Shaik Abdul Rehman

Email: cybershaik66@gmail.com | LinkedIn: www.linkedin.com/in/shaik-abdul-rehman-b2175b354
Portfolio: https:https://shaikabdulrehman-cybersoc.netlify.app/

Professional Summary

Aspiring SOC Analyst and final-year BCA student with hands-on experience in cybersecurity investigations, SIEM monitoring, phishing analysis, malware traffic analysis, and incident response labs. Trained on Microsoft Defender XDR, Microsoft Sentinel, Google Chronicle SIEM, and security investigation tools. Passionate about threat detection, log analysis, and security operations.

Technical Skills

Security Tools: Microsoft Defender XDR, Microsoft Sentinel, Google Chronicle SIEM, Wireshark, VirusTotal
Security Concepts: Incident Response, Threat Detection, Log Analysis, Phishing Analysis, Malware Traffic Analysis
Other Skills: Generative AI Fundamentals, Security Automation Concepts

Cybersecurity Project

AI Security Assistant Agent – Automated SOC Workflow (Google × Kaggle Capstone Project)
Designed and built a multi-agent AI system to automate SOC operations such as threat detection, log parsing, and incident report generation. Implemented GenAI-driven decision logic to reduce manual alert workload and accelerate incident response.

Cybersecurity Training & Certifications

Cisco Introduction to Cybersecurity
IBM Cybersecurity with Generative AI
Google Chronicle Security Operations (SIEM) Training
Microsoft Sentinel & Microsoft Defender XDR Training
Microsoft Purview Information Protection and Data Loss Prevention
EC-Council SQL Injection Fundamentals
Advanced Prompt Engineering – UpGrad
Gemini University Student Program
Kaggle × Google AI Agent Intensive Program

Virtual Internships

Tata – Identity and Access Management (IAM) Security Internship
Deloitte – Cybersecurity Log Analyst Internship
AIG Shield – Cybersecurity Incident Response Simulation

SOC Investigation Labs (LetsDefend)

Phishing Email Analysis
Malware Traffic Analysis with Wireshark
Web Attack Investigation
Cyber Incident Handling
VirusTotal Threat Analysis
SIEM 101 Monitoring
Brute Force Attack Detection

Education

Bachelor of Computer Applications (BCA) – Final Year