Ahmed Al-Senaidi

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

SUMMARY

A cybersecurity professional with hands-on experience in designing and defending network infrastructure. Proven ability to build and secure complex lab environments (SOC, OT/ICS) by applying a Threat-Informed Defense methodology. Skilled in using frameworks like MITRE ATT&CK and Zero Trust to validate security controls and mitigate real-world adversary techniques.

SKILLS

Cybersecurity Concepts: Threat-Informed Defense, Network Security, Threat Detection & Hunting, SOC Operations, OT/ICS Security (Purdue Model), Vulnerability Management, Zero Trust.
Security Tools: Wazuh (SIEM), Suricata (IDS), pfSense, Nessus, Wireshark, Kali, Metasploit, VMware.
OS & Scripting: Linux, Windows Server, Python, Bash.

PROJECTS

Secure ICS Testbed — Zero Trust & Encrypted Modbus/TCP

- Designed and built a reusable ICS security testbed with a dual purpose: to gain hands-on experience and to create a low-cost, educational platform for future students to learn OT defense.
- Applied a Threat-Informed Defense strategy by modeling XENOTIME TTPs; deployed layered controls (MFA Jumpserver, pfSense) that successfully prevented lateral movement (T0886).
- Validated the architecture by proving that TLS encryption prevented Unauthorized Command Messages (T0855), while Suricata and Wazuh provided full detection visibility of the attempt.

Cybersecurity Virtual Lab — Enterprise Segmentation & SIEM

- Engineered a multi-VLAN enterprise network from scratch, using pfSense to segment and secure assets including a Domain Controller and containerized vulnerable applications (DVWA).
- Deployed a Wazuh SIEM as a central SOC monitoring tool, successfully ingesting logs from all segments to detect and correlate simulated attacks launched from Kali Linux.

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 Universit, 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