KANASANI NAVEEN

✉ naveenkanasani96@gmail.com ☎ 9398579064 Hyderabad https://www.linkedin.com/in/kanasani-naveen

OBJECTIVE:

Entry-level cybersecurity professional with hands-on SOC and VAPT experience, skilled in monitoring, alert analysis, and incident response, seeking to contribute to proactive threat detection and mitigation.

EDUCATION:

B. TECH: CSE IN CYBER SECURITY:	**2021-2025**
MALLA REDDY UNIVERSITY, HYDERABAD	88 %
INTERMEDIATE:	**2019-2021**
SRI CHAITANYA JUNIOR COLLEGE, KHAMMAM	96%
SSC:	**2018 - 2019**
TALENT ENGLISH MEDIUM SCHOOL, SATHUPALLY	88%

TECHNICAL SKILLS:

- **Security Tools & Platforms**: Splunk, (SIEM – log monitoring, alert triage), Wireshark, Nmap.
- **SOC Operations:** Alert monitoring & response, escalation procedures, incident response lifecycle, report generation.
- **Vulnerability Management & VAPT:** CVE/CVSS scoring, scanning tools, remediation planning.
- **Networking & Infrastructure Security**: TCP/IP, DNS, DHCP,VPN, firewalls, IDS/IPS concepts, OSI model,
- **Malware Awareness:** Knowledge of common attack vectors, malware types, and basic malware analysis.
- **Operating Systems:** Windows & Linux system administration, command-line operations.

WORK EXPERIENCE:

Cybersecurity Intern | Slash Mark IT Solutions (OPC) Pvt Ltd |

- Assisted in configuring and testing security tools for network and application protection.
- Gained practical exposure to threat monitoring, log analysis, and SOC operations.
- Worked on security concepts including Ethical Hacking, Linux Security, and Incident Handling.

Cybersecurity Intern | Supraja Technologies

- Performed SOC alert monitoring, log analysis, and escalation in simulated & live environments
- Executed VAPT on 10+ web applications, uncovering and remediated critical vulnerabilities to enhance security posture
- Utilized Burp Suite, Nmap, and Wireshark for proactive defense analysis.

PROJECTS:

Web Fort Security - Innovating Cyber Defense for the Modern Web

- Developed a secure and scalable backend framework to strengthen application defense.
- Enhanced data flow efficiency and optimized server response times for better performance.
- Improved system resilience through streamlined architecture and security best practices.

AnomaliScan - See Threats Before They Strike

- Processed and labeled mixed benign–malicious traffic datasets for threat detection.
- Applied feature engineering to improve anomaly detection accuracy.
- Delivered real-time threat visualizations, enabling SOC teams to respond faster.

CERTIFICATES:

- Google Cybersecurity Professional Certificate – Includes modules on cloud security and data protection
- IBM Penetration Testing & Incident Response – Applied Python scripting and analysis
- Google IT Support Professional Certificate – Covered networking, APIs, and cloud basics
- Introduction to Networking – Cisco NetAcad – Fundamentals of network and data communication
- Palo Alto Networks Cybersecurity Foundation – Exposure to threat detection using data-driven methods