

YAZAN AL SHAMAKHI

Cyber and Information Security Analyst

✉ y7n@outlook.it ☎ +968 79997834 📍 Muscat, Oman 🔗 site.yzn.lol

PROFESSIONAL SUMMARY

Motivated Cybersecurity Analyst with a Bachelor of Technology (B.Tech) in Information Technology – Cyber and Information Security at UTAS. Experienced in network administration, cybersecurity operations, Linux and Windows Server management, vulnerability assessment, SIEM deployment, and blockchain development. Skilled in implementing defensive security controls, troubleshooting enterprise networks, and developing automation solutions using Python, Bash, and Solidity.

EDUCATION

Bachelor of Technology (B.Tech) in Information Technology – Cyber and Information Security

2020 – 2026

University of Technology and Applied Sciences (UTAS)

GPA: 3.09

PROFESSIONAL EXPERIENCE

Cybersecurity & IT Trainee

05/2025 – 07/2026

Oman Broadband | Muscat, Oman

Muscat

- Configured and maintained Windows workstations, providing hardware, software, and network troubleshooting for end users.
- Built and managed a Wazuh SIEM environment, integrating Windows and Linux endpoints, developing custom detection rules, and investigating Sysmon events aligned with the MITRE ATT&CK framework.
- Implemented ZTNA using Netbird eliminating public exposure of internal services.
- Secured web applications by deploying a BunkerWeb Web Application Firewall (WAF).
- Conducted vulnerability assessments using Tenable Nessus Essentials, identifying and remediating security weaknesses across Windows Server and Active Directory environments.
- Monitored network and server health with ManageEngine OpManager using WMI and SNMP, forwarding operational telemetry to the SIEM for centralized monitoring.
- Developed foundational knowledge of an XDR and their role in endpoint protection, threat detection, investigation, and response within SOC environments.

TECHNICAL PROJECTS

Blockchain Development

Architected functional blockchain DApps and deployed secure Ethereum smart contracts using Solidity programming.

Cybersecurity Home Lab & Infrastructure Hardening

- Built dedicated cybersecurity home lab environments to conduct rigorous security testing, infrastructure hardening, and network administration.
- Deployed centralized SIEM solutions and configured host-based endpoint agents for real-time monitoring and log aggregation.
- Conducted vulnerability assessments using Tenable Nessus to identify, analyze, and remediate system misconfigurations.

Network Security & System Administration

- Configured custom WAF policies, perimeter firewall rules, and secure network segmentation to protect local application deployments.
- Administered Windows Server infrastructures with Active Directory (AD) and Group Policies, alongside Linux servers running DHCP, NFS, and HTTP web services.
- Automated routine system tasks and network operations by engineering custom Bash scripts and Python utilities.

TECHNICAL SKILLS

Cybersecurity

SIEM, Security Monitoring, Log Analysis, Vulnerability Assessment, Tenable Nessus, WAF, Firewall Configuration, Threat Detection, SOC Operations.

System Administration

Windows Server, Active Directory, Group Policy, Linux Administration, DHCP, DNS, NFS, HTTP Services, Office 365.

Blockchain

Ethereum, Smart Contracts, dApps.

Research & Documentation

Technical Research, Security Research, Report Writing, Technical Documentation, Microsoft Word, Excel, PowerPoint, Data Analysis, Presentation Development.

Networking

TCP/IP, OSI Model, Routing, Switching, Network Design, Network Security, Troubleshooting, zero trust network access.

Programming & Development

Python, Bash, JavaScript, PHP, SQL, HTML, Solidity.

Operating Systems & Support

Windows 10/11, OS Installation & Troubleshooting, Hardware Troubleshooting, System Diagnostics, PC Maintenance.

CERTIFICATIONS

Cisco Cyber Threat Management

2026

Palo Alto: Cloud Security Fundamentals

2026

Palo Alto: Introduction to SecOPS

2026

Cisco Enterprise Networking, Security, and Automation

2025

Cisco JavaScript Essentials

2025

Oracle Database Programming with SQL

2022

Cisco IT Essentials: PC Hardware and Software

2021

Palo Alto: Network Security Fundamentals

2026

Palo Alto: Security Operations Fundamentals

2026

Cisco Linux 1

2025

Cisco Network Security

2025

Cisco Switching, Routing, and Wireless Essentials

2023

Cisco Introduction to Networks

2022