Ahmed Al-Senaidi

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

INTRO

Computer Science graduate specializing in Cybersecurity and Computer Infrastructure, with hands-on experience in SOC operations, OT/ICS security, and network defense. Skilled in SIEM platforms, network segmentation, and Zero Trust implementation, with a focus on securing critical infrastructures through practical labs, projects, and CTF challenges.

KEY SKILLS

Security Operations: SIEM (Wazuh, LogRhythm), Incident Response, Threat Hunting
Network Defense: pfSense Firewall, VLAN Design, Network Segmentation
ICS/OT Security: SCADA Simulation, Modbus Encryption, Purdue Model
Cloud & Virtualization: AWS IAM, Security Groups, VPC Networking, Hyper-V, Docker
Zero Trust & Web Security: NIST SP 800-207, OWASP Top 10 Awareness
Systems Administration: Windows Active Directory, Group Policy Hardening, Ubuntu, Kali Linux

EXPERIENCE

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

- Monitored and analyzed over 300 security events using SIEM platforms.
- Investigated alerts, classified incidents, and documented response procedures.
- Conducted malware triage and basic threat hunting, leveraging threat intelligence to proactively detect emerging threats.

Projects

Enterprise Cybersecurity Lab

- Designed and deployed a multi-VLAN enterprise lab integrating pfSense firewall, Wazuh SIEM, Suricata IDS, Docker-based applications, Active Directory, and Linux environments to simulate real-world cyberattack and defense scenarios.
- Simulated real-world security scenarios such as VLAN hopping attacks, SIEM alert correlation, and basic penetration testing, enhancing hands-on skills in network defense and incident response.

The lab environment enhanced practical incident response skills and demonstrated real-world attack and defense techniques.

ICS Security Testbed (Graduation Project)

- Built a comprehensive ICS security testbed simulating IT, DMZ, and OT networks using GRFICSv2 to study attack surfaces and validate Zero Trust segmentation strategies in OT environments.
- Applied Zero Trust principles by configuring an MFA-protected jump server, deploying Suricata IDS and Wazuh SIEM, and securing Modbus communications, reducing risk of lateral movement within ICS networks.

The ICS testbed validated the effectiveness of Zero Trust segmentation in reducing lateral movement risks within critical OT networks.

EDUCATION

Sultan Qaboos University **August 2025**
Bachelor of Science (B.Sc.) in Computer Science (Cyber Security & Computer Infrastructure)

Certifications / Training Courses:

- **TryHackMe Learning Paths:** Introduction to Cyber Security, Pre-Security, Complete Beginner
- **Let's Defend:** Practical SOC Analyst Training (Ongoing)
- **Capture the Flag (CTF) Challenges Completed:** RootMe, Bounty Hacker, Anthem, Pickle Rick, Fowsniff, Agent Sudo, Anonforce, Basic Pentesting, Ignite
- Currently preparing for CompTIA Security+ Certification, Linux Professional Institute (LPI).