# MUHAMMED ALI S

Dubai, UAE | muhammedali0021@outlook.com | +971 502121435 |
https://www.linkedin.com/in/muhammed-ali-2829a5292 | UAE Driving License

## Professional Summary

Cybersecurity-focused IT professional with CEH certification and hands-on experience in FortiGate firewall management, Microsoft Entra ID administration for 500+ users, endpoint security, and vulnerability assessment across enterprise environments. Delivered cybersecurity awareness programs to 200+ employees. Currently pursuing Microsoft SC-200 certification and seeking opportunities as a SOC Analyst, Cybersecurity Analyst or IT Security Engineer, where I can contribute to enterprise security operations while continuing to develop expertise in threat detection, incident response and security monitoring.

## Technical Skills

- **Cybersecurity:** Vulnerability Assessment, Basic Penetration Testing, Web Application Security (OWASP Top 10), Security Monitoring, Incident Awareness, Security Awareness Training.
- **Security Solutions:** FortiGate Firewall (40F, 80F, 100F), IPS, Web Filtering, Application Control, Anti-Malware, Endpoint Security, Identity & Access Management, Policy Management.
- **Microsoft Technologies:** Microsoft 365 Administration, Exchange Online, MFA Configuration, User Management, Licensing, Outlook Troubleshooting.
- **Networking:** TCP/IP, DNS, DHCP, VPN, Routing & Switching Fundamentals, Network Troubleshooting.
- **Tools:** Nmap, Burp Suite, Wireshark, Nessus, Kali Linux, Microsoft 365 Admin Center.
- **Endpoint Security:** Acronis Cyber Protect, Microsoft Defender, Endpoint Protection, Anti-Malware.
- **System Administration:** Windows Installation, Patch Management, Printer Configuration, Software Deployment, User Support.
- **Backup Solutions:** 3CX Backup and Restore, Configuration Backup.
- **Operating Systems:** Windows 10/11, Windows Server Fundamentals, Linux (Ubuntu, Kali Linux).

## Professional Experience

**IT Security & Support Engineer** Sep 2025 – Present

*Sahhim Trading and Technology* Dubai, UAE

- Administered Microsoft 365 and Microsoft Entra ID environments across multiple client organizations supporting 500+ users, managing user accounts, licensing, MFA and resolving authentication and email issues.
- Configured and maintained FortiGate firewalls (40F, 80F, and 100F), implementing IPS, Web Filtering, Application Control, Anti-Malware and security policies to strengthen network security across multiple client environments.
- Installed, configured and monitored Acronis Cyber Protect endpoint security solutions, ensuring enterprise endpoints remained protected against malware, ransomware and other security threats.
- Performed Windows operating system and application patch management, ensuring endpoints remained up-to-date with the latest security updates and reducing exposure to known vulnerabilities.
- Installed, configured, and maintained Windows workstations, printers and enterprise software while providing technical support to end users across multiple client environments.
- Supported VPN user access configuration and troubleshooting, ensuring secure remote connectivity for employees.
- Managed DHCP services and assisted in maintaining network infrastructure, endpoint connectivity and network availability.
- Conducted cybersecurity awareness training sessions for more than 200 employees across 3+ organizations, covering phishing, ransomware, password security, social engineering and cybersecurity best practices.
- Managed a high-availability, direct-response IT support channel, triageing and resolving 15+ Tier 1/2 incidents daily regarding endpoint configuration, network connectivity, and M365 access
- Participated in vulnerability assessment activities for internal web applications and network environments, identifying common security weaknesses and documenting remediation recommendations.
- Managed and troubleshot 3CX IP-PBX systems, including backups and restoration, ensuring reliable communication and minimal downtime

## Certifications

- Certified Ethical Hacker (CEH)
- Certified Penetration Tester (CPT)
- Google IT Support Professional Certificate
- Microsoft SC-200 Security Operations Analyst - In Progress (Expected Q3 2026)

## Projects & Lab Work

**Web Application VAPT - Real World Assessment**

- Conducted vulnerability assessments on live internal web applications using Burp Suite, Nmap, and Nessus.
- Identified OWASP Top 10 vulnerabilities including misconfigurations and sensitive data exposure; delivered prioritized remediation reports.

**Network Security Assessment - Infrastructure Audit**

- Performed internal network scanning and security analysis using Nmap and Wireshark to identify open ports, weak protocols, and misconfigurations.
- Recommended security hardening measures including firewall rule optimization and network segmentation.

**Security Awareness Program - Campus & Corporate**

- Conducted cybersecurity awareness workshops for 60+ university students covering core security practices and threat awareness.
- Designed and delivered phishing awareness training for 200+ corporate employees across 3 organizations, improving resistance to social engineering attacks.

## Education

**B.Tech in Computer Science and Engineering** 2021 – 2025

*APJ Abdul Kalam Technological University* Kerala, India

## Internship

**Cyber Security Intern** April 2025 - June 2025

*Infotact Solutions* Bengaluru, India

- Assisted in vulnerability assessment and penetration testing of web applications and network systems.
- Performed reconnaissance, scanning and vulnerability analysis using security tools.
- Supported security reporting and documentation under supervision.

## Languages

- **English**: Professional Proficiency
- **Hindi**: Basic proficiency
- **Tamil**: Basic proficiency
- **Malayalam**: Native