Mohammed A

UK-Manchester | contact@sanclogic.com | sanclogic.com

SUMMARY OF QUALIFICATIONS

- SOC analyst with hands-on incident response experience including investigation and remediation of botnet infections in production environments
- Develop CTF scenarios and detection content for cyber range training platforms
- Use KQL and SPL for threat hunting, detection engineering, and alert creation
- Create Sigma rules and custom detections mapped to MITRE ATT&CK framework
- Present investigation walkthroughs using MDE and Splunk during community training sessions
- Proficient in Windows and Linux systems with basic scripting in PowerShell, Python, and Bash

TECHNICAL SKILLS

SIEM & Detection: Microsoft Sentinel, Splunk Enterprise, KQL, SPL, Sigma Rules, Alert Engineering

Endpoint & Analysis: Microsoft Defender for Endpoint, Sysmon, Windows Event Logs, Wireshark, Zeek, Static/Dynamic Malware Analysis

Frameworks & Scripting: MITRE ATT&CK, Cyber Kill Chain, PowerShell, Python, Bash

EDUCATION & CERTIFICATIONS

BSc Computing (First Class Honours) Feb 2024 – Apr 2025
Arden University, United Kingdom

Microsoft Azure Fundamentals (AZ-900) Sept 2024
Microsoft

RELATED WORK EXPERIENCE

SOC Analyst Intern (Tier 2) | Adversary Simulation | Jan 2026 – Present
MYDFIR

- Investigate and escalate complex alerts across Microsoft Sentinel, Splunk, Defender XDR, and Sysmon telemetry to identify attack progression and determine scope of compromise
- Conduct proactive threat hunts using KQL and SPL to identify malicious activity outside of alert-based detection, focusing on persistence mechanisms and lateral movement indicators
- Tune detection rules and use cases to reduce false positive rates while maintaining coverage for high-fidelity attack techniques
- *Validate findings from junior analysts and provide guidance on investigation methodology and evidence correlation*
- *Build threat profiles documenting attacker TTPs with MITRE ATT&CK mappings to support knowledge sharing and detection development*

SOC Intern / CTF Engineer (Contract) Mar 2025 – Present
LogNPacific Cyber Range

- Led incident response for two botnet infections affecting 7 VMs; traced Microsoft abuse notifications to compromised systems performing outbound brute force attacks against external services
- Root caused infections to Linux systems with weak credentials discovered by botnet scanners, resulting in C2 callbacks and cryptominer deployment
- Built Sentinel alerts to monitor for C2 callbacks and suspicious outbound traffic; conduct ongoing threat hunting to ensure environment integrity
- Create CTF scenarios for beginner students covering attack simulation and telemetry generation
- Support peers during CTF exercises and assist with investigation methodology

SPECIALIZED TRAINING

- **MYDFIR SOC Analyst Course** (90-day hands-on program): Splunk SIEM, investigation methodology (network, malware, AD, identity, email, OSINT), threat hunting with Sigma/YARA rules, incident response
- **TCM Security SOC Level 1**: Phishing analysis, Wireshark network analysis, endpoint security
- **SOC Core Skills (Antisyphon**): Windows/Linux forensics, memory forensics, Active Directory analysis