Ahmed Al-Senaidi

+968 9334 8051 | ahmedalsenaidi@outlook.com | linkedin.com/in/ahmedalsenaidi

SUMMARY

Cybersecurity professional with hands-on experience in network security, threat detection, and secure infrastructure design. Proven ability to build complex lab environments (SOC, OT/ICS) to simulate and defend against cyber threats. Familiar with and applying principles of MITRE ATT&CK and Zero Trust frameworks for defense validation.

SKILLS

Cybersecurity: Network Security, Threat Detection & Hunting, SOC Operations, OT/ICS Security, Vulnerability Management, Zero Trust, MITRE ATT&CK
Tools: Wazuh, Suricata, pfSense, Nessus, Wireshark, Kali, Metasploit, VMware, Hyper-V, Docker, Portainer
OS/Scripting: Linux, Windows Server/AD, Python, Bash

PROJECTS

Secure ICS Testbed — Zero Trust & Encrypted Modbus/TCP

- Engineered Purdue-segmented ICS lab (3 zones, 12 VMs) with 15 default-deny firewall rules and MFA-gated jump-server access, mitigating Initial Access & Lateral Movement (e.g., T1133, T1021).
- Implemented Modbus/TCP encryption via stunnel, countering Defense Evasion (e.g., T1027) and securing OT communications.
- Achieved 100% detection/containment of 8 simulated attacks via SIEM/IDS, preventing Impact and demonstrating practical application against various Execution & Command and Control techniques.

Cybersecurity Virtual Lab — Enterprise Segmentation & SIEM

- Deployed multi-VLAN environment with strict inter-VLAN rules, enhancing network segmentation and control over Lateral Movement.
- Centralized log collection and integrated Nessus reports for correlation, improving Detection and vulnerability management.

EXPERIENCE

Cybersecurity Intern | Oman Electricity Transmission Company (OETC) 06/2024 - 08/2024

- Observed daily SOC monitoring; practiced alert triage and documentation in lab settings.
- Reviewed Nessus scan reports and drafted remediation notes by severity and asset criticality.
- Explored OT/ICS security principles (Purdue layers, segmentation, jump-server access patterns).
- Compared defensive controls (XDR/EDR, IDS/IPS, SOAR, WAF/proxy, DNS filtering) and summarized use cases.

EDUCATION

B.Sc. Computer Science (Cyber Security & Computer Infrastructure) — Sultan Qaboos University — **Degree Conferral: Sep 2025**

Certifications & Training

- CompTIA Security+ (In progress)
- Linux Professional Institute (LPI) (In progress)
- TryHackMe: Intro to Cybersecurity, Pre-Security, Complete Beginner, Security Engineer (In progress)
- CTFs completed: RootMe, Pickle Rick, Agent Sudo, Ignite, Bounty Hacker, Fowsniff