Haris Ali.

Peshawar, Khyber Pakhtunkhwa • +923320071000 • harisalikhan1218@gmail.com •
linkedin.com/in/harisali-infosec • hariscyber.tech

ABOUT

Passionate and results-oriented Cybersecurity Analyst with 3+ years of hands-on experience in SIEM monitoring, IDS/IPS, firewall security, and security automation. Proven track record in identifying and mitigating threats, enhancing network defenses, and streamlining incident response. Known for improving operational efficiency and reducing false positives through smart automation. Continuously learning to stay ahead in the evolving cyber threat landscape.

WORK EXPERIENCE

Syntraq **04/2025 – Present**

Chief Executive Officer · Part-time **Remote**

- Cybersecurity Analyst
- Monitors, analyzes, and responds to security threats to protect systems, data, and networks from unauthorized access and cyberattacks.
- Network Security
- Implements and manages firewalls, intrusion detection systems, and encryption protocols to secure organizational networks against internal and external threats.
- Leadership

ECHO **04/2024 – 10/2024**

Cyber Security Analyst · Contractor **Peshawar, Pakistan**

- Conducted vulnerability scans and penetration testing across client networks.
- Strengthened firewall and intrusion detection systems, enhancing overall security.
- Reduced incident response time by automating log monitoring.
- Leadership

Shahid Ahmad & Co **01/2023 – 11/2023**

Security Analyst & IT Technician · **Contractor** **Remote**

- Spearheaded daily **cyber risk management** operations, ensuring adherence to industry regulations and cybersecurity best practices.
- Developed and deployed **advanced encryption protocols**, proactively identifying and mitigating system vulnerabilities.
- Led **continuous improvements** to organizational security frameworks, enhancing resilience against evolving cyber threats.
- Leadership

VIRTUAL TRAINING & INTERNSHIP EXPERIENCE

Cybersecurity Intern – Deloitte *(Remote | Apr – Jun 2025)*
Analyzed web activity logs for anomalies, supported simulated breach response, and investigated suspicious user activity.

Cybersecurity Intern – Commonwealth Bank *(Remote | Feb – Apr 2025)*
Built Splunk dashboards for fraud detection, responded to simulated incidents, and designed security awareness content.

Cybersecurity Student – J.P. Morgan *(Remote | May 2024)*
Gained hands-on exposure to cyber operations and digital forensics in a financial sector simulation.

Cybersecurity Intern – Datacom *(Remote | Feb – May 2024)*
Investigated simulated cyberattacks, conducted risk assessments, and developed mitigation strategies.

Cybersecurity Trainee – Tata Group (TCS) *(Remote | Jan – May 2024)*
Focused on IAM implementation and delivered reports aligning cybersecurity with business objectives.

Security Awareness Analyst – Mastercard *(Remote | Jan – May 2024)*
Reported phishing threats and helped develop targeted security training to improve user awareness.

Cybersecurity Student – Telstra *(Remote | Mar – Apr 2024)*
Participated in simulated incidents and enhanced understanding of enterprise security practices.

EDUCATION

Bachelor's degree of Science in Computer Science
City University of Science and Information Technology • GPA: 2.67 09/2018 – 01/2023

CERTIFICATIONS

Google IT Automation with Python Specialization
Google
CompTIA Security+ ce Certification
CompTIA
ISC2 Candidate
ISC2
Fortinet Certified Fundamentals Cybersecurity
Fortinet
Fortinet Network Security Expert Level 1: Certified Associate
Fortinet
Fortinet Network Security Expert Level 2: Certified Associate
Fortinet

PROJECTS

Network Intrusion Detection with Splunk
Set up Splunk with sample logs and used correlation searches to detect brute-force attacks, port scans, and DDoS activity. Built dashboards and documented findings in a detailed report.

Vulnerability Assessment with Nessus
Scanned test systems using Nessus Essentials to identify CVEs. Analyzed risk levels and compiled a security assessment report with remediation steps.

Web Application Penetration Testing
Used DVWA and Burp Suite to exploit OWASP Top 10 vulnerabilities (e.g., XSS, SQLi). Documented findings and provided mitigation recommendations.

Incident Response Simulation
Simulated phishing attacks and collected IoCs. Executed containment actions and wrote an incident report aligned with the NIST 800-61 framework.

Threat Hunting with ELK Stack
Deployed ELK Stack to analyze system logs. Created visualizations and queries to detect suspicious login attempts and abnormal activity.

SKILLS

- Analytical Skills
- Business Process Alignment
- Business Process Analysis
- Communication
- Creative Problem Solving
- Critical Thinking
- Digital/Open Source Investigations
- IAM Design
- Identify file types
- Network Traffic Analysis
- Open source investigation
- OSINT
- Project Planning
- Research Risk Assessment
- Secure Computing
- Security report writing
- Social Engineering concepts
- Solution Design Strategy Assessment
- Statistical Data Analysis
- Technical Security Awareness