# PAVANI GOVINDA

SOC Analyst

+91 9618073210 Hanamkonda https://www.linkedin.com/in/pavani-govinda-291b9625b govindapavani2000@gmail.com

## PROFESSIONAL SUMMARY

Dynamic and dedicated SOC Analyst with over two years of experience in cybersecurity operations. Specialized in threat detection, incident response, and proactive threat mitigation. Committed to enhancing security, staying updated on industry trends, and safeguarding organizational assets. Proficient in leveraging advanced SIEM tools, conducting vulnerability assessments, and performing log analysis. Skilled in vigilant monitoring and rapid incident response to ensure a secure cyber environment.

## SKILLS

- Threat Management: Log Analysis, Incidence Response, Threat Hunting, End point detection and response
- Testing Expertise: Vulnerability assessment, WAPT, advanced Phishing Simulations
- Security Frameworks: Proficient in using MITRE ATTACK , SIEM Platforms
- Platform Proficiency: Extensive experience with Linux and windows environments

## PROFESSIONAL EXPERIENCE

**SOC Analayst** **WYDUR | 2022-PRESENT**

- Monitor network traffic, system logs, and security alerts using advanced SIEM tools to identify potential security incidents and anomalies.
- Analyze logs, monitor network devices, review SIEM rules and alerts, and develop incident response actions to ensure prompt detection and mitigation of security threats.
- Proficient in utilizing Sophos EDR for log monitoring and analysis, with hands-on experience using helpdesk services for incident response ticketing
- Deep Investigations and prioritize incidents based on the severity to minimize downtime and mitigate critical Vulnerabilities
- Detect anomalies behaviour and policy violations using the Mitre attack framework to enhance threat intelligence efforts
- Investigate Phishing attempts, malware infections and suspicious activities using tools
- Perform a network vulnerability assessment scan, making generated reports available to customers
- Author detailed incidence response(IR) Reports for high impact events, outlining root causes and implementing remediation strategies to prevent recurrence
- Deliver 24/7 security monitoring and support to ensure seamless threat detection during critical operations
- Generate detailed reports on threat patterns and operational metrics, contributing to executive decision making process
- Collaborate with multidisciplinary teams to refine incidence response playbooks, improving operational efficiency

## TOOLS & TECHNOLOGIES

- SIEM: Seceon, Splunk
- Endpoint Security : Sophos EDR/XDR, DLP
- Vulnerabilty Assessments: Tenable Nessus Expert, GVM OpenVAS
- Web Application Testing: Burpsuite profesional, OWASP ZAP.
- Threat Analysis: Virus Total, IPVoid, URLScan.io, AbuseIPDB, browserling
- Additional Tools: Metasploit, Aircrack-ng, Wireshark, SEToolKit, Nmap, MXToolbox, Waybackmachine

## CERTIFICATIONS

Sophos:

- Sophos Central Endpoint and Server v4.0-Engineer
- Sophos Central Endpoint and Server
- Sophos Firewall v19.5- ENGINEER

Seceon: AISIEM Profesional Certificate

Certifications from Fortinet:

- NSE 1 Network Security Associate

Certifications from Codered:

- Ethical Hacking Essentials (EHS)
- Network Defense Essentials (NDE)
- Digital Forensics Essentials (DFE)

## EDUCATION

- **Kakatiya University**

  Master Of Computer Applications
- **Kakatiya Mahila Degree College**

  Bachelor Of Science

## LANGUAGES

- **English**
- **Telugu**