Muhammad Talha

SOC Analyst (Entry-Level) | Purple Team Practitioner | Security Educator (Cyberster)

Email: infosectalha@gmail.com | LinkedIn: linkedin.com/in/infosectalha | GitHub: github.com/infosectalha | Portfolio: infosectalha.github.io

PROFESSIONAL SUMMARY

SOC-oriented cybersecurity practitioner with hands-on experience deploying and operating Wazuh SIEM, performing log-based alert triage, and validating detections through controlled attack simulations in virtual lab environments. Strong working knowledge of MITRE ATT&CK mapping, OWASP web testing in lab contexts, and evidence-led reporting. Cofounder & COO at Cyberster, delivering paid, instructor-led training that builds foundations (OS, hardware, security concepts) and progresses to practical SOC workflows.

CORE SKILLS

Defensive / SOC: Wazuh SIEM, Log Analysis, Alert Triage, File Integrity Monitoring (FIM), Incident Reporting, Threat Intel Enrichment (VirusTotal), IDS/IPS Concepts.
Offensive (Purple Depth, Lab): Nmap, Burp Suite, Nessus Essentials, OWASP Top 10 testing, Metasploit (lab simulation), Web vulnerability validation.
Systems & Tooling: Kali Linux, Docker, Git/GitHub, OpenSSL, Basic Python scripting, Technical documentation.

EXPERIENCE

Cofounder & COO | Lead Instructor — Cyberster (Training Venture)

Pakistan | Paid instructor-led batches | 2025–Present

- Lead curriculum design and delivery for cybersecurity foundations (Operating Systems, hardware fundamentals, security principles, and problem-solving) and intermediate SOC workflows (SIEM usage, alert triage, investigation mindset).
- Coordinate instructors and batch operations, ensuring consistent delivery, lab readiness, and student progression.

SOC Analyst Intern — Cyborts (Remote)

1 month

- Deployed and configured Wazuh manager and agents across Windows and Ubuntu endpoints.
- Implemented File Integrity Monitoring (FIM) and validated detections with controlled brute-force and payload simulation in a safe lab.
- Performed alert correlation and enrichment using VirusTotal reputation checks; produced weekly evidence-led reports.

Associate Project Manager Intern — Excelerate (Remote)

1 month

- Coordinated remote team deliverables, task delegation, and progress tracking to meet project goals.

SELECTED PROJECTS (EVIDENCE-LED)

- Simulation & Analysis of Cyber Attacks using MITRE ATT&CK: mapped TTPs across three organizational scenarios and proposed detection & mitigation strategies. (PDF available)
- OWASP Juice Shop VAPT (Lab): validated authentication weaknesses and injection risks; documented findings and recommendations. (PDF available)
- DVWA & bWAPP VAPT (Lab): recon + manual verification of common web vulnerabilities with remediation guidance. (PDFs available)
- Metasploitable Network VAPT (Lab): Nessus Essentials scan summarizing severity distribution and key critical findings. (PDF available)
- Crypto & Secret Retrieval via Docker: Base64/XOR/RSA/AES workflows demonstrating secure secret handling practices. (PDF available)

EDUCATION

Bachelor of Business Administration (BBA) — NUML University, Faisalabad (In progress)

- Elected Class Representative (CR); developing leadership, communication, and coordination skills