

Muhammad Bilal

✉ mian.muhammad.bilal@proton.me ☎ +92 316 4343827 💻 in/mian-muhammad-bilal 🌐 mian-muhammad-bilal.github.io/

SUMMARY

Cybersecurity Analyst specializing in SOC operations, threat detection, and SIEM management. Proficient in log analysis and incident response using Wazuh and Splunk. Hands-on experience in vulnerability assessment and web application penetration testing. Cyber Security graduate dedicated to proactive risk mitigation and strengthening organizational security posture.

EDUCATION

Bachelor of Science in Cyber Security

University of Management and Technology • Lahore, Pakistan • 2025 • 3.42 CGPA

EXPERIENCE

Cyber security trainer

SparkED

December 2024 – Present

- Designed and delivered technical workshops on Network Security and Ethical Hacking, utilizing Kali Linux and Wireshark for live demos.
- Simplified complex concepts such as packet analysis and digital hygiene for non-technical audiences, enhancing security awareness posture.

PROJECT

Wazuh SOC Automation & Threat Detection

Self Initiated Project • github.com/Mian-Muhammad-Bilal/Wazuh-Threat-Detection-Lab.git

- Designed and deployed a hybrid SOC environment integrating Wazuh (SIEM) and Sysmon to monitor Windows 10 and Linux endpoints.
- Simulated and investigated 6+ attack scenarios (including credential theft and persistence techniques), mapping detected TTPs to the MITRE ATT&CK framework.
- Reduced alert fatigue by tuning correlation rules and authoring custom detections for PowerShell download cradles to validate security controls.
- Developed Python automation scripts to parse Wazuh alerts and automate incident reporting, streamlining the incident triage process.

SOC Simulation & Incident Response

LetsDefend

- Executed incident response workflows using IBM QRadar and Splunk, performing root cause analysis for simulated phishing and malware alerts.
- Wrote custom SPL queries to detect anomalies and analyzed log flows to validate security incidents.

CyberED – AI-Powered Cyber security Awareness Game (Final Year Project)

UMT • github.com/Mian-Muhammad-Bilal/CyberED-AI-Powered-Cybersecurity-Awareness-Game.git

- Developed a 2D Unity-based game with 5+ mini-games to gamify complex cybersecurity concepts and enhance learner engagement.
- Integrated an AI chatbot (Genesis) to provide real-time learning support and in-game assistance.

Website Penetration Testing

- Conducted black-box testing aligned with OWASP Top 10 using Burp Suite (manual), Nessus (automated), Nmap, and Nikto.
- Identified 5 critical vulnerabilities (e.g., SQLi, XSS) and provided remediation strategies that mitigated 87% of risks.

CERTIFICATIONS

Google Cybersecurity Professional Certificate

Google / Coursera • 2025

- Includes Linux, MySQL, and Python hands-on labs.

ISO 27001 Foundation – Information Security Certification

Skill Front • 2025

SKILLS

- **SOC & SIEM Operations:** Wazuh, Splunk, IBM QRadar, XDR Concepts, SOC L1 Operations, Log Analysis, Threat Detection.
- **Network Security:** OSI Model Security (Layers & Threats), Subnetting & IP Addressing, Firewalls & ACLs, Wireshark, Packet Tracer.
- **Web Security & Ethical Hacking:** OWASP Top 10, Burp Suite, Metasploit, Nessus, Nmap, Nikto, WPScan, SQL Injection.
- **Operating Systems & Virtualization:** Linux (Kali, Ubuntu, Tails), Windows, VMware, VirtualBox.
- **Malware Analysis & Forensics:** Static & Dynamic Analysis, Autopsy, FTK Imager.
- **Programming & Tools:** Python, C++, MySQL, Git, GitHub.
- **Soft Skills:** Cybersecurity Awareness Training, Workshop Delivery, Technical Reporting.