Mohammed Abdullatif

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

Community Moderator | Adversary Simulation Oct 2025 – Present
MYDFIR Community

- Triage and investigate simulated intrusions by performing tactical review of EDR telemetry (MDE), Windows Event Logs, and Sysmon data to determine root cause of attacks including persistence mechanisms, lateral movement, and data exfiltration attempts
- Perform malware analysis and develop Sigma detection rules mapped to MITRE ATT&CK for attack techniques including PowerShell abuse, scheduled task persistence, credential dumping, and C2 communications
- Contribute to detection engineering efforts by creating and tuning custom alerts in Splunk and Sentinel based on real-world attack simulations and investigation findings
- Led collaborative investigation sessions with peer analysts, explaining complex attack chains and remediation strategies to support team skill development and knowledge sharing

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