SHAIK NIYAZUDDIN

SOC Analyst | Security Operations & Incident Response

+91-77995-85022 | niyazuddinshaik5484@gmail.com | https://www.linkedin.com/in/shaik-niyazuddin/ | Andhra Pradesh, India

PROFESSIONAL SUMMARY

SOC Analyst with hands-on experience in security monitoring, incident response, and threat detection in a simulated SOC environment using SIEM/XDR platforms. Skilled in log correlation, alert triage, and incident investigation across Linux and Windows systems. Familiar with developing basic detection rules and documenting security incidents aligned with the MITRE ATT&CK framework and SOC best practices.

TECHNICAL SKILLS

- **Security Operations:** Log Monitoring, Incident Triage, Alert Analysis, Threat Detection
- **SIEM/XDR:** Wazuh, ELK Stack
- **Operating Systems:** Linux (Ubuntu, Kali), Windows
- **Networking:** TCP/IP, Ports & Protocols, Firewalls, Traffic Analysis
- **Frameworks:** MITRE ATT&CK (alert mapping), NIST
- **Security Assessment Exposure:** Nmap, OWASP Top10, OWASP ZAP
- **Scripting:** Python (log parsing), Bash (basic)

PROJECT EXPERIENCE

Independent Security Operations Experience – Simulated Enterprise SOC Environment

- Designed and maintained a multi-machine SOC lab to continuously practice security monitoring and incident response.
- Configured and managed Wazuh SIEM to collect, correlate, and analyse endpoint security logs.
- Monitored authentication, system, and security events to identify suspicious activities.
- Developed and tested detection rules for brute-force attempts, privilege escalation, and port scanning.
- Performed alert triage, root cause analysis, and incident classification following SOC workflows.
- Documented incidents, findings, and response actions to improve detection accuracy and analysis skills.

Security Assessment Experience– Simulated Enterprise Environment

- Performed basic vulnerability assessment activities in a simulated enterprise lab environment.
- Conducted reconnaissance and service enumeration using Nmap to identify exposed services.
- Identified common web application vulnerabilities aligned with OWASP Top 10.
- Documented findings to understand attack impact and remediation approaches.

ADDITIONAL SKILLS

- Strong analytical and problem-solving skills
- Understanding of SOC workflows and escalation processes
- Clear documentation and reporting abilities

EDUCATION

B.Sc. – MPC | 2014 - 2017

ANU/Annabattuni Satyanarayana Degree and PG College, Tenali (68%)

CERTIFICATION

Cyber Security training program – Frontlines EduTech Private Limited

June 2025 – January 2026

LANGUAGES

Telugu, English, Hindi