Tomiwa Oladejo

Milton Keynes, Buckinghamshire | +44 7342897651 | tommdej@gmail.com

Profile

Cybersecurity graduate with laboratory hands-on experience in information security, cloud monitoring, and incident response. Skilled in log analysis, vulnerability management and policy writing. Practical understanding of ISO 27001-aligned security frameworks, Microsoft Sentinel, and Azure-based security solutions. A clear communicator, problem-solver, and team-oriented with strong documentation and risk awareness skills.

Education

Nottingham trent university, nottingham | September 2020 – July 2023

- BSc (Hons) Computer Systems (Cyber Security) - Degree Classification: 2:1

Portfolio

https://tomiwa-oladejo.github.io/Portfolio/

Relevant Experience

Microsoft sentinel & azure lab (cloud-based siem and monitoring)

- Created and configured a honeypot VM in Azure, simulating brute-force login attacks to test detection workflows.
- Connected VM logs to Log Analytics Workspace (LAW) and integrated with Microsoft Sentinel to centralise security event analysis.
- Queried logs using KQL (Kusto Query Language) to detect failed login events (Event ID 4625) and correlated IP data via Sentinel Watchlists.
- Built a real-time attack map dashboard using Sentinel Workbooks and JSON configuration to visualise threat origin and frequency.
- Gained hands-on experience in log enrichment, SIEM correlation, threat detection, and incident visualisation in a simulated enterprise environment.

Security incident response & vulnerability management

- Detected and triaged 29 high-risk vulnerabilities using OpenVAS and Nmap in a Metasploit lab simulating enterprise infrastructure.
- Conducted exploitation testing on PostgreSQL misconfigurations and IRC backdoors, producing technical reports and mitigations.
- Recommended enterprise-aligned security controls including IDS (SNORT), strong access policies, and firewall rule adjustments.

Isms development - alibaba breach case study

- Designed an Information Security Management System (ISMS) in response to a real-world data breach affecting over 1.1 billion user records.
- Developed risk registers, escalation paths, and stakeholder-aligned control strategies using principles from ISO 27001 and data protection legislation.

- Evaluated Disaster Recovery and Business Continuity policies and suggested resilience improvements.

Denial of service attacks and mitigations

- Researched common DoS attack types targeting transport and application layers, including SYN Flood, HTTP Flood, and Slowloris.
- Assessed threat impacts on availability and resilience of enterprise systems.
- Recommended mitigations including TCP SYN cookies, WAFs, and reverse proxies to enhance continuity and protect against downtime.
- Connected findings to real-world disaster recovery and security control strategies.

Computer forensics & investigation

- Extracted and analysed mobile device data using Cellebrite Physical Analyzer, recovering both logical and physical evidence.
- Reconstructed digital timelines and compiled court-admissible forensic reports linking evidence to simulated criminal activity.
- Practiced chain-of-custody principles, metadata inspection, and secure report preparation.

Email spam filter development

- Developed a deep learning-based spam detection model in TensorFlow/Keras, achieving 92% accuracy on real email datasets.
- Applied natural language processing (NLP) techniques, tokenization, and evaluation using AUC/confusion matrices.
- Simulated email threat classification workflows applicable to enterprise environments.

Core Skills

- Security Operations & Analysis: Incident Response | Vulnerability Management | SIEM Monitoring | Log Analytics | IDS/IPS (SNORT)

- Compliance & Governance: ISO 27001 (familiar) | GDPR & PIPL Contexts | Risk Register Creation | Security Policy Development

- Documentation & Communication: Security Reports | Technical Procedures | Policy Writing | Stakeholder Summaries

- Cloud & Tools: Microsoft Sentinel | Azure | Log Analytics Workspace | OpenVAS | Nmap | Metasploit | Cellebrite | Wireshark

- Languages & OS: Python | Java | Bash (basic) | Linux (Kali, Ubuntu) | Windows | VMware

- Behavioural Skills: Attention to Detail | Clear Communicator (technical and non-technical) | Organised | Team player with a customer-focused mindset | Comfortable in fast-paced, dynamic environments

Additional Information

- Working towards Certification in CompTIA Security+

- Experience working in both solo and collaborative academic environments simulating real enterprise SOC operations

- Interested in developing further expertise in cloud security, SIEM integration, and risk governance