Talha Muneer

ID: 4240132972985 | **Place of birth:** Pakistan | **Nationality:** Pakistani | **Gender:** Male | **Phone number:** (+92) 03206805269 (Mobile) | **Email address:** talhamuneer258@gmail.com |

Address: lalazar estate lane 02, Rawalpindi, 46000, Rawalpindi, Pakistan (Home)

ABOUT ME

Dynamic cybersecurity-focused system administrator with over 2 years of hands-on experience managing and securing IT environments. Proven expertise in virtualization (VMware ESXi, Proxmox), Windows/Linux server administration, Active Directory, DNS/DHCP, and VPN/firewall configuration. Demonstrated success deploying centralized monitoring (Nagios, PRTG) and integrating Wazuh SIEM to enable proactive threat detection and swift incident response. Skilled in backup (Veeam) and antivirus management to maintain resilient, secure infrastructure.

EDUCATION AND TRAINING

2024 – CURRENT Rawalpindi, Pakistan

MASTER'S IN COMPUTER SCIENCE Foundation University Islamabad

2019 – 2023 Multan, Pakistan

BACHELOR IN COMPUTER SCIENCE MNS University of Agriculture Multan

WORK EXPERIENCE

06/2023 – CURRENT Rawalpindi, Pakistan

SYSTEM ADMINISTRATOR CSD - HEAD OFFICE

In my role as System Administrator, I successfully handled the following responsibilities:

- Configured and managed Active Directory (ADDS, CDC), DNS, DHCP, RAID, and NAS.
- Administered virtualization platforms: VMware ESXi, Xen Server, Proxmox VE.
- Monitored server health with HPE OneView, iLO, PRTG, and Nagios.
- Configured Zimbra mail server, integrated NextCloud & OwnCloud.
- Managed Kaspersky Security Center and VPN solutions.
- Administered Red Hat Linux, NFS, and Veeam Backup solutions.
- Monitored network security with NMS and Wazuh SIEM.

PROJECTS

10/2024 – 02/2025

Security Information and Event Management (SIEM) Implementation - CSD

- Performed Proof of Concept (POC) and deployment of Wazuh SIEM to enhance real-time log analysis and threat detection.
- Integrated various log sources, including endpoint agents and firewalls, into the Wazuh syslog server.
- Managed Kaspersky EDR for proactive threat hunting, IOC, and automated remediation.

10/2024 – CURRENT

Endpoint Security & Threat Detection Deployment

- Deployed and managed Sangfor Endpoint Detection and Response (EDR) across the organization's head office and remote stations.
- Established secure site-to-site VPN connectivity between Data Center and remote sites using pepwave & pfSense.
- Conducted cybersecurity awareness sessions and training for staff at remote sites to improve security posture and incident reporting culture.

SKILLS

IT Security Operation | SOC (Security Operation Center) | WAZUH | LDAP | implement a virtual private network | KASPERSKY | Office 365 | EXSI vSphere & Web | E-Mail Exchange Server | REDHAT CENT OS | Mail Services

(Zimbra) | Cloud storage - NextCloud and Owncloud - integration knowledge | Proxmox Mail Gateway | PRTG Monitoring | Monitoring tools - Kibana, Grafana, Nagios | Endpoint Detection & Response | LAN Switching, Advanced | nagios / zabbix