

ABISHEK N.S

CYBER SECURITY ENGINEER & SOC ANSLYST

+91-7200822497

abishek22ns@gmail.com

Thuckalay, Tamil Nadu, Imdia -629175

OBJECTIVE:

Innovative and detail-oriented Mechanical Engineer with a strong analytical background and a keen interest in cybersecurity with Redteam Hacker Academy Certified Security Professional training, possessing the ability to solve problems, perform business risk analysis, examine breaches, and recommend corrective actions. Well-versed in security fundamentals, incident response, threat detection, vulnerability assessment, and penetration testing. Seeking to leverage engineering problem-solving skills and technical knowledge in a dynamic SOC Analyst role to contribute to the protection and security of an organization's digital assets.

KEY COMPETENCIES

Certifications:

CompTIA Security+ (2024)
Certified Ethical Hacker (CEH)
(2024)
Python beginner

Technical Skills:

Network protocols Linux and
Windows administration Scripting
languages: Python, Java
TCP/ IP, DNS, HTTPS
SIEM, EDR, OpenVAS, PSI-DSS

Strategic Thinking

Ability to develop and execute
strategic business plans.
Knowledge of industry trends and
market dynamics.
Experience in identifying growth
opportunities and driving
innovation.

PROFESSIONAL EXPERIENCE

Euro tech Oil and Gas LLC- Dubai Executive Assistant

2022- 2023

Oversee day-to-day operations to ensure efficiency and productivity. Monitor financial performance and ensure profitability. Communicate the company's vision, strategy, and performance. Effective communication and negotiation skills.

Sree krishna Automobile private Ltd.

2017-2019

Supervisor

Develop and maintain production schedules to meet deadlines and customer demands. Ensure that products and documentation. Coordinate with other departments such as engineering, maintenance, and quality assurance to resolve production issues.

EDUCATION & CERTIFICATIONS

Diploma in Mechanical Engineering

Sun Polytechnic College

Certified SOC Analyst

EC - Council

INTERESTS

- Investigating real-time threat intelligence and analysis for incident response.
- Enhancing SIEM tools through custom rule development and log correlation.
- Studying malware behavior and reverse engineering for proactive defenses.
- Implementing innovative solutions using machine learning in anomaly detection.
- Participating in CTF (Capture the Flag) events to strengthen incident-handling skills.
- Designing proactive defenses against emerging threats like ransomware and APTs (Advanced Persistent Threats).
- Implementing innovative solutions using machine learning in anomaly detection.