HAFIZ ASIM SHAYAN KHAN

CYBERSECURITY ANALYST · NETWORK ADMINISTRATOR · CLOUD & AI SECURITY

Email: shahyankhan886@gmail.com Phone: +92 310 5945021 Location: Peshawar, Pakistan LinkedIn: /in/hafiz-asim-shayan-khan

PROFESSIONAL SUMMARY

CCNA-certified BS Computer Science graduate specialising in security operations, network engineering, and AI-driven security. Hands-on across the full attack–defend lifecycle: red-team reconnaissance and Active Directory attacks through to Wazuh-based threat detection, custom SOC rules, and active response. Experienced in cloud security across AWS and Azure, with applied AI/ML security research. Seeking roles in SOC analysis, penetration testing, threat detection, or network engineering.

EXPERIENCE

Network Administrator — Abasyn University

Jun 2026 – Present

BLUE TEAM · SOC · PESHAWAR, PAKISTAN

- Manage the university's network infrastructure — configuring and maintaining **switches and Wi-Fi access points**, monitoring performance, and troubleshooting connectivity issues across campus.
- Deployed the **Wazuh XDR platform** and write **custom detection rules** for threat detection and **active response** per the university's requirements, with proper documentation of every rule and workflow.
- Automate routine network and configuration tasks using **AI** for faster, consistent, and more efficient deployments.
- Triage alerts and correlate logs mapped to **MITRE ATT&CK**; configure VPN and access controls and provide day-to-day network & system support.

Red Team Intern — Cyberster

Mar 2026 – May 2026

OFFENSIVE SECURITY · REMOTE

- Ran end-to-end penetration tests across Linux, Windows, and **Active Directory** labs — passive OSINT to Domain-Admin compromise.
- OSINT and subdomain enumeration (Subfinder, Assetfinder, OWASP Amass) — **352 subdomains**, 21 live hosts validated with httpx & Gowitness.
- AD attacks: **AS-REP Roasting, Kerberoasting, LLMNR/NBT-NS poisoning, GPO ACL abuse** — reaching SYSTEM on domain controllers.
- Phishing with GoPhish and **Havoc C2**; AMSI bypass, LOLBAS, payload obfuscation; findings reported against CVSS and MITRE ATT&CK.

FEATURED PROJECTS & RESEARCH

ThreatFusion AI — CTI Fusion Pipeline
Defensive threat-intel pipeline: IOC extraction, MITRE ATT&CK mapping, risk scoring, knowledge graph, and STIX 2.1 export over 60 reports. Honest evaluation exposed a data-leakage artefact behind a 0.90 F1.

ThreatNet — AI-Assisted SOC Detector
Deep-learning detector classifying network flows into benign + 5 attack types (0.9994 macro-F1 on 30K flows); GRU host-log model extends coverage to Linux auth sessions.

Network Scanning & Asset Discovery
Python auditing tool: SYN stealth host discovery across CIDR subnets, port/service/version detection, and OS fingerprinting, producing clean inventory reports.

AWS Aurora Multi-AZ Failover
Dual-AZ VPC hosting Aurora MySQL 8.0 Multi-AZ cluster; validated zero-downtime failover with role promotion under 60 seconds.

QSVM vs Classical SVM (Final-Year Research)
Quantum vs classical SVM for email-spam detection; PCA for qubit constraints; probing AI reliability limits in threat detection.

HANDS-ON CLOUD & AI LABS

AWS Cloud Security: S3 resource-based & IAM policies · KMS encryption at rest (SSE-KMS, EBS) · CloudTrail + CloudWatch monitoring · automated remediation with AWS Config + Lambda.
Azure Security (AZ-500): Azure Firewall · Privileged Identity Management (PIM) · directory synchronization · securing ACR & AKS container workloads.
AWS ML — Amazon SageMaker: notebook instances · data ingestion & EDA · feature encoding · model training/deployment · performance metrics · hyperparameter tuning (airplane-delay prediction).
Azure AI — AI Foundry: generative-AI project setup · GPT-4.1 model deployment & testing · project/model endpoints · AI Foundry toolkit in VS Code.

TECHNICAL SKILLS

Offensive Security: Nmap, Metasploit, Burp Suite, BloodHound, Mimikatz, Subfinder, OWASP Amass, OSINT, Kerberoasting, AS-REP Roasting, Havoc C2, GoPhish, AMSI Bypass, LOLBAS, MITRE ATT&CK, CVSS
Defensive / SOC & SIEM: Wazuh XDR (custom rules, active response), Wireshark, Log Analysis, Alert Triage, Threat Detection, Incident Response, Cisco ASA
Networking: TCP/IP, OSI, Routing & Switching, VLANs, Inter-VLAN, NAT/PAT, DNS, DHCP, SNMP, IPSec VPN, IKE 1&2, Site-to-Site VPN, ACLs
Cloud & Containers: AWS (EC2, VPC, IAM, S3, RDS/Aurora, KMS, CloudTrail, CloudWatch, Config, Lambda), Azure (Firewall, Entra ID/PIM, ACR, AKS), Docker, Kubernetes
AI / Machine Learning: Python, Scikit-Learn, TensorFlow, Pandas, NumPy, Amazon SageMaker, Azure AI Foundry, GPT-4.1, Isolation Forest, SVM/QSVM, GRU, PCA
Systems & Tools: Kali Linux, Ubuntu, Windows Server, GNS3, Cisco Packet Tracer, VMware, VirtualBox, Hyper-V, Git, SSH, Java

LEADERSHIP & PROFESSIONAL SKILLS

Cyberster Ambassador (Current) — represent and advocate for Cyberster Security Academy, promoting its offensive-security training and supporting new red-teamers.
Class Representative (CR), Abasyn University (2022–2026) — elected cohort representative across the full four-year BS Computer Science program; liaison between students and faculty.
Professional skills: Leadership · Mentorship · Analytical Thinking · Technical Report Writing · Communication · Cross-Functional Collaboration · Problem-Solving · Adaptability · Ethics & Responsible AI · Continuous Learning.

CERTIFICATIONS & EDUCATION

CCNA — Cisco (2026)
AWS Solutions Architect – Associate (2026)
CCSP — Certified Cloud Security Professional (2025)
IT Security: Defence Against the Digital Dark Arts — Google (2025)
Python for Active Defence — Infosec (2025)
Detection & Incident Response — Google (2025)
Network Monitoring & Analysis — Google (2025)
System Administration & IT Infrastructure — Google (2025)
Foundations of Cybersecurity — Google (2025)
Cisco Network Administration — NAVTTC (2025)

Education: BS Computer Science — Abasyn University, Peshawar (2022–2026) · Concentration: Cybersecurity & Artificial Intelligence.