T LITHEESH KUMAR

SOC Analyst | Security Operations & Incident Response

9705263197 | chinnakumarr1930@gmail.com | https://www.linkedin.com/in/litheesh-kumar/ |
Andhra Pradesh, India

PROFESSIONAL SUMMARY

SOC Analyst (Entry-Level) 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

- **SIEM/XDR Platforms**: Wazuh, ELK Stack
- **Security Operations**: Log Analysis, Alert Triage, Incident Response, Threat Detection
- **Security Frameworks**: MITRE ATT&CK (TTP Mapping), NIST Cybersecurity Framework, Cyber Kill Chain
- **Network Security**: TCP/IP, Wireshark, Firewalls, IDS/IPS Concepts, Traffic Analysis
- **Operating Systems**: Linux (Ubuntu, Kali), Windows (Server/Desktop)
- **Vulnerability Assessment**: Nmap, OWASP Top 10, OWASP ZAP
- **Scripting & Automation**: Python (log parsing, automation), 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. Tech – Mechanical Engineering | 2018 – 2024

JNTUA/Mother Theresa Institute of Engineering and Technology, Palamaner (62%)

CERTIFICATION

Ai Powered Cyber Security – FrontLines Edu Tech

June 2025 – January 2026

LANGUAGES

Telugu, Hindi, English