

SHAHUL HAMEED MAHEEN

■ shm.sec008@gmail.com | ■ 9345256883 | ■ linkedin.com/in/shm008 | ■ github.com/shm008 |
■ Tamilnadu, India

PROFILE SUMMARY

IT and Cybersecurity enthusiast with a strong foundation in Security Operations, Threat Detection, and Adversary Simulation. Hands-on experience with SIEM tools, log analysis, and incident detection workflows, developed through self-driven projects and internships. Adept in Python, Linux environments, and network forensics — aspiring to build a career as a SOC Analyst and Cybersecurity Architect.

EDUCATION

B.Tech – Information Technology | St. Xavier's Catholic College of Engineering (2022 – 2025) – CGPA: 8.23
Diploma – Computer Science and Engineering | Morningstar Polytechnic College (2022) – 96%
AISSCE – CBSE, The Rajas International School (2019) – 64%
SSLC – CBSE, Ibn-Al-Hytham Islamic School, Bahrain (2017) – 8.2 CGPA

TECHNICAL SKILLS

Core Areas: SOC Monitoring, Threat Detection, Log Analysis, Adversary Simulation, Vulnerability Management, Incident Response

Tools: Wazuh, Splunk, QRadar, ArcSight, Wireshark, Burp Suite, Metasploit, Nmap

Languages: Python, Bash | **Technologies:** Linux, Virtual Machines

PRACTICAL EXPERIENCE

Security Operations Center (SOC) Analyst | DefendShield CyberSecurity (07/2024 – 01/2026)

Threat Detection & Incident Response

- Built and tuned detection rules in Wazuh for SSH brute-force, web attacks, privilege escalation, and ransomware behavior.
- Monitored Linux, endpoint, and web server logs; performed alert triage and root cause analysis.
- Mapped detections to MITRE ATT&CK techniques (T1110, T1068, T1486) for structured threat reporting.
- Implemented automated active response for malicious IP blocking and attack containment.
- Configured File Integrity Monitoring (FIM) to detect abnormal file changes and encryption patterns.

Achievements: Built custom Wazuh correlation rules, integrated MITRE ATT&CK; mapping, and documented detection logic in lab setups.

Intern – VAPT & Cybersecurity | DefendShield CyberSecurity (06/2024 – 07/2024)

Performed vulnerability scanning and penetration testing using Burp Suite and Metasploit. Assisted in security assessments for web applications and APIs with detailed risk categorization.

PROJECTS

Vulnerability Analyzer (Python, JS, Flask) – Automated scanning and reporting system.

Data Breach Monitor (Python, Flask) – Real-time breach lookup with compliance emphasis.

LANGUAGES

English, Tamil, Hindi, Malayalam