SALAH UD DIN NASIR

SOC Analyst | Cybersecurity Researcher | IT & Network Support Engineer

Gujranwala, Punjab, Pakistan | (+92) 3107933283 | salahuddinnasirbutt@gmail.com

LinkedIn | GitHub

PROFESSIONAL SUMMARY

Analytical and technical Cybersecurity Researcher, SOC Analyst, and Systems Engineer with hands-on experience in **threat detection, network defense, enterprise IT support, and generative AI deception architectures**. Proven track record in designing low-latency threat-intelligence platforms, configuring enterprise SIEM/telemetry tools (Wazuh, Elasticsearch), and managing telecom transport operations. Possesses industry certifications from Cisco (CCST Cybersecurity), IBM, and TCM Security. Adept at bridging hardware/network troubleshooting with advanced threat research to secure enterprise infrastructures.

CORE COMPETENCIES & TECHNICAL SKILLS

- **SOC Operations & Threat Intelligence:** SIEM Logging & Monitoring (Wazuh, Elasticsearch), Indicator of Compromise (IOC) Extraction, MITRE ATT&CK Mapping, Threat Hunting, Vulnerability Assessment, Incident Response Protocols.
- **Networking & Infrastructure Support:** Enterprise Network Architecture, VLAN Segregation, Routing Protocols (OSPF, EIGRP), Telecommunications Transport Infrastructure, Hardware & Systems Troubleshooting, IT Help Desk Administration.
- **Security Engineering & AI Research:** Generative AI Deception Systems, Prompt Sanitization & Injection Defense, Containerization (Docker, Docker Compose), API Integration & Rate Limiting, Linux System Administration (Parrot OS, Ubuntu Server), Windows Server.
- **Programming & Systems:** C++, Python, Bash Scripting, REST APIs, Low-Level System Design, Data Structures & Algorithms, LaTeX Technical Publishing.

WORK EXPERIENCE

Transport Operations Internee

Pakistan Telecommunication Company Limited (PTCL) | *Gujranwala, Pakistan*

(18/02/2026 – 01/04/2026)

- **Network Infrastructure Maintenance:** Assist Transport Operations Managers in monitoring, maintaining, and troubleshooting regional telecommunication hubs and fiber transport infrastructure.

- **IT Support & Systems Diagnostics:** Provide Level-1/Level-2 hardware and network support, performing physical/logical diagnostics to ensure high operational uptime for regional nodes.
- **Security & Operations Protocols:** Adhere to enterprise technical support protocols, access control policies, and system escalation procedures across live production networks.

FEATURED CYBERSECURITY & RESEARCH PROJECTS

CyberNix Weaver Adaptive Generative AI Deception Platform *(Lead Architect)*

- **Architecture & Emulation:** Engineered a dynamic cybersecurity honeypot platform using Llama 3.3 and Groq LPU inference to simulate Linux/SSH command environments with sub-800ms execution latency.
- **Prompt Injection Defense:** Built a multi-stage middleware sanitization pipeline combining RegEx signature matching and semantic keyword inspection to neutralize LLM jailbreak attempts.
- **SIEM & Telemetry Pipeline:** Integrated real-time threat logging into Elasticsearch and Wazuh SIEM, mapping attacker keystrokes to MITRE ATT&CK tactics for automated SOC analysis.
- **Container Hardening:** Deployed edge listener sockets in isolated, read-only Docker containers to prevent container escapes and secure host infrastructure.

Enterprise Network Architecture & VLAN Security *(Cisco Packet Tracer)*

- **Network Segregation:** Designed and simulated a multi-building enterprise topology featuring inter-VLAN routing, redundant links, and strict Access Control Lists (ACLs).
- **Protocols & Hardening:** Configured dynamic routing, DHCP snooping, and Port Security rules to mitigate rogue device access and internal network spoofing attacks.

Tiny-CFG-Visualizer — Compiler-Level Security Analysis

- **Static Analysis:** Developed a lightweight C++ tool that parses subset code to generate Control Flow Graphs (CFG) via Graphviz (`.dot`).
- **Logic Auditing:** Designed for auditing binary logic bombs, infinite loops, and out-of-bounds execution paths prior to system compilation.

ACADEMIC PUBLICATIONS & RESEARCH

- **Design and Implementation of an Adaptive Generative AI Honeypot for Mitigating Static Fingerprinting**

  Co-Author | Submitted to Conference on AI & Cyber Frameworks (AICF / IEEE)

  Authored full architecture specifications, benchmark latency analyses, and deception efficacy studies for LLM-driven decoy systems.

- **QMS-Crypt: A Next Generation Framework for Quantum Resilient Architecture**

First Author / Lead Researcher | The Journal of Supercomputing (Springer Nature)

Designed a post-quantum security framework utilizing Quantum Support Vector Machines (QSVM) for advanced network anomaly detection.

- **The HALEM Model: A Computational Framework for Evaluating Adaptive Learning Ecosystems**

  Co-Author | SN Computer Science (Springer Nature)

  Developed computational evaluation pipelines for complex engagement and performance data analysis.

EDUCATION

Bachelor of Science in Computer Science (BSCS Honors)

University of Central Punjab | *Lahore, Pakistan*

(09/2022 – 08/2026)

CERTIFICATIONS

- **Cisco Certified Support Technician (CCST) — Cybersecurity** | *Cisco*
- **IBM Cybersecurity Fundamentals** | *IBM*
- **Practical Help Desk & IT Support** | *TCM Security*