SHAHZEB ALI

SOC Analyst (Level 1) | Cybersecurity Analyst | Purple Team Specialist

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

Nationality: Pakistani | Visa: UAE Family-Sponsored Residence Visa | Languages: English (Fluent), Urdu (Native)

PROFESSIONAL SUMMARY

Results-driven SOC Analyst with over 2 years of hands-on incident response experience across healthcare and technology environments. Specialises in SIEM-based threat detection, log correlation, and full-lifecycle incident management. Holds a unique purple team advantage — using penetration testing knowledge to sharpen defensive detection logic and reduce false-positive rates. Recognised on YesWeHack for responsibly disclosing a critical Broken Access Control vulnerability in Deezer, resulting in a global patch. Proficient in Splunk, Microsoft Sentinel, ELK Stack, Wireshark, and Sysmon; deeply versed in MITRE ATT&CK, the Cyber Kill Chain, and ISO/IEC 27001.

TECHNICAL SKILLS

SIEM & Monitoring: Splunk, Microsoft Sentinel, ELK Stack (Elasticsearch/Kibana), Azure Cloud Defender, Snort, Sysmon, EDR/XDR, SOAR

Incident Response: Alert Triage, IOC Extraction, Escalation, Root Cause Analysis, Phishing Analysis, Post-Incident Reporting

Log Analysis: Windows Event Logs, Linux Syslog, Firewall Logs, IDS/IPS Alerts, Azure AD Sign-in Logs, Web Activity Logs

Threat Intelligence: MITRE ATT&CK, Cyber Kill Chain, Pyramid of Pain, Diamond Model, TTP Mapping, Vulnerability Tracking

Offensive Security: Burp Suite, Nmap, Metasploit, Hydra, Gobuster, OWASP Top 10, API Security Testing, Responsible Disclosure

Network & Protocols: Wireshark, TCP/IP, DNS, HTTP/S, OSI Model, Packet Analysis, DNS Tunnelling Detection

Systems & Scripting: Windows Internals, Linux CLI, Active Directory, PowerShell, Python, Bash, Privilege Escalation Analysis

Frameworks & GRC: ISO/IEC 27001, NIST CSF, CIS Controls, RBAC, Security Awareness Programme Design

PROFESSIONAL EXPERIENCE

SOC Analyst L1

Dec 2022 – Jul 2024

CureMD | Lahore, Pakistan

- Monitored and triaged 150+ daily security alerts across Microsoft Sentinel, EDR, and Azure Cloud Defender, sustaining a false-positive rate below 12% through structured severity classification and endpoint baseline profiling.
- Investigated phishing campaigns, credential-based intrusions, and lateral movement activity; escalated fully-documented, actionable cases to L2/L3 analysts with an average mean time to escalate (MTTE) of 25 minutes.
- Deployed Sysmon across critical healthcare endpoints and authored custom detection rules that surfaced Living-off-the-Land (LotL) tactics, reducing estimated attacker dwell time by 30%.
- Correlated Windows Event Logs, Azure AD audit logs, and cloud trails against MITRE ATT&CK techniques, producing structured threat intelligence reports consumed by senior analysts and the CISO.
- Contributed to the organisation's HIPAA compliance audit renewal by collaborating with DevSecOps to harden cloud infrastructure configurations and close identified control gaps.
- Designed and ran bi-monthly phishing simulation campaigns, achieving a 40% reduction in click-through rates across high-risk business units within two quarters.

SOC Analyst L1 (Internship)

Feb 2022 – Aug 2022

Arwen Tech | Lahore, Pakistan

- Triaged 100+ daily security events from SIEM, IDS/IPS, and perimeter firewalls; implemented a severity classification framework that reduced average escalation time by 20%.
- Distinguished true positives from false positives through structured initial analysis, delivering complete case files to L2/L3 analysts and reducing duplicated investigation effort across shifts.
- Maintained audit-ready incident records within the case management system, enabling seamless shift handover and consistent knowledge transfer across the SOC team.
- Correlated firewall and endpoint logs in Splunk against MITRE ATT&CK TTPs, identifying and containing multiple IOCs before they progressed to active exploitation stages.
- Proposed three detection rule optimisations during post-incident reviews, all of which were adopted into the team's standard SOC playbook.

Independent Security Researcher *Aug 2025 – Aug 2025*

YesWeHack Bug Bounty Platform | Remote

- Discovered a critical Insecure Direct Object Reference (IDOR) / Broken Access Control vulnerability in Deezer's production API by manipulating JSON POST parameters to bypass backend authorisation logic.
- Authored a comprehensive Proof of Concept (PoC) mapped to OWASP Top 10 (A01:2021), enabling Deezer's engineering team to deploy a global security patch within their disclosed SLA window.
- Applied systematic API endpoint behavioural analysis using Burp Suite, demonstrating advanced API security methodology directly transferable to SOC threat hunting and alert triage workflows.

KEY PROJECTS & SIMULATIONS

Enterprise Phishing & Data Exfiltration Investigation | TryHackMe *Dec 2025*

- Reconstructed the full Cyber Kill Chain from initial phishing access through DNS tunnelling exfiltration across a simulated compromised enterprise endpoint using EDR concepts and Sysmon log forensics.
- Decoded Base64 payloads, uncovered obfuscated PowerShell execution chains, and mapped all attacker TTPs to MITRE ATT&CK, producing a structured detection gap analysis with actionable rule recommendations.

Mastercard Cybersecurity Virtual Experience | Forage *Dec 2025*

- Identified active phishing campaigns, assessed departmental risk exposure, and designed targeted security awareness training programmes that demonstrably reduced simulated click-through rates across high-risk business units.

CERTIFICATIONS

- **Certified SOC Analyst L1 —** TryHackMe
- **Jr Penetration Tester —** TryHackMe
- **Fortinet Certified Associate in Cybersecurity (FCA) —** Fortinet
- **ISO/IEC 27001 Information Security Associate —** SkillFront
- **CyberSecurity 101 —** TryHackMe
- **Linux 100: Fundamentals —** TCM Security

EDUCATION

Bachelor of Science in Computer Science *2020 – 2025*

Lahore Garrison University | Lahore, Pakistan