SAIF ULLAH

• +92-3146201244• Saifullah62012@gmail.com • LinkedIn:saifsocx

Education

University of the Punjab - Bachelor of Information Technology — Lahore,Pakistan 2022-2026

Professional Experience

SOC L1 @ DWP Group — Lahore,Pakistan 10/08/26 -Current

- Monitor and investigate security alerts from endpoints, firewalls, network devices, and business applications.
- Analyze logs and alert context to assess severity, identify false positives, and escalate incidents with supporting evidence.
- Develop and tune Wazuh detection rules, dashboards, and log integrations across the SOC environment.
- Connect Wazuh with n8n, OpenCTI, DFIR-IRIS, and Slack for alert enrichment, case creation, and notifications.
- Validate agent connectivity, log ingestion, and alert workflows to identify monitoring gaps.
- Document investigations and coordinate incident response with the SOC team.

Associate Security Engineer @ Ebryx Pvt. Ltd — Lahore,Pakistan 09/02/26 - 01/07/26

- Monitored and investigated endpoint, network, and cloud security alerts.
- Analyzed EDR/MDR alerts using CrowdStrike Falcon and VIPRE.
- Performed alert triage and log analysis using ELK Stack, Wazuh, and Microsoft Sentinel.
- Documented alert verdicts, investigation summaries, and case closure decisions.
- Coordinated escalations with L2/L3 analysts and completed the SOC training roadmap.

Security Engineer @ITFortress — Wellington,New Zealand 15/03/2025 - 27/06/2026

- Promoted from SOC Analyst to Security Engineer within six months.
- Designed, deployed, and managed Wazuh SIEM for multi-tenant SOC environments.
- Developed detections for file changes, SSH/RDP brute force, suspicious PowerShell activity, and web shells.
- Integrated Suricata, Snort, pfSense, Sophos, Sysmon, VirusTotal, and AbuseIPDB to expand security visibility.
- Automated alert enrichment and notifications using Shuffle, n8n, Slack, WhatsApp, and email.
- Created security dashboards, technical documentation, and client presentations.

SOC Analyst @ITSOLERA Pvt — Islamabad,Pakistan 16/06/25 - 09/08/26

- Monitored client security alerts and investigated suspicious endpoint and network activity.
- Performed alert triage, log analysis, incident documentation, and escalation.
- Deployed Wazuh and developed detection rules for phishing, anomalous activity, and network threats.
- Supported threat intelligence and incident response workflows for SOC operations.
- Led SOC interns and delivered practical Wazuh SOC training.

Wazuh Ambassador @Wazuh — California,US 12/01/26 - Current

- Represent the Wazuh community in Pakistan through technical content and practical SOC use cases.
- Share hands-on labs and guidance on Wazuh deployment, detection rules, and integrations.
- Promote open-source security monitoring practices within the cybersecurity community.

IT Support @Akhuwat — Lahore,Pakistan 26/07/25 - 30/08/25

- Supported day-to-day IT operations, user requests, and ticket resolution.
- Assisted with DHCP administration and network switch configuration.
- Integrated switch and firewall logs with Wazuh to support security monitoring.

Certifications

- Google: Professional Cybersecurity, AI Essentials, Technical Support, AI Seekho
- Cisco Networking Academy: Ethical Hacker, Junior Cybersecurity Analyst Career Path, Cyber Threat Management, Cybersecurity Essentials, Networking Basics, Introduction to Cybersecurity
- Microsoft Learn: Microsoft Sentinel, KQL, Defender for Endpoint, Defender XDR, Azure security, and AI security modules
- TryHackMe: Advent of Cyber 2024, Hackfinity Battle, Advent of Cyber 2025
- Udemy: Linux Security Basics
- DigiSkills: Freelancing, WordPress
- Forage: Cybersecurity Job Simulation

Projects

SOC Home Lab (SIEM-Based)

- Built a Wazuh-based SOC lab with Suricata, firewall logs, SOAR automation, Grafana dashboards, and multi-tenant access.

Cyber Defense System (FYP)

- Built a cyber defense system with a New Zealand-based company using Wazuh SIEM and SOAR.
- Developed 40+ use cases covering endpoint, network, cloud, AI, and LLM security, with threat intelligence and automated response.

Client Projects

- **Angola | Wazuh Branding:** Customized the login page, favicons, banners, report logos, dashboard titles, and overall Wazuh interface.
- **United States | AmaraTechIT Cloud SIEM:** Deployed Wazuh on AWS and configured BYOD onboarding, FIM, Microsoft 365 integration, multi-tenancy, custom branding, and domain access.

Additional

Technical Skills:

- SIEM & cloud: Wazuh, ELK Stack, Microsoft Sentinel, AWS, Azure
- EDR & security monitoring: CrowdStrike Falcon, VIPRE, Sysmon, Microsoft Defender, Wireshark
- Automation & case management: n8n, Shuffle, DFIR-IRIS, TheHive
- Network & threat intelligence: Suricata, Snort, pfSense, Sophos, VirusTotal, AbuseIPDB, MISP
- Other: Detection engineering, incident investigation, technical documentation

Languages:

- English, Urdu, Saraiki, Punjabi