MUHAMMAD SHAHZAIB

SOC ANALYST — ENTRY LEVEL

Lahore, Pakistan | +92 327 9369066 | shahzaib.cybersec@gmail.com
linkedin.com/in/shahzaibcybersec | github.com/MuhammadShahzaib-umt

Available Immediately • Open to Remote / Onsite / Hybrid

PROFESSIONAL SUMMARY

BS Cyber Security undergraduate (University of Management and Technology) with a hands-on foundation in network security, real-time traffic monitoring, and anomaly detection, built through an independent, end-to-end rule-based firewall project. Google Cloud Cybersecurity Certificate holder (5 of 5 badges) covering security principles, risk management, and incident detection, response, and recovery. Comfortable working with logs, structured data (SQL), and scripting (Python, C++) to support alert triage and investigation. Fast learner who documents work clearly and follows through on independent projects end-to-end; seeking a Security Operations Center (SOC) Analyst role to monitor security events, triage alerts, and support incident detection and response within a security operations team.

CORE COMPETENCIES

Security Monitoring & Response: Real-Time Network Traffic Monitoring, Anomaly & Intrusion Detection, Security Alert Triage, Incident Detection, Response & Recovery, Threat Identification & Risk Management

Network & Firewall: Network Security Fundamentals, Rule-Based Firewall Configuration, Packet-Level Traffic Analysis, TCP/IP Concepts

Cloud Security: Google Cloud Security Fundamentals, Cloud Security Risk Management, Cloud Incident Response

Programming & Data: Python, C++, SQL & Relational Database Design, HTML, CSS, JavaScript

Security Practices: Security Documentation & Reporting, Vulnerability Awareness, Log-Driven Analysis, Applied AI Tools for Security Research (ChatGPT, Claude, Gemini)

Professional Attributes: Analytical Problem-Solving, Attention to Detail, Clear Technical Communication, Fast Learning & Adaptability, Self-Motivated

EXPERIENCE

AI & Machine Learning Internship — Big Brains Aug – Sep 2026

- Completed a remote Artificial Intelligence and Machine Learning internship, working through structured coursework and applied assignments covering core ML concepts and workflows.
- Graded across the program with a 97% average score; earned a verified Certificate of Completion (ID: BB-96172951899E).

PROJECTS

Custom Rule-Based Firewall & Real-Time Network Traffic Monitor | *C++*

- Engineered a firewall from the ground up, implementing rule-based packet filtering and real-time traffic monitoring to detect and flag anomalous, unauthorized connections — core SOC-style monitoring and threat-detection skills.
- Applied pattern-based anomaly detection and classification-style rule logic to live data streams, then tested and documented the system end-to-end, mirroring the alert-triage and investigation workflow used in security operations.

Hospital Database System | *SQL*

- Architected a normalized relational database to manage patient, doctor, and appointment records across 3 core entities, applying structured data modeling to protect data integrity and eliminate redundancy.
- Practiced security-conscious schema design and clean data preparation — directly transferable to log- and database-driven security monitoring.

Web Development Projects | *HTML, CSS, JavaScript*

- Independently designed, built, and published 2 browser games (Snake, Whack-a-Mole) and a personal portfolio site, owning the full development lifecycle solo — from concept to launch.

EDUCATION

BS in Cyber Security — University of Management and Technology (UMT), Lahore 2024 – Present

Secondary & Higher Secondary Education — India International School, UAE

CERTIFICATIONS

Google Cloud Cybersecurity Certificate — 5 of 5 badges completed:

- Security Principles in Cloud Computing
- Strategies for Cloud Security Risk Management
- Cloud Security Risks: Identify and Protect Against Threats
- Detect, Respond, and Recover from Cloud Cybersecurity Attacks
- Put It All Together: Prepare for a Cloud Security Analyst Job

Artificial Intelligence and Machine Learning — Big Brains, September 2026 (Certificate of Completion, 97% average score)

Claude 101 — Anthropic Education, June 2026 (LLM fundamentals & practical prompt engineering)

Claude Code 101 — Anthropic Education, July 2026 (AI-assisted development workflows)