

FARHAN MOHAMMED FATHAH

IT Support & NOC Analyst | Transitioning into
SOC / Security Operations

Dubai, UAE • +971 55 557 2142 •
farhanfathah@gmail.com



PROFESSIONAL SUMMARY

IT Operations analyst with 13 years in NOC, service desk, and identity & access management, now transitioning into Security Operations. Resolved identity-based security incidents — phishing, compromised accounts, MFA, VPN anomalies — for 3,500+ users, and monitored enterprise infrastructure across BMC TrueSight, SCOM, Nagios, and Site24x7. Built SOC-ready skills through self-study labs in Microsoft Sentinel, Splunk, and OPNsense, including device onboarding and playbook configuration. (ISC)² CC and CEH v13 certified, Microsoft SC-300 (Identity & Access), CCNA; currently preparing for Microsoft SC-200 (Security Operations Analyst) and building Python/AI-ML skills for SOC automation.

CORE SKILLS

- Security Operations & Incident Response: Phishing/malware response, compromised-account remediation, MFA enforcement, sign-in & risk analysis, VPN security (Cisco AnyConnect), endpoint protection, firewall access control
- Understanding of common attack frameworks (MITRE ATT&CK), network protocols, and endpoint behavior.
- Identity & Access Management: Active Directory, Microsoft Entra ID (Azure AD), hybrid identity, RBAC, Conditional Access, Identity Protection, Microsoft SC-300
- Monitoring & Threat Detection: BMC TrueSight, Entuity, NetFlow Analyzer, Site24x7, SCOM, Nagios, ManageEngine OpManager, Microsoft Defender ATP
- Compliance & ITSM/ITIL: Incident, problem & change management, SLA/KPI ownership, root cause analysis, ServiceNow, BMC Remedy, ManageEngine ServiceDesk Plus
- Infrastructure & Networking: Windows Server, VMware, SCCM, Intune, Linux, TCP/IP, DNS, DHCP, Microsoft 365 (Exchange Online, Teams)
- Hands-on Labs (self-study): Microsoft Sentinel (device onboarding, playbook configuration), Splunk, OPNsense firewall configuration — personal SOC lab environment
- In Progress: Microsoft SC-200 (Security Operations Analyst) exam; Python, AI/ML fundamentals, AIOps

EXPERIENCE

IT Support Specialist & NOC Analyst | ENOC — Dubai

Feb 2022 – Present

Security Operations & Incident Response

- Triaged abnormal user activity, suspicious browser behavior, and identity-related incidents across Active Directory/Entra ID for 3,500+ users.
- Investigated suspicious VPN logins — foreign IPs, mismatched geolocation, MFA failures — blocking unauthorized access attempts.
- Remediated compromised accounts via password resets and MFA re-enforcement, closing confirmed identity incidents.
- Validated and cleaned phishing-exposed endpoints through AV scanning and malware checks.
- Logged and categorized incidents in BMC Remedy with root-cause notes, maintaining escalation workflow compliance.

Monitoring & Alert Triage

- Monitored enterprise infrastructure in BMC TrueSight, Entuity, Site24x7, and NetFlow Analyzer, flagging anomalies and traffic deviations before service impact.
- Triaged first-level alerts — latency spikes, abnormal device behavior — and escalated confirmed incidents to L2/L3.
- Monitored POS, Pumpomat, and NCR retail systems across 800+ locations, sustaining stable and secure operation.

Identity & Access Security

- Administered access controls (privileged accounts, groups, licenses, hybrid identity sync) in Active Directory/Microsoft 365 for 3,500+ users.
- Validated MFA challenges and sign-in anomalies, escalating confirmed cases to L2/L3 security teams.

Recognition

- Earned a Certificate of Recognition (Q2 2023) from ENOC for monitoring responsiveness and incident handling.

IT Operations & Support Engineer | Expo 2020 — Dubai

Jun 2021 – Feb 2022

- Secured IT operations supporting delegations from 190+ countries during Expo 2020 Dubai.
- Enforced patch and software-deployment compliance via ManageEngine Desktop Central, reducing endpoint attack surface.
- Resolved security incidents across Active Directory, Exchange/Outlook, and Cisco AnyConnect VPN.
- Standardized endpoint builds via Acronis imaging, cutting deployment time and configuration drift.
- Maintained AV, CCTV, and VMS/SMS physical-security systems for continuous operation.
- Managed mobile device compliance via Microsoft Intune and monitored network health via ManageEngine OpManager, flagging incidents for NOC escalation.
- Logged and resolved tickets via ServiceNow and ManageEngine ServiceDesk Plus, maintaining SLA compliance.
- Onboarded endpoints to Microsoft Defender ATP, extending threat-detection coverage across the device fleet.

Employment Gap — COVID-19 Layoff | Dubai, UAE

Jul 2020 – Jun 2021

- Role eliminated due to pandemic-related business downsizing; resumed IT operations at Expo 2020 Dubai.

IT Coordinator | KPFF Global — Dubai

Aug 2015 – Jul 2020

- Administered identity and access on Windows Server 2012 R2 Active Directory and Exchange Online for 40+ users.
- Managed patching, antivirus, licensing, and backups across the IT asset lifecycle, reducing unlicensed/unpatched exposure.
- Administered firewalls, routers/switches, and biometric access control for facility security.

System Engineer | Infosys Ltd — Bangalore

Jun 2013 – Dec 2014

- Delivered L1/L2 infrastructure support for Daimler Mercedes-Benz's European Data Centre under regulated change control.
- Monitored infrastructure via SCOM and Nagios, flagging service risks before customer impact.
- Administered Active Directory, HP/Dell servers, VMware, SCCM, and LAN/WAN under ITIL-aligned change management.

CERTIFICATIONS

- (ISC)² Certified in Cybersecurity (CC)
- Certified Ethical Hacker v13 with AI
- Microsoft SC-300: Identity and Access Management Associate
- CCNA
- Microsoft SC-200: Security Operations Analyst — in progress
- Cybersecurity Internship — National Institute of Electronics & Information Technology (NIELIT)
- IBM Cloud Core Essentials, 2020
- Artificial Intelligence & Machine Learning using Python — in progress

EDUCATION

Bachelor of Engineering, Electronics & Telecommunications — Visvesvaraya Technological University (VTU), Mar 2012