Ahmed Al-Senaidi

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

INTRO

Computer Science graduate (degree awarded September 2025) specializing in Cybersecurity & Infrastructure. I have built and secured multiple hands-on lab environments—an enterprise VLAN network with pfSense, a Zero-Trust ICS testbed with Modbus/TCP encryption, and an IoT monitoring stack—using tools such as Wazuh, Suricata, Docker, and Windows AD. These experiences honed my skills in SIEM rule tuning, vulnerability assessment, incident response, network segmentation, threat emulation, log analysis, and incident documentation aligned with MITRE ATT&CK frameworks. Proficient across Linux and Windows systems, with basic Python automation, and preparing for CompTIA Security+ certification (target September 2025). Eager to contribute practical, lab-proven expertise in an entry-level SOC, blue-team, or OT-security role.

CERTIFICATIONS

CompTIA Security+ (Target: October 2025)
Let's Defend – Practical SOC Analyst Path (In Progress)
TryHackMe – Intro to Cybersecurity, Pre-Security
CTF Challenges Completed: RootMe, Pickle Rick, Agent Sudo, Ignite, Bounty Hacker, Fowsniff

Core Technical Skills

Security Operations & Detection

• SIEM (Wazuh) • Incident Response • Vulnerability Assessment • Threat Hunting • Threat Analysis • MITRE ATT&CK

Network Defense & Segmentation

• pfSense Firewall • VLAN Architecture • Suricata IDS • Zero Trust (NIST 800-207) • Log Analysis • Risk Management

ICS / OT Security

• Purdue Model • SCADA Simulation • Modbus/TCP Encryption (Stunnel TLS) • Jump Server Access Control

Virtualization & Infrastructure

• Docker • Docker Compose • Hyper-V • VMware • Ubuntu Server • Windows AD & Group Policy

Scripting & Tools

• Python (log parsing, automation) • Nmap • Burp Suite • Wireshark • Grafana • MQTT • Git

Cloud & DevSecOps (Entry Level)

• AWS IAM, VPC – conceptual • Least Privilege & Cloud Segmentation

Projects

Zero Trust ICS Security Testbed (Graduation Project)

Simulated a segmented ICS environment using the Purdue Model with encryption, monitoring, and real attack validation.

- Built a 3-zone ICS lab (IT/DMZ/OT) simulating industrial network environments
- Applied segmentation, firewall policies, and TLS wrapping for Modbus/TCP using stunnel
- Deployed Suricata IDS and Wazuh SIEM for real-time alerting and analysis
- Simulated attacks: replay, port scan, lateral movement, injection, and credential brute-force

Enterprise Cybersecurity Lab

Designed a realistic enterprise lab with attack/defense simulations using open-source tools.

- Designed multi-VLAN enterprise lab with pfSense, Docker, Active Directory, and Wazuh
- Deployed vulnerable apps (DVWA, WebGoat, bWAPP) to test detection logic
- Applied firewall zoning and monitored SIEM logs for SSH brute-force and web attack patterns

IoT / WSN Monitoring Lab

Simulated sensor data for environmental monitoring with real-time visualization and alerts.

- Built simulated sensor network using Mosquitto MQTT → Python → InfluxDB → Grafana
- Monitored temperature, humidity, air quality with real-time dashboards and alert rules

Secure WLAN with VLAN & RADIUS

Designed a secure wireless network with role-based access control.

- Designed corporate WLAN across 3 VLANs (IT, HR, Guest) with WPA2-Enterprise (RADIUS)
- Implemented access policies, firewall restrictions, and guest isolation

EXPERIENCE

Cybersecurity Intern **06/2024 - 08/2024**

Company: Oman Electricity Transmission Company (OETC)

- Monitored and triaged 100+ daily security events, reducing false positives by approximately 20% through alert tuning
- Communicated incident findings to IT teams and documented SOC response procedures to improve inter-departmental clarity
- Applied basic incident response processes—identification, documentation, escalation—in a simulated SOC workflow
- Gained exposure to NGFW, IDS/IPS tools, and SOC team operations

EDUCATION

Sultan Qaboos University **September 2025**

Bachelor of Science (B.Sc.) in Computer Science (Cyber Security & Computer Infrastructure)

Final exam completed on 14 August 2025; official degree conferral in September 2025