

KEHINDE ODUYEYE

Security Engineer

ma19kdo@gmail.com | 07470 731407 | 194 Weekes Drive, Slough SL1 2YR

Portfolio: www.kehinde-oduyeye.dev | GitHub: github.com/Dorkiee

PROFESSIONAL SUMMARY

Security Engineer with 4+ years in Security Operations, specialising in SOC automation, detection engineering, and incident response across multi-cloud environments. Proven track record of eliminating manual SOC tasks, reducing incident response times from hours to minutes, and improving detection fidelity through custom Microsoft Sentinel KQL detections and automated enrichment workflows. Experienced operating at scale with 250,000+ user environments, integrating AI-driven identity analytics, MITRE ATT&CK-aligned detection, and cloud-native automation across Azure, AWS and Defender for Cloud. Currently extending this expertise into broader automation consulting, building ServiceNow and Logic App-based automation and identity/access workflows. Recognised for technical leadership, cross-functional collaboration, and mentoring junior analysts into engineers.

PROFESSIONAL EXPERIENCE

Automation Engineer & Security Consultant – Crowd-Now

Sep 2026 – Present

- Design and build security and business-process automation, primarily connecting Azure Logic Apps with ServiceNow.
- Developing ServiceNow citizen-developer solutions, building workflows and apps directly on the ServiceNow platform.
- Contributing to Microsoft AI Foundry initiatives as part of the wider automation programme.
- configuring Azure AD app registration required to provision access to ServiceNow/SharePoint sites, working against an existing ServiceNow catalog item to deliver an end-to-end request-to-access workflow.

Security Operations Engineer – Indivior

Aug 2021 – Dec 2025

- Built Python (Jupyter) and PowerShell tooling for automated device timeline analysis, multi-device isolation, and VirusTotal/API-driven URL and IOC enrichment, following version control and peer-review best practice.
- Designed and maintained automation playbooks in Azure Logic Apps and ServiceNow TISC for incident response, threat hunting, CTI processing, and vulnerability management.
- Built and tuned Microsoft Sentinel KQL detections in collaboration with Threat Intelligence, IR, and Attack Surface Management teams, aligning rules to MITRE ATT&CK to improve SOC visibility and enable proactive hunting.
- Performed advanced threat hunting and investigations using Sentinel, Defender XDR, DarkTrace, PhishER and Python notebooks, including Microsoft 365 investigations (impossible travel, phishing inbox rules, audit log reviews), malware analysis, and digital forensics/reverse engineering.
- Managed 15–20 SOC incidents per week end-to-end (triage, categorisation, escalation, closure) via ServiceNow SIR/CSIR, maintaining SLA compliance; authored and maintained 50+ Knowledge Base Articles aligned to IRR and REACTS frameworks.
- Applied security monitoring and automation across Azure, AWS and Defender for Cloud, and administered Active Directory (password resets, group assignments, account management) in support of Zero Trust principles.

EDUCATION

BSc (Hons) Computer Science — Brunel University London

Jun 2023

Key modules: Final Year Project, Software Project Management, Cybersecurity, Network Computing & Advanced Topics, Algorithms & their Applications, Networks & Operating Systems, Usability Engineering, Software Development & Management.

TECHNICAL ABILITIES

Java, Python, PowerShell, C#, HTML, Active Directory, Microsoft Office, TCP/IP, ITIL Service Management, APIs, Automation, Azure Logic Apps, ServiceNow (incl. citizen development), Microsoft Graph, Microsoft AI Foundry, SharePoint, AWS, Microsoft Azure, Jupyter, Information Security, Risk Management, Incident Management & Response, Vulnerability Management, Threat Intelligence, NIST 800, ISO/IEC 27001, Security Analysis, Cloud Security, Microsoft Sentinel, Defender XDR, DLP, Linux, Windows.

PROJECT WORK

NRT RMM Tool Detection & Response (Microsoft Sentinel Analytics + Logic Apps)

- Developed a near real-time Sentinel KQL analytic rule to detect unauthorized RMM tool execution from endpoint telemetry and behavioural patterns.
- Triggered an automated Logic App to retrieve affected hosts, validate against an Azure Table exclusion list, and enrich incident context, with Defender for Endpoint performing automated full device isolation.
- Reduced attacker dwell time by enabling rapid, consistent containment within minutes, eliminating manual validation.

Microsoft Sentinel Home Lab (Azure + Microsoft Sentinel + Azure Monitor Agent)

- Built a Sentinel home lab covering SIEM deployment, data source onboarding, and detection engineering, provisioning Resource Groups, Log Analytics Workspace, and Sentinel.
- Onboarded Azure AD, Identity Protection, Azure Activity, and Windows VMs via Azure Monitor Agent, Data Collection Rules, and Azure Policy; built analytic rules with entity mapping and MITRE ATT&CK alignment.

Automating Device Timeline Analysis (Python + Jupyter Notebooks)

- Automated device timeline and phishing analysis, extracting IPs, URLs, headers and attachments, and enriching via VirusTotal and internal sources with caching to reduce redundant API calls.
- Applied ML-based risk scoring for verdicts and analyst-ready reports, feeding downstream ServiceNow incident creation.

Phishing Response & Sentinel Incident Enrichment Automation (Logic Apps + APIs + Python)

- Built Logic App workflows to automate phishing email analysis and response, and to enrich Sentinel incidents (IPs, URLs, hashes, IOCs) using external threat intelligence APIs and Python/Jupyter integrations.
- Implemented automated risk scoring and ServiceNow incident creation, reducing manual analysis time and improving triage efficiency and response consistency.