

SHAHZEB ALI

SOC ANALYST INTERN | CYBERSECURITY OPERATIONS

Abu Dhabi, UAE | +971 58 611 2232 | shahzeb@shahsmen.com
linkedin.com/in/ishahzeali | shahsmen.com

UAE family-sponsored residence visa | Available immediately | Open to relocation to Dubai

PROFESSIONAL SUMMARY

Cybersecurity practitioner with a Bachelor of Science in Computer Science and hands-on practice in SOC-focused labs, CTFs, log analysis, phishing investigation, and threat hunting. Familiar with SIEM concepts and Splunk, EDR telemetry, Windows Event Logs, Linux syslog, network traffic analysis, and mapping attacker behaviour to MITRE ATT&CK. Uses Python and Bash for basic scripting and values accurate evidence handling, clear incident documentation, and continuous learning. Seeking to contribute to ProofOps' 24x7 SOC while developing practical alert-triage and incident-response skills.

TECHNICAL SKILLS

SOC & Detection: Alert triage fundamentals, event classification, escalation, IOC enrichment, false-positive awareness, incident timelines and reporting

SIEM / Endpoint: Splunk, Microsoft Sentinel, ELK Stack, Sysmon, Microsoft Defender for Cloud, EDR/XDR concepts, Snort, IDS/IPS alerts

Logs & Network: Windows Event Logs, Linux syslog, firewall and DNS logs, TCP/IP, OSI model, HTTP/S, Wireshark, packet analysis

Threat Analysis: MITRE ATT&CK, Cyber Kill Chain, phishing analysis, IOC extraction, threat hunting fundamentals, OWASP Top 10, API security

Systems & Scripting: Linux CLI, Windows internals, Active Directory fundamentals, Python, Bash, PowerShell

Security Frameworks: NIST CSF, ISO/IEC 27001, Pyramid of Pain, Diamond Model

PROJECTS & PRACTICAL EXPERIENCE

Enterprise Phishing & Data Exfiltration Investigation | TryHackMe | Dec 2025

- Investigated a simulated enterprise compromise spanning phishing activity, suspicious PowerShell execution, and DNS-tunnelling indicators.
- Reviewed Sysmon and endpoint-related evidence, decoded Base64 content, and reconstructed attacker activity using the Cyber Kill Chain.
- Mapped observed tactics and techniques to MITRE ATT&CK and documented detection gaps with practical rule recommendations.

Blue-Team CTFs & SOC Practice Labs | Blue Team Labs Online (BTL) and TryHackMe

- Practised investigation-oriented challenges and security labs to build familiarity with alert analysis, log review, and evidence-led reasoning.
- Applied networking and Linux fundamentals while investigating suspicious activity in controlled training environments.

Responsible Vulnerability Disclosure — Deezer | YesWeHack | Aug 2025

- Identified and responsibly reported an IDOR / Broken Access Control issue affecting a production API; the report contributed to a production fix.
- Prepared a proof of concept and documented the issue in line with OWASP Top 10: A01 Broken Access Control.

Mastercard Cybersecurity Virtual Experience | Forage | Dec 2025

- Reviewed simulated phishing campaigns and departmental risk exposure, then developed targeted security-awareness recommendations.

CERTIFICATIONS

Fortinet Certified Associate in Cybersecurity (FCA) • Certified SOC Analyst Level 1 — TryHackMe • Junior Penetration Tester — TryHackMe • ISO/IEC 27001 Information Security Associate — Skill Front • Cybersecurity 101 — TryHackMe • Linux 100: Fundamentals — TCM Security

EDUCATION

Bachelor of Science in Computer Science | Lahore Garrison University, Lahore, Pakistan | 2020–2025