

Syed Muntazir Mehdi

✉ info@muntazirmehdi.com  muntazirmehdi.com  [LinkedIn](#)

WORK EXPERIENCE

IT Support Specialist

Vision Industrial Company

Dammam, Saudi Arabia

June 2025 - Present

- Delivered first-line support to staff, fixing common hardware and software issues.
- Set up new PCs, installed applications, and made sure systems were updated and secure.
- Helped with account management, including creating, disabling, and resetting passwords.
- Logged support requests and passed more complex problems to senior IT staff.

Security Analyst

Asia Pacific University of Technology & Innovation

Kuala Lumpur, Malaysia

Jan 2024 - April 2024

- Performed vulnerability assessments and penetration testing on APU lab devices.
- Identified and resolved vulnerabilities in the lab environment, reducing security risks.
- Delivered clear reports with findings and remediation steps.

IT Intern - LAB Security Analyst

Asia Pacific University of Technology & Innovation

Kuala Lumpur, Malaysia

Sep 2023 - Jan 2024

- Deployed and supported lab PCs imaged devices, configured standard accounts, troubleshoot hardware and software issues.
- Created documentation and user guides with the tech lab team for APU Knowledgebase

SOC Analyst Training

Asia Pacific University of Technology & Innovation

Kuala Lumpur, Malaysia

Apr 2023 - July 2023

- Used the SIEM (MSSGard) to run searches, create content, and compile reports, coordinating with team leads and the SOC Manager.
- Monitored host, network, and device logs and triaged alerts when activity looked suspicious.

EDUCATION

Asia Pacific University (Malaysia) & De MontFort University (UK)

B.Sc. (Hons) in Cyber Security - Dual Degree Awarded

Kuala Lumpur, Malaysia

Sep 2021 - Aug 2024

CERTIFICATIONS

- | | |
|--|-----------|
| • Blue Team Level 1 (BTL1) Security Blue Team | Sep 2025 |
| • Red Hat System Administration (RH124) Red Hat | Sep 2024 |
| • SOC Analyst Learning Path LetsDefend | July 2024 |
| • Junior Penetration Tester (eJPT) eLearnSecurity | May 2024 |
| • INE Certified Cloud Associate (ICCA) eLearnSecurity | May 2024 |
| • Switching, Routing, and Wireless Essentials Cisco | Jan 2023 |

SKILLS

Threat Hunting & SIEM: Splunk, Elastic (KQL), Windows Security, Sysmon, PowerShell, ATT&CK

DFIR & Network Analysis: Autopsy, Windows Artifact and timelines, packet analysis with Wireshark

Monitoring: Wazuh, Velociraptor, Osquery, Grafana, Prometheus, Node Exporter, cAdvisor

Linux/Ops: Arch Linux, Docker & Docker Compose, Cloudflare Tunnel/Zero Trust, Tailscale, Adguard

Security Testing: Metasploit, Hydra, gobuster, John the Ripper, Phishing /email-dear analysis.