HASSAN ZANNOON

Bangalore, India | 80899 39738 | hassanzannoon@gmail.com
LinkedIn: linkedin.com/in/hassanzannoon

PROFILE SUMMARY

Entry-level SOC Analyst with hands-on practice in SIEM tools, log analysis, network traffic monitoring, and basic incident investigation. Strong understanding of cybersecurity fundamentals and SOC workflows. Quick learner with good analytical skills and eager to contribute to security monitoring and threat detection.

CORE SKILLS

SIEM: Wazuh, Splunk (basic), QRadar (basic)
Network: Wireshark, Nmap, tcpdump
Security: Log Analysis, Alert Triage, Threat Identification, Incident Response (beginner)
Systems: Windows, Linux (Ubuntu/Kali – beginner)
Other: Documentation, Problem Solving, Basic Python/Bash

PROJECT EXPERIENCE

SIEM Log Monitoring & Investigation — Wazuh
- Set up Wazuh SIEM and onboarded Windows/Linux endpoints for monitoring.
- Analyzed authentication logs, system events, and security alerts.
- Investigated simulated brute-force attempts using log correlation.
- Created an incident summary report with findings.

Network Traffic Analysis — Wireshark
- Captured and analyzed packets using tcpdump and Wireshark.
- Identified unusual DNS requests and repeated connection patterns.
- Documented findings with screenshots and explanations.

Security Event Analysis — Splunk / QRadar
- Practiced SIEM searches, dashboards, and alert triage.
- Performed event filtering, analysis, and reporting.

Vulnerability Assessment — Nessus
- Conducted host scanning and reviewed vulnerability findings.
- Provided simple remediation recommendations.

CERTIFICATIONS

• Certified Ethical Hacker (CEH) — EC-Council
• Certified Cyber Security Analyst (CICSA) — EC-Council

EDUCATION

Bachelor of Computer Applications (BCA)
P.A First Grade College, Mangalore University — 2024

STRENGTHS

Attention to Detail • Analytical Thinking • Adaptability • Communication • Teamwork

AVAILABILITY

Immediate – Open to SOC Analyst (L1) / Cybersecurity Analyst roles