Mortadah Jaballah
UK
Email: cyber@mjaballah.co.uk | Phone: 07438 966189
Website: https://www.mjaballah.co.uk/
LinkedIn: https://www.linkedin.com/in/mortadah-jaballah-7b9a38305/
GitHub: https://github.com/Mortadah-ux

Professional Summary

Motivated and detail-oriented cybersecurity learner with a strong foundation in security principles, networking, and cloud technologies. Certified in CompTIA Security+, Network+, Microsoft Azure Fundamentals (AZ-900), Google Cybersecurity, and Splunk Core Certified Power User. Currently studying a Level 4 Extended Diploma in Computing (Cyber Security Technologist). Actively building hands-on skills through home labs, GitHub projects, and TryHackMe practice. Seeking an entry-level SOC Analyst L1 role in a 24/7 environment.

Education

Level 4 Extended Diploma in Computing (Cyber Security Technologist) — In progress

Certifications

CompTIA Security+
CompTIA Network+
Microsoft Certified: Azure Fundamentals (AZ-900)
Google Cybersecurity Professional Certificate
Splunk Core Certified Power User
Planned: Microsoft Certified: Security Operations Analyst (SC-200)

Cybersecurity Projects

Splunk SOC Home Lab (2024)
• Installed and configured Splunk Free Edition to ingest and analyse Windows event logs.
• Used SPL to investigate security events and build dashboards and alerts.
• Simulated real SOC monitoring and detection workflows.

Windows Event Log Analysis (Sysmon Practice) (2024)
• Deployed Microsoft Sysmon for enhanced endpoint logging.
• Analysed process creation, network connections, and file modifications.
• Practised identifying suspicious behaviour and writing incident summaries.

Azure Cloud Security Fundamentals (2024)
• Completed hands-on labs focused on identity and access management.
• Gained practical experience with RBAC and Azure monitoring features.

Technical Skills

Security & SOC: SIEM Monitoring, Log Analysis, Incident Triage (entry level)
Tools: Splunk, Sysmon, Wireshark, Nmap, Microsoft Defender, Azure Portal
Programming: Python (basic scripting)
Networking: TCP/IP, DNS, Firewalls, VPN fundamentals
Operating Systems: Windows, basic Linux familiarity

Career Objective

To secure an entry-level L1 SOC Analyst role where I can apply my technical knowledge, develop real-world monitoring and incident response skills, and grow within a 24/7 SOC environment.