Ahmed Al-Senaidi

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

SUMMARY

Cybersecurity professional with a strong foundation in network security, threat detection, and secure infrastructure design. Proven ability to translate security theory into practice by building complex lab environments to simulate both enterprise (SOC) and industrial (OT/ICS) security challenges. Passionate about problem-solving and skilled in using frameworks like MITRE ATT&CK and Zero Trust to build and validate robust defenses.

SKILLS

Security Concepts: Network Security, Threat Detection & Hunting, SOC Operations, OT/ICS Security Principles, Vulnerability Management, Zero Trust, MITRE ATT&CK
Security Tools: SIEM (Wazuh), IDS/IPS (Suricata), Firewall (pfSense), Nessus, Wireshark, Kali, Metasploit
Platforms & Infrastructure: Linux, Windows Server/AD, VMware, Hyper-V, Docker, Portainer
Scripting & Automation: Python, Bash

PROJECTS

Secure ICS Testbed — Zero Trust & Encrypted Modbus/TCP
Stack: GRFICSv2 (SCADA/PLC), pfSense, Wazuh SIEM, Suricata IDS, stunnel (TLS), VirtualBox, Metasploit

- Built a Purdue-segmented ICS lab (3 zones, 3 VLANs, 12 VMs) with default-deny policies (15 firewall rules) and MFA-gated jump-server access.
- Encrypted Modbus/TCP via stunnel; verified with Wireshark; validated detections via simulated attacks.
- Executed 8 attack scenarios; 8/8 (100%) detected/contained with SIEM/IDS; 0 direct IT→OT paths permitted.

Cybersecurity Virtual Lab — Enterprise Segmentation & SIEM
Stack: Hyper-V, pfSense, VLANs, Docker/Portainer, Kali, Nessus, Windows Server/Win10

- Deployed multi-VLAN environment with strict inter-VLAN rules and DHCP scopes; stood up DVWA/bWAPP/WebGoat for testing.
- Collected/centralized logs and planned integration of Nessus reports for correlation.

EXPERIENCE

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

- Observed daily SOC monitoring; practiced basic alert triage and documentation in a lab setting
- Reviewed Nessus scan reports and drafted remediation notes by severity and asset criticality
- Explored OT/ICS security: Purdue layers, IT/DMZ/OT segmentation, jump-server access patterns
- Compared defensive controls and data sources (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 scheduled Sep 2025**

CERTIFICATIONS & PLATFORMS

CompTIA Security+ (In progress — target Sep/Oct 2025)
Linux Professional Institute (LPI) (In progress)
TryHackMe: Intro to Cybersecurity, Pre-Security, Complete Beginner
CTFs completed: RootMe, Pickle Rick, Agent Sudo, Ignite, Bounty Hacker, Fowsniff

LANGUAGES

Arabic (native) • English (Proficient)