



FARHAN MOHAMMED FATHAH

+971555572142

farhanfathah@gmail.com

Dubai

Security-Focused IT Operations Engineer

PROFESSIONAL SUMMARY

Security-focused IT professional with 11+ years of experience in monitoring, incident response, identity security, threat investigation, and enterprise infrastructure operations across ENOC and Expo 2020. Skilled in alert triage, log analysis, access security, compromised account handling, and endpoint threat remediation. Strong foundation in cybersecurity principles, CEH concepts, network security, Windows/AD security, and hybrid identity environments. **Certified in CEH v13, ISC2 CC, Microsoft SC-300, CCNA.** Actively transitioning into SOC Analyst role with strong analytical ability, rapid learning, and operational discipline.

EXPERIENCE

ENOC - Emirates National Oil Company

Dubai

Feb 2022 - Present

IT Support Engineer(Security Assisted Operation)

ENOC operates 24/7 critical infrastructure where network reliability and secure access are essential. In my current role, I monitor enterprise systems, respond to alerts, support identity-related security incidents, and ensure uptime of critical retail systems. My responsibilities align directly with SOC Analyst L1 functions including event triage, anomaly detection, and escalation.

Security Operations & Incident Response

- Analyze and respond to abnormal user activity, suspicious browser behavior, and identity-related security incidents.
- Investigate suspicious VPN login attempts such as foreign logins, geolocation mismatches, and MFA failures.
- Perform compromised account remediation, secure password resets, MFA enforcement, and escalate cases to cybersecurity teams.
- Conduct malware validation, antivirus scans, and threat cleanup for endpoints impacted by phishing or malicious links.
- Document incidents in BMC Remedy with correct categorization, root-cause notes, and adherence to escalation workflows.
- Collaborate with Cybersecurity and IAM teams on identity security events and potential compromise indicators.

Monitoring & Alert Triage

- Proactively monitor enterprise infrastructure using BMC TrueSight and Entuity to detect anomalies, unusual traffic, device faults, and potential security risks.
- Perform first-level triage of alerts and escalate potential security incidents such as latency spikes, abnormal device behavior, and traffic anomalies.
- Monitor critical retail systems (POS, Pumpomat, NCR) to ensure stable and secure operations across 400+ national locations.

Identity & Access Security

- Manage access controls for 3,500+ users across Active Directory and Microsoft 365, including privileged accounts, groups, license management, and hybrid identity synchronization.
- Validate suspicious MFA prompts, login failures, and sign-in anomalies before escalating to L2/L3 security teams.

EXPO 2020

DUBAI

Jun 2021 - Feb 2022

IT SUPPORT ENGINEER

Expo 2020 Dubai was one of the largest global events, hosting 190+ participating countries and millions of visitors. IT infrastructure played a mission-critical role in enabling seamless operations, real-time connectivity, security, and visitor engagement across the Mobility Zone. As part of the frontline IT team, I ensured stability, responsiveness, and excellence in technical support throughout this high-profile international event.

- Supported high-availability operations across 500+ endpoints with secure configuration, patching, and identity management.
- Worked closely with NOC and cybersecurity teams to apply firewall rules and harden network access during peak operations.
- Ensured secure VPN access (Cisco AnyConnect), AD authentication, and M365 account stability for international delegations.
- Delivered zero-downtime operations in a mission-critical global environment.

KPFF GLOBAL

DUBAI

Aug 2015 - Jul 2020

IT COORDINATOR

At KPFF Global, a leading construction consultancy, IT plays a vital role in powering engineering design, project collaboration, and operational efficiency. Supporting both corporate systems and specialized construction software, I ensured uninterrupted access to tools critical for planning, modeling, and delivery—enabling teams to meet tight deadlines and maintain project excellence.

- Led IT operations and maintenance across users, servers, and infrastructure—ensuring maximum system uptime.
- Administered AD 2012 R2 and Exchange Online, streamlining user access, policies, and permissions for 40+ employees.
- Optimized Office 365 and network printer performance, reducing support requests through proactive troubleshooting.
- Managed hardware, software, and network assets end-to-end, including backups, patching, and license compliance.
- Supported critical infrastructure—firewalls, routers, switches, PABX, and biometrics during major network expansions.
- Enhanced service delivery by standardizing device setups, mobile mail configurations, and reimaging workflows.
- Maintained inventory of parts for emergency repairs.

INFOSYS LTD

BANGALORE

Jun 2013 - Dec 2014

SYSTEM ENGINEER

Started my IT career with Infosys Ltd through campus placement in 2012, assigned to the prestigious Daimler Mercedes-Benz European Data Centre project. In this high-availability environment, I ensured seamless operations and infrastructure stability through proactive monitoring and support. My contributions helped maintain 24/7 uptime across critical systems, earning recognition for reliability and technical excellence.

- Monitored Daimler Mercedes-Benz Data Centre environment end-to-end, ensuring
- Supported 24/7 monitoring of Daimler's European data center using Nagios/SCOM.
- Managed Windows Server, VMware, LAN/WAN troubleshooting, and patch compliance.
- Ensured secure, stable operations through proactive monitoring and ITIL-based change management.

EDUCATION

Visvesvaraya
Technological
University (2008-
2012)

Bachelor of Engineering in Electronics and Telecommunications

GPA: 6.8

CORE SECURITY SKILLS

- **Security Monitoring & Alert Triage** (anomalies, identity alerts, suspicious login patterns)
- **Identity Security** (Azure AD / Entra ID, MFA, Conditional Access, compromised accounts)
- **Network Security Fundamentals** (firewalls, routing/switching, NetFlow monitoring, CCNA-level)
- **Incident Response Support** (containment, escalation, documentation, coordination)
- **Log Analysis** (Windows Event Logs, authentication logs, M365 sign-in logs)
- **SIEM (Beginner)** – hands-on training and foundational understanding for L1 SOC roles
- **Threat Investigation** (VPN anomalies, foreign logins, phishing indicators, malware cleanup)
- **Endpoint & User Security** (antivirus cleanup, threat validation, secure configurations)
- **ITSM & Monitoring Tools:** BMC TrueSight, Entuity, ManageEngine, BMC Remedy

CERTIFICATIONS

- Certified in Ethical Hacking v13
- Internship in Cybersecurity from National Institute of Electronics & Information Technology(NIELIT)
- Certified in Cybersecurity, (ISC)2 CC
- CCNA
- Microsoft SC-300 Identity and Access Management Associate
- IBM Cloud Core essential

ETHICAL HACKING SKILLS

- Conducting penetration tests on networks, systems, and web applications to identify vulnerabilities.
- Proficient in vulnerability assessment and exploitation using tools such as Metasploit, Nmap, Burp Suite, and Wireshark.
- Knowledge of OWASP Top 10 vulnerabilities and secure coding practices.
- Performing password attacks, privilege escalation, and lateral movement in Windows and Linux environments.
- Testing wireless network security (WEP/WPA/WPA2/WPA3) and mobile application security.
- Experience with vulnerability scanning tools like Nessus .
- Strong understanding of ethical hacking principles, cybersecurity laws, and responsible disclosure.
- Skilled in implementing security controls, incident response procedures, and risk mitigation strategies.

LOOKING AHEAD

Eager to apply my monitoring experience, security awareness, and analytical skills to a forward-thinking security team focused on threat detection, incident response, and operational resilience.

REFERENCES

Upon Request

PROJECTS / PORTFOLIO

Nmap Blue Team Toolkit (GitHub Pages)

- Built an interactive blue-team focused Nmap command builder for authorized testing and education.
- Scan library with categories/tags, copy-to-clipboard command generation, and SOC-style notes + sample outputs.
- Command history (saved locally) to support documentation and quick comparisons between runs.
- Designed for safe usage: no live scanning from the site; commands run only in user-controlled lab environment.

Link

GitHub: <https://github.com/farhanfathah-cyb/nmap-blue-team-toolkit>

Update the link above if your repo URL is different.