azure DevOps Pipelines for repeatable rollouts.

IT Analyst, Application and Cloud Support | Mott MacDonald *Apr 2023 to Mar 2025*

Newcastle, UK (Hybrid)

- Delivered L3 support across Microsoft 365, Azure, ServiceNow, AutoDesk, and Bentley for a global engineering user base, protecting uptime on critical platforms.
- Hardened Intune, Autopilot, and Entra ID configurations, rolling out Conditional Access, device compliance, and zero-touch provisioning.
- Troubleshot Azure App Services, virtualisation, and identity issues alongside platform teams to unblock upgrades and integrations.
- Wrote knowledge-base articles, runbooks, and process flows that cut repeat tickets and lifted first-time fix rates.
- Partnered with security on escalations and early Defender adoption, which led to my internal move into the SOC role.

IT Support Engineer, 2nd and 3rd Line | BT / EE via Hays Talent Solutions *Oct 2021 to Mar 2023*

Gosforth, North Tyneside and Remote

- Supported 5,000+ BT and EE users across UK call centres and remote sites, hitting SLAs on Windows 10/11, Microsoft 365, VPN, and Active Directory incidents.
- Provisioned users and devices through AD and Intune, enforced Group Policy and Conditional Access baselines, and executed Windows patching through SCCM.
- Acted as backfill engineer across UK sites for upgrades, new-site rollouts, and decommissioning projects.
- Worked with the cybersecurity team on phishing triage, access reviews, and incident escalations, sharpening the security mindset I use in the SOC today.

IT Analyst, Remote Infrastructure and Cloud | Naynav Engineering Services *May 2019 to Sep 2021*

Newcastle, UK (Remote)

- Delivered infrastructure and cloud support for a remote workforce, covering Intune policies, Conditional Access, and Microsoft 365.
- Performed compliance checks and helped implement cloud security policies across Entra ID and Azure workloads.
- Documented SOPs and onboarding guides that reduced repeat queries and scaled operational knowledge.

NOC Engineer and Network Surveillance Specialist | Biswal Telecoms *Sep 2017 to Apr 2019*

Lagos, Nigeria

- Monitored telecom networks 24 by 7, triaged critical alarms across regions, and coordinated field engineers to hit MTTR and SLA targets.
- Produced incident reports and shift handovers that kept the NOC synchronised and customer-facing services stable.
- Built the TCP/IP, routing, and fault-management fundamentals that still underpin how I investigate today.

CERTIFICATIONS AND TRAINING

- Certified Ethical Hacker (CEH v12), EC-Council
- ISC2 Certified in Cybersecurity (CC)
- Microsoft SC-900: Security, Compliance and Identity Fundamentals
- AWS Certified Cloud Practitioner
- CompTIA Network+
- ITIL v4 Foundation
- Azure DevOps and IaC training, AppMigro, 2024 to 2025 (Terraform, Docker, Jenkins, Git, CI/CD)
- In view: CompTIA Security+, Microsoft MD-102, Microsoft AZ-900, ServiceNow Admin

EDUCATION

B.Tech, Computer Science | Ladoke Akintola University of Technology, Nigeria *2011*

PROFESSIONAL MEMBERSHIPS

ISC2 | EC-Council | BCS (British Computer Society)

References available on request