

# ARBAZ KHAN

SOC Analyst L1 | IT Support | Information Security Fundamentals

Karachi, Pakistan | +92 331 2264940 | arbazakbarkhuwaja@gmail.com | [LinkedIn](#) | [GitHub](#)

## PROFESSIONAL SUMMARY

IT professional with a foundation in information security, networking, and endpoint monitoring, seeking to build a career as a SOC Analyst. Experienced in reviewing and responding to endpoint security alerts, investigating basic security incidents, and following structured escalation procedures in a live IT environment. Practiced in SIEM and intrusion detection concepts through hands-on home lab work with Wazuh and Suricata, alongside network and Active Directory attack awareness. Holds ISO/IEC 27001:2022 certification and CEH v13 training, with a strong interest in threat monitoring, log analysis, and security operations.

## CORE SKILLS

**Security Monitoring & Incident Response:** Endpoint alert review, threat isolation, basic incident investigation and escalation

**Networking Fundamentals:** TCP/IP, DNS, DHCP, VLAN, firewalls, network troubleshooting

**Operating Systems:** Windows 10/11, Windows Server, Linux (Debian, RedHat, Rocky, Ubuntu), macOS

**SIEM & Intrusion Detection (Lab):** Wazuh (log ingestion, alerting, event correlation), IDS/IPS, Zabbix, Grafana, Prometheus

**Security Awareness:** ISO/IEC 27001:2022 fundamentals, CEH v13 concepts, OWASP frameworks, basic vulnerability awareness

**Documentation & Communication:** Incident and support documentation, clear written communication, ticket handling

**Scripting :** Python, Bash

## PROFESSIONAL EXPERIENCE

**Sapphire Consulting Services** | Karachi, Pakistan

October 2025 – Present

**IT Support Executive**

- Administer endpoint security through BitDefender GravityZone EDR, reviewing alerts, performing threat isolation, and taking response actions on flagged endpoints.
- Provide L1–L2 technical support across Windows, Linux, and macOS endpoints, resolving hardware, software, and connectivity issues while documenting recurring problems.
- Manage DNS, DHCP, VLAN, and firewall rules to support stable network operations and resolve connectivity issues.
- Maintain clear documentation of support tickets, configurations, and procedures to support consistent IT operations.

**SignDevOps** | Remote — Florida, USA

September 2024 – May 2025

**Information Security Associate (Contract)**

- Audited production Linux web environments, networks, and server configurations to identify authentication flaws and access gaps prior to deployment.
- Evaluated application and infrastructure setups against OWASP frameworks and delivered remediation guidance aligned with ISO/IEC 27001 standards.

## TECHNICAL PROJECTS

- Built a home lab environment running Wazuh SIEM on Ubuntu for centralized log ingestion, real-time alerting, and event correlation.
- Configured Zabbix, Grafana, and Prometheus in a lab environment for infrastructure monitoring, dashboarding, and threshold-based alerting practice.
- Built a mixed enterprise network simulation with a Windows Server 2022 Domain Controller alongside Rocky Linux and Ubuntu servers to practice Active Directory administration and monitoring.
- Set up an isolated lab using EVE-NG to practice security fundamentals against OWASP Juice Shop, a simulated Active Directory environment, and Metasploitable.
- Practiced foundational security assessment concepts on TryHackMe and other learning platforms.

## ACADEMIC PROJECTS

- Automated Patch Management Tool** (Final Year Project) — Built a patch and update orchestration tool in Python for Windows and Linux endpoints, with a Django-based UI and PostgreSQL database.
- 7-Machine Network Topology** — Designed a networking project verifying connectivity using ICMP and capturing traffic with Ettercap.

## EDUCATION & CERTIFICATIONS

- Bachelor of Science in Computer Science (BSCS) — University of Sindh (Graduated: December 2025)
- Certified Ethical Hacker (CEH v13) Training — Corvit Lahore (Completed)
- ISO/IEC 27001:2022 Information Security Associate — SkillFront
- Google IT Support Professional Certificate — Google / Coursera