Emmanuel Adegbite

Cybersecurity Analyst · SOC & Detection

m33tdamilare@gmail.com · linkedin.com/in/thedamilare · github.com/cybernuel · cybernuel.github.io
Full and permanent right to work in the UK, no sponsorship required.

PROFILE

Cyber Security Advisor at The Cyber Helpline, supporting victims of cybercrime, with SOC experience in alert triage, investigation and detection engineering on Microsoft Sentinel and Defender for Endpoint. Background in IT service desk and customer support, which shapes a calm, people-first approach to incidents. Writer of the weekly Cybernuel newsletter.

EXPERIENCE

Cyber Security Advisor (Volunteer) · The Cyber Helpline (remote) — 2025 – present

- Support victims of cybercrime and online harm with clear, practical recovery steps.

SOC Analyst · Amdari, London — Feb 2026 – Aug 2026

- Triaged and investigated security alerts using Microsoft Sentinel and Defender for Endpoint.
- Mapped activity to MITRE ATT&CK and tuned detections to reduce noise.

IT Service Desk Analyst · PayPoint, UK — 2022 – 2025

- Handled incidents, access issues and user support at scale.

IT Support · Dots ICT and Femtech, Nigeria — Earlier

- Hardware, network and customer-facing technical support.

PROJECTS

- **SOC automation pipeline:** Wazuh → n8n → TheHive → VirusTotal → AI summary → Telegram alerting.
- **Microsoft Sentinel detection labs:** business email compromise and impossible-travel analytics rules in KQL.
- **Security labs on GitHub:** honeypot, YARA malware detector, network anomaly detector, Active Directory enumeration and privilege escalation, phishing simulation.

EDUCATION

MSc Cybersecurity · Edinburgh Napier University
BEng Computer Engineering · University of Ilorin
National Diploma, Computer Science · Gateway Polytechnic

CERTIFICATIONS

CompTIA Security+ · CompTIA CySA+ · Microsoft SC-200 · Microsoft AZ-900 · Cisco Ethical Hacker · arcX Cyber Threat Intelligence Analyst

SKILLS

Microsoft Sentinel, KQL, Defender for Endpoint, Wazuh, TheHive, n8n (SOAR), VirusTotal, MITRE ATT&CK, OSINT, Azure, incident handling, clear written communication.