

BHAVYA NIDIMAMIDI

+91 8125323218 ◊ nidimamidibhavya@gmail.com ◊ <https://www.linkedin.com/in/nidimamidi-bhavya-4224a628a>

PROFESSIONAL SUMMARY

Detail-oriented and motivated Security Operation Center Analyst with hands-on experience in threat monitoring, incident response, and security operations. Proficient in Security Information Event Management tools like Splunk and Wazuh, with strong knowledge of network security, log analysis, and malware detection. Possess a proactive mindset, analytical thinking, and a continuous learning approach in a fast-paced cybersecurity environment.

EDUCATION

Bachelor of Technology in Computer Science and Engineering Parul Institute of Engineering and Technology, Vadodara. CGPA : 7.4	2021-2025
Higher Secondary Education , Class XII Narayana College, Anantapur, 95%	2020-2021
Secondary School Certificate , Class X Lakshmi English Medium High School, Anantapur, 98.8%	2018-2019

TECHNICAL SKILLS

Security Operations: Incident Response, Threat Hunting, Security Monitoring, Malware Analysis.

SIEM and Tools: Splunk, Wazuh, Seceon, Wireshark.

Endpoint and Network Security: IDS/IPS, Firewalls, Endpoint Protection, TCP/IP, Network Protocol Analysis.

Log Analysis: Correlation, Alert Tuning, Anomaly Detection.

Operating Systems: Windows, Linux (Ubuntu/Kali)

Others: Vulnerability Management, MITRE ATTACK Framework.

EXPERIENCE

Security Operation Center Analyst Intern 12/2024-Present
TechDefenceLabs Solutions Limited.

- Monitored and analyzed SIEM alerts and logs to detect potential security threats.
- Investigated security incidents including phishing, malware, and unauthorized access.
- Contributed to tuning and optimizing SIEM rules for better threat detection.
- Demonstrated strong problem-solving abilities and collaboration in dynamic incident response teams.

PROJECTS

Network Intrusion Detection System Using Advanced Machine Learning Algorithms (Academic Group Project)

- A Network Intrusion Detection System using machine learning algorithms is a security system designed to monitor, analyze for malicious activity and policy violations.
- It leverages machine learning techniques to enhance the detection of abnormal behavior by identifying patterns and network protocols.

Pentest On ColdBox

- Conduct a penetration test on the coldbox to identify the root privileges and flags to address security potential vulnerabilities.
- Documented vulnerabilities and recommended remediations in a structured report.

CERTIFICATIONS

- Q1 2025 Innovation Certification Days– Seceon
- VAPT - Quick Heal Academy
- Ethical Hacking Essentials- EC Council
- Network Defense Essentials - EC Council
- Network Essentials - Cisco Network Academy

SOFT SKILLS

- Analytical Thinking
- Problem Solving
- Attention to Detail
- Communication Skills
- Team Collaboration