Tomiwa Oladejo

Buckinghamshire, United Kingdom • tommdej@gmail.com • (+44) 7342-897-651 •
tomiwa-oladejo.github.io/Portfolio/

SUMMARY

Cybersecurity graduate with hands-on experience in SIEM alert triage, incident investigation, and behavioural threat detection. Skilled in using Microsoft Sentinel to simulate and analyse real-world threats, write detection rules in KQL, and produce structured response documentation. Curious, collaborative, and committed to continuous development.

RELEVANT PROJECT EXPERIENCE

SOC Simulation – Microsoft Sentinel Threat Detection Lab

- Deployed and monitored a honeypot VM in Azure, collecting logs via Log Analytics Workspace.
- Investigated failed login events (Event ID 4625) and analysed trends using KQL queries.
- Enriched alerts with IP threat intelligence and visualised activity in Sentinel workbooks.
- Simulated escalation procedures aligned with SOC-to-IR handover logic.

Threat Intelligence & Real-World Breach Analysis

- Analysed the Alibaba cloud breach; mapped attacker TTPs to the Cyber Kill Chain.
- Authored a risk register and remediation plan aligned with ISO 27001 principles.
- Gained understanding of how to apply threat intelligence to real-world breach scenarios.

Threat & Vulnerability Analysis Lab

- Performed system scanning and threat identification using OpenVAS and Nmap, uncovering 29 vulnerabilities including weak service configurations.
- Produced technical reports outlining root causes, exploitability, and potential threat actor profiles aligned with attacker goals.
- Prioritised vulnerabilities by risk and likely impact, and proposed structured, actionable remediation guidance.

EDUCATION

Bsc (Hons) Computer Systems (Cyber Security)

Nottingham Trent University, Nottingham • 2.1 (2023)

CERTIFICATIONS & TRAINING

Security+

CompTIA • Actively preparing

Microsoft Learn • Azure Fundamentals, KQL Querying, Terraform Concepts

SKILLS

SIEM & Detection Tools: Microsoft Sentinel • KQL • Log Analytics Workspace

Security & Infrastructure: Firewalls (basic), Active Directory (intro), Wireshark • Nmap • OpenVAS

Scripting: PowerShell (intro) • Python (basic) • Bash (basic)

Concepts: Incident response lifecycle • Cyber Kill Chain • Threat Intelligence

Soft Skills: Analytical • Problem-solving • Communication • Problem Solver • Collaborative • Organised • Proactive learner • Independant • Adaptable