Md. Mahim Hossain

Dhaka faaiz.mahim@gmail.com +880 18669-28533
LinkedIn GitHub

Professional Summary

I am a learner SOC Analyst Level 1, focusing on cybersecurity and basic networking for security. I am building my skills in threat detection, incident response, and security operations.

My goal is to grow as a SOC Analyst, work in Blue Team roles, and become a Security Engineer in the future. I am always learning and improving to stay prepared for new challenges in cybersecurity.

Education

BSc in Computer Science & Engineering Feb 2022 – Jan 2026
Green University of Bangladesh

Experience

SOC Intern — CodeAlpha Aug 2025 – Oct 2025
Monitored security alerts and analyzed logs using SIEM tools, gaining hands-on SOC experience.

SOC Intern — Cyber Academy Aug 2025 – Oct 2025
Performed alert triage and initial investigations using IDS/IPS and endpoint security tools.

SOC Analyst Level 1 (Intern) — 9AM Solution Sep 2025
Monitored events with Wazuh SIEM and detected threats using Suricata, Sysmon, YARA, and VirusTotal.

Campus Ambassador — Tech Secure 2.0 May 2025 – Present
Organized cybersecurity awareness activities and represented the program on campus.

Certifications

Pre Security — TryHackMe 2025
Introduction to Bash — Security Blue Team 2025
Complete Practical SOC for Blue Teaming — Udemy 2025
Beginner-Friendly SOC Analyst Course — Udemy 2025
30 Days SOC Challenge — Rajneesh Gupta 2025
Linux Log Analysis, Wireshark Traffic Analysis, Wazuh SIEM, Splunk, Phishing Analysis

Thesis

NeuroCrypt: Secure BCI Data Sharing Framework 2025 – Present
Privacy-preserving architecture for secure brain-computer interface data sharing.

Projects

Basic Network Sniffer
Developed a simple network sniffer for packet capture and analysis.
Tools: Python (Scapy/pcap), Wireshark

End-to-End SOC Monitoring & Response (Wazuh)
Designed a full SOC workflow with centralized logging, alert correlation, and automated response.
Tools: Wazuh, Sysmon, Suricata, YARA, VirusTotal

Technical Skills

Programming & Scripting: Python, C/C++, Java, Bash
Cybersecurity Tools: Log Analysis, Incident Response, Wazuh, Suricata, Snort, Wireshark, Nmap, Burp Suite
Platforms & Practice: Linux, Windows, Docker, TryHackMe, Hack The Box, LetsDefend