Muhammad Talal Ahmed

SOC Analyst

mail@ta1al.com | Pakistan | ta1al.com | Ta1al

CompTIA **Security+** certified Computer Science graduate with hands-on experience deploying and monitoring Wazuh, integrating pfSense and endpoint logs, investigating security alerts, and automating high-severity notifications. Skilled in alert triage, IOC analysis, incident documentation, Windows and Linux systems, TCP/IP networking, and network traffic analysis. Seeking an L1 SOC Analyst role where I can contribute to security monitoring, incident investigation, and continuous improvement of SOC operations.

TECHNICAL SKILLS

Security Operations
- SIEM: Wazuh, ELK Stack, Splunk
- Security Monitoring and Alert Triage
- Log Analysis and Event Correlation
- IOC Analysis and Threat Intelligence
- Incident Documentation and Reporting
- Incident Response Fundamentals

Systems and Network Security
- Windows and Linux
- TCP/IP, VLANs and Network Segmentation
- pfSense Firewall Configuration and Log Monitoring
- Wireshark and Network Traffic Analysis
- IDS/IPS Concepts
- Burp Suite

Programming & Scripting
- Python (automation, alerting scripts)
- JavaScript / TypeScript
- C++

PROFESSIONAL EXPERIENCE

SOC Analyst Intern 01/2026 – 04/2026
ITSOLERA PVT LTD
- Deployed and configured Wazuh SIEM with pfSense and endpoint log integration for centralized security monitoring.
- Reviewed firewall and endpoint alerts, analyzed supporting logs, and investigated suspicious activity.
- Built a Python and n8n workflow to forward high-severity security alerts for faster review.
- Documented deployment procedures, investigation findings, and recommended security improvements

IT Intern 07/2025 – 09/2025
Jauharabad Sugar Mills Pvt Ltd
- Provided end-user support for Windows, hardware and network-connectivity issues, communicating identified problems and next steps clearly.
- Diagnosed issues affecting OLT, CCTV and switching infrastructure and escalated detailed technical findings to senior IT staff.
- Assisted with troubleshooting VLAN, routing and access-control configurations in a production environment.

PROJECTS

Alert Automation with Wazuh and n8n 01/2026
at ITSOLERA PVT LTD
- Built automated SOC alerting pipeline using Wazuh, Python, n8n, and Discord API
- Enabled real-time forwarding of high-severity security alerts for faster response

pfSense Firewall Security Monitoring 02/2026
at ITSOLERA PVT LTD
- Configured pfSense firewall rules and network segmentation policies
- Integrated firewall logs into Wazuh using rsyslog for centralized monitoring
- Analyzed blocked traffic and intrusion attempts via SIEM dashboard

TryHackMe - SOC L1 Capstone 07/2025
- Investigated full attack chain using ELK, Kibana, and Wireshark
- Analyzed PowerShell, macros, and LNK-based attack artifacts
- Reconstructed attacker lifecycle including lateral movement and persistence

EDUCATION

BS Computer Science 2022 – 2026
Sargodha University
CGPA: 3.8 (Bronze Medal)
- Relevant Coursework: Software Engineering, Web Development, Database Systems, Computer Networks, Network Security and Information Security
- **President, Programming Society:** Led student teams, coordinated workshops and competitions, mentored junior members and communicated with faculty stakeholders.

CERTIFICATIONS & TRAININGS

CompTIA Security+
Passed July 2026

IBM Operating Systems Administration

Google Cybersecurity Professional

Google Tech Support Fundamentals

National Skills Competency Test
Rank 65 Nationwide | Top 0.2%