Shaik Abdul Rehman

Andhra Pradesh, India | Open to Relocate — Kuwait / Saudi Arabia / UAE
+91-8247877558 cybershaik66@gmail.com LinkedIn GitHub Portfolio

Summary

CompTIA Security+ SY0-701 certified (Score: 829) BCA Honours graduate with hands-on experience in SIEM monitoring, incident response, threat detection, and SOC operations through internships, virtual simulations, and security-focused projects. Proficient in Microsoft Sentinel, Splunk, QRadar, Google Chronicle, TCP/IP, DNS, firewalls, and incident documentation. Familiar with SAMA CSF and NCA ECC compliance frameworks. Available for immediate relocation to Riyadh with full 24x7 shift flexibility.

Education

Yogi Vemana University **2023 – 2026**
Bachelor of Computer Applications Honours — CGPA: 8.50/10 *Andhra Pradesh, India*

Experience

Sandspace Technologies Pvt. Ltd. (APSCHE-Certified Internship) **Jan 2026 – Apr 2026**
Data Science Intern *Remote*

- Performed daily security checks using threat detection tools; identified and escalated malware alerts, phishing indicators, and suspicious network activities.
- Built ML-based malicious account detection system using Python and XGBoost; generated SOC-style investigation reports.

Codeworks EduTech Services (APSCHE-Certified Internship) **May 2025 – Jul 2025**
UI Developer Intern *Remote*

- Developed secure UI components and mitigated XSS vulnerabilities using input validation; gained hands-on exposure to network-facing application development.

Virtual Cybersecurity Simulations — Deloitte, AIG Shields, PwC, TCS (via Forage) **2025**
Cybersecurity Virtual Experience *Remote*

- Deloitte: Monitored SIEM alerts (Sentinel), triaged phishing, malware and unauthorized access attempts; collected evidence and prepared incident records per SOPs.
- AIG Shields: Tracked open vulnerabilities, supported remediation follow-up, forensic analysis and risk prioritization.
- PwC: Analyzed security incidents and prepared client-ready cybersecurity risk reports aligned to enterprise compliance frameworks.
- TCS: Supported user access reviews, verified access rights compliance, escalated unauthorized access attempts, maintained incident logs.

Projects

Multi-Agent AI SOC Automation System — Google x Kaggle AI Intensive **2026**

- Designed LLM-based multi-agent pipeline for SOC Level 1 alert triage, false positive reduction, and MITRE ATT&CK aligned threat classification.

Fake Profile Detection System **2026**

- Built end-to-end ML system using Logistic Regression, Random Forest, and XGBoost achieving 99% accuracy; deployed via Flask for real-time malicious account detection.

Technical Skills

SIEM & SOC: Microsoft Sentinel, Splunk, QRadar, Google Chronicle, SOAR
Security Tools: Defender XDR, Wazuh, VirusTotal, CrowdStrike (Basic), Wireshark, Nmap
Networking: TCP/IP, DNS, HTTP/HTTPS, Windows Event Logs, Firewall Monitoring
Security Operations: Incident Response, Alert Analysis, Threat Detection, Vulnerability Assessment
Compliance: SAMA CSF, NCA ECC, Access Reviews, Policy Compliance, Security Documentation
Programming: Python, Flask, SQL, HTML/CSS
Web Security: XSS, OWASP Top 10, Input Validation
Languages: English (Professional), Telugu (Native), Arabic (Basic — Actively Developing)

Certifications

CompTIA Security+ SY0-701 (2026, Score: 829) | **ISC2 Certified in Cybersecurity** (Scheduled July 2026) | **Certified Online Fraud Prevention Specialist** — Hack and Fix | Microsoft Sentinel | Google Chronicle SIEM | Cisco Cybersecurity | IBM Ai Cybersecurity | LetsDefend SOC Labs (20+ Badges)