Ehsan Ali
Email: ehsan.ali786@outlook.com
LinkedIn: https://www.linkedin.com/in/ehsan-ali-469ab5152/

PROFESSIONAL SUMMARY

Security+ certified, with hands-on experience in SOC labs, CTF platforms, and home network defence simulations. Supported real-world IT setups during office infrastructure projects, including PC imaging and basic network troubleshooting. Now seeking a role in IT support or cybersecurity operations, with a focus on developing technical depth in tools like Active Directory, SIEMs, and EDR. Long-term goal: to grow into incident response, threat detection or Pen testing roles.

CERTIFICATIONS

- CompTIA Security+ – Passed score of 788 in July 2025
- TryHackMe Penetration Testing Jr path - 100% completion - Feb 2026
- Google Cybersecurity Certificate – Completed in March 2025
- Qualys Vulnerability Management Foundation – Completed in March 2025

EMPLOYMENT EXPERIENCE

Current employment | **Creative Networks – *Service Desk / Field IT Engineer***

- Deliver 1st & 2nd line support for SME clients, resolving incidents across Windows OS including Office 365 (admin center, lighthouse), accessing Azure AD for user management.
- Performed networking resolutions on-site hands-on including understanding network layouts with routers, switches, patch panels, server setups etc.
- Used remote tools to diagnose issues to investigate user issues via many fundamentals methods including replicating faults and using documentation to resolve specific issues and creating technical documentation for future us.
- Provided on-boarding services including provisioning of laptops & desktops which included backup measures of old devices, domain join or entra join end-user devices and understood their security baseline established and installed AV (ESET), correct access levels via computer management.
- Followed ITIL practices for logging, prioritising and completing tickets to ensure structured problem-solving and incident tracking.
- Gained exposure to AV rollouts, MFA enforcement via Microsoft Intune, security posture checks across various client environments
- Supported SME active infrastructures including tracing/crimping data cables, configuring switch ports, resolving TCP/IP connectivity issues.
- Documented work done and clearly stated via video/images the network layouts of client infrastructure.
- Provided practical steps for clients for password policy, End-user device security including FDE, MFA.

May 2025 to Jul 2025 | **Distology – *Solutions Sales Specialist***

Although this was primarily a commercial role, I focused heavily on the technical aspects of cybersecurity solutions and vendor technologies to accelerate my learning curve within the UK cyber ecosystem.

- Completed 5 vendor technical certifications within the first 3 weeks via OPSWAT Academy around IT/OT environments.
- Studied and supported real-world use cases in FS&I, public sector, and manufacturing, gaining exposure to key cybersecurity compliance requirements (e.g. NIST, ISO 27001).

- Created a technical SWOT analysis and opportunity mapping deck aligned with cybersecurity channel go-to-market strategy.
- Participated in over 20+ technical discovery calls and training sessions, learning how channel partners deploy perimeter-level defenses, file sanitisation, and threat detection layers using solutions like MetaDefender and MetaAccess.

August 2023 to May 2025 | ***Watt Utilities – Customer account manager***

- Managed customer accounts through proactive cold calling, achieving daily sales targets.
- IT Initiative: Assisted in setting up IT systems for 50–100 employees during an office relocation, configuring PCs, monitors, Ethernet cables, and peripherals.
- Effectively marketed and sold services across diverse gas, electric, and water suppliers to achieve sales goals.
- Cultivated strong communication and teamwork with various departments and suppliers, providing thorough support and assistance to clients during contract implementation.

CURRENT TRAINING & LABS

- HacktheBox Penetration Testing path (CTPS) – 15% completed.
- TryHackMe SOC Level 1 - 50% completed.
- Built lightweight SOC environment on a home lab setup incorporating log aggregation, SIEM, Active Directory and several VMs enabling network/endpoint security traffic auditing across isolated NAT network

SKILLS

- Cybersecurity & Blue Team Tools: Wireshark, Tcpdump, SIEM (Wazuh)
- Platforms: Windows 10/11, Kali Linux (VM), Python, SQL, PowerShell
- Networking: VLAN config, Packet Analysis, DNS config, VPNs
- IT Support Skills: Hardware setup, Troubleshooting, Office 365, User Training
- Lab Simulations: SOC alert triage, incident playbooks, phishing detection
- Active Directory (lab-based): Created test domain, managed users/groups, applied password policy

PERSONAL PROJECTS

- Built Home Servers for various purposes including WireGuard VPN, AdGuard, Plex Media Server.
- Hardware & Troubleshooting: Proficient in PC assembly, maintenance, and troubleshooting.
- Ethereum Crypto Mining & System Maintenance: Self-built & managed a multi-GPU crypto mining rig, ensuring performance and temperature control
- Built 5–10 gaming and workstation PCs from scratch, selecting components and troubleshooting issues.

EDUCATION

- University of Salford - 2:2 in Physics (BSc) 2014-2017
- NCN High Pavement College - A Levels; Maths (C), Physics (C) and Chemistry
  (C) - AS Levels; Further Maths (C) – 2012-2014
- Ellis Guildford Sports College - 6 GCSE's A*-C with Maths (B), English (B) and Science (B) - 2009 – 2011