Darren Obi

Cybersecurity Analyst

London, United Kingdom | darren.obi@gmail.com | +44 7482 331 920 | linkedin.com/in/darrenobi

Cybersecurity analyst with four years of experience working in SOC environments and incident response across financial services. Currently on the security operations team at a retail bank monitoring threats across 8,400 endpoints and 320 servers. I like finding the thing that doesn't look right and figuring out why.

EXPERIENCE

Cybersecurity Analyst, Nationwide Building Society, Swindon *Oct 2022 – Present*
Part of the security operations centre protecting 16 million members' data and banking infrastructure.

- Monitor and triage **1,200+ daily security alerts** across SIEM (Splunk), EDR (CrowdStrike), and email gateway — maintain a false positive rate below 8%
- Led incident response for a **phishing campaign** targeting 4,300 employees — contained within 2 hours, zero data exfiltration
- Built **34 custom Splunk detection rules** for lateral movement and credential stuffing patterns, catching 12 incidents the default rules missed
- Conducted **6 tabletop exercises** with senior leadership, testing ransomware, insider threat, and supply chain scenarios

Junior Security Analyst, NCC Group, Manchester *Mar 2021 – Sep 2022*
Worked in NCC Group's managed security services division, monitoring client environments.

- Monitored security for **18 client organisations** across finance, retail, and healthcare sectors
- Wrote **42 incident reports** and post-incident reviews, escalating 8 critical incidents to client CISOs
- Assisted with **3 penetration testing engagements** — found a misconfigured S3 bucket exposing 140,000 customer records for a retail client

IT Security Intern, BAE Systems Digital Intelligence, Guildford *Jun 2020 – Dec 2020*
Six-month placement with the threat intelligence team.

- Analysed malware samples and contributed to **4 threat intelligence reports** distributed to government and defence clients
- Built a Python tool to parse and correlate **STIX/TAXII threat feeds** from 6 sources into a unified dashboard

EDUCATION

BSc (Hons) in Information Security, Royal Holloway, University of London, Egham *Sep 2017 – Jun 2021*
First Class Honours. The programme is certified by GCHQ as meeting the requirements for a Certified Master's degree in Cybersecurity. Dissertation on *detection of credential stuffing attacks using behavioural analysis*.

SKILLS

SIEM (Splunk, Microsoft Sentinel) • EDR (CrowdStrike Falcon) • Incident Response & Triage • Threat Intelligence (MITRE ATT&CK) • Python scripting (automation & analysis) • Network Analysis (Wireshark, tcpdump) • Vulnerability Scanning (Nessus, Qualys) • Firewall & IDS/IPS management • Linux & Windows Server administration • NIST & ISO 27001 frameworks

CERTIFICATIONS

CompTIA Security+, CompTIA *Jun 2021 – Jun 2024*

Certified SOC Analyst (CSA), EC-Council *Nov 2022*

Splunk Core Certified Power User, Splunk *May 2023 – May 2026*

LANGUAGES

English (native)

PROJECTS

Custom Detection Rules – Nationwide *Feb 2023 – Nov 2023*
Developed a library of custom Splunk detection rules tailored to the bank's environment.

- Wrote **34 custom rules** covering credential stuffing, lateral movement, and unusual admin activity
- Caught **12 genuine incidents** that the vendor's out-of-the-box rules missed entirely
- Reduced average detection time for lateral movement from **4 hours to 22 minutes**

Phishing Simulation Programme – Nationwide *Jun 2023 – Mar 2024*
Designed and ran a quarterly phishing simulation programme for all 18,000 employees.

- Created **12 phishing scenarios** of increasing sophistication
- Click rate dropped from **14% to 4.8%** over four quarters
- Reporting rate (employees flagging suspicious emails) increased from **22% to 61%**

REFERENCES

Karen Whitfield, Head of Security Operations, Nationwide Building Society, karen.whitfield@nationwide.co.uk, +44 7700 900 821

Marcus Adebayo, Security Consulting Manager, NCC Group, marcus.adebayo@nccgroup.com, +44 7700 900 934

EXTRA CURRICULAR ACTIVITY

Volunteer – CyberFirst Schools Programme (NCSC) *Sep 2023*

Volunteer with the National Cyber Security Centre's schools outreach programme. Deliver workshops on online safety and careers in cybersecurity to GCSE students. Visited 6 schools in the London area so far.

CTF Competitor – Team 'NullByte' *Jan 2021*

Compete in Capture The Flag competitions as part of a 4-person team. Placed 23rd out of 412 teams in the 2024 SANS Holiday Hack Challenge. Focus areas are web exploitation and forensics.