MUHAMMAD WALEED

SOC Analyst | Blue Team | Cybersecurity

Dubai, United Arab Emirates • (+971) 50 690 8284 • muhammadwaleed2280@gmail.com

walsec.com • LinkedIn • GitHub

First Class Honours Cybersecurity graduate (De Montfort University) specialising in threat intelligence, network forensics, and SOC automation. Hands-on with Splunk, Wazuh, and MITRE ATT&CK for detection and incident response, and able to ship the tooling behind the defence — from a fully local LLM-powered SIEM-Lite to ML detection pipelines. Comfortable translating technical findings into decisions a SOC can act on.

Technical Skills

Security Operations:	Splunk, Wazuh, SIEM rule tuning, EDR, MITRE ATT&CK, packet & log analysis, incident response
Tools:	Nessus, Burp Suite, Wireshark, VirusTotal, threat-intelligence feeds
Networking & Systems:	VLAN/NAT, routing, firewall rules, Linux (Ubuntu, Mint, REMnux, Kali), Windows
Programming & Automation:	Python, C++, SQL, data visualisation & dashboards
AI & Automation:	Claude (Anthropic AI Fluency, Claude 101), generative AI engineering (IBM), Python automation

Experience

Receptive Tech Communications **Jun 2025 – Sep 2025**

Cyber Security Intern *Lahore, Pakistan*

- Tuned SIEM correlation rules and alert thresholds, raising threat-detection accuracy by 20%.
- Cut endpoint vulnerabilities 25% through recurring scans and patch verification, confirming fixes actually landed.
- Rewrote escalation matrices, bringing incident response times down 15–20%.

Telstra, Mastercard & Deloitte — Virtual Job Simulations **2025**

Cybersecurity Analyst roles (Remote)

- **Telstra:** contained a simulated malware attack, cutting projected impact by 80%, and authored the post-incident analysis (3 vulnerabilities, 5 hardening actions).
- **Mastercard:** triaged and reported phishing on the Security Awareness Team; delivered targeted training to high-risk business units.
- **Deloitte:** analysed web-activity logs for incident indicators and investigated suspicious user activity during a simulated breach.

Key Projects

WalSec A-TIOC Hub — Air-Gapped SIEM-Lite & Threat-Intel Platform **Final-Year Project**

- Built an end-to-end, fully local SOC platform: automated deep packet inspection feeding a threat-intel-grounded local LLM (RAG), giving SMEs enterprise-grade threat hunting with no cloud, cost, or GDPR exposure.
- Achieved 100% hallucination prevention via retrieval grounding, 1.8–2.4s AI time-to-first-token, and 3,200+ concurrent threat writes; mapped detections to 30+ MITRE ATT&CK techniques.
- Faculty-commended and formally recommended for publication.

Network Forensics & ICS Security **2025**

- Reconstructed a multi-stage SCADA/ICS attack purely from packet captures, tracing the full intrusion chain across OT network segments using Wireshark, TShark, and PyShark.
- Produced an incident-response writeup mapping attacker behaviour to MITRE ATT&CK for ICS with concrete detection and segmentation recommendations.

AI-Driven Phishing Detection **2025**

- Engineered and adversarially tested an ML detection pipeline over 235k+ URLs (XGBoost, Random Forest, MLP) for SOC alert automation, hardening it against evasion.

Incident Response Maturity & Threat Intelligence **2025–26**

- Ran a SIM3/ENISA IR-maturity assessment for a logistics SME and structured threat intelligence into STIX for repeatable, machine-readable sharing.

Penetration Testing & Malware Investigations **2025–26**

- Conducted a black-box penetration test and multi-sample malware reverse-engineering (static + dynamic) using Nessus, Metasploit, Burp Suite, IDA, GDB, and REMnux.

Education

De Montfort University **Jul 2026**

BSc (Hons) Cyber Security — First Class Honours *Dubai, UAE*

Certifications

- ISC2 Certified in Cybersecurity (CC)
- Google Cybersecurity Professional Certificate
- AI Fluency & Claude 101 – Anthropic
- Generative AI Engineering Professional – IBM
- Oracle Certified Foundations Associate (AI & Cloud)
- Microsoft SC-900: Azure Security *(in progress)*