SOLLETI VASAVA SANJEETH

✉ vasavasanjeeth@gmail.com ☎ +91 94911 60802 Tuni, Andhra Pradesh github.com/sanjeeth-solleti

in/vasava-sanjeeth-solleti

PROFESSIONAL SUMMARY

Entry-level Cybersecurity Analyst with hands-on experience in SOC operations, SIEM monitoring, vulnerability assessment, and digital forensics through internships and enterprise-grade simulations. Proven ability to evaluate high-volume security alerts, identify threats, and deliver actionable remediation aligned with OWASP Top 10 and SOC workflows. CEH-certified professional with strong analytical, documentation, and incident response skills.

EXPERIENCE

Cyber Forensics Specialist with SOCMINT Intern, *Cyber Privilege* 08/2025 – 11/2025 | Remote

- Performed digital forensic investigations on compromised systems while maintaining evidence integrity using MD5, SHA-1, SHA-256, and SHA-512.
- Executed SOCMINT and OSINT investigations to trace threat actors and validate digital artifacts.
- Maintained ISO 9001:2015-compliant forensic documentation and case reports.

Cybersecurity Specialist Intern, *Future Interns* 06/2025 – 07/2025 | Remote

- Conducted web and network vulnerability assessments using OWASP ZAP, Burp Suite, and SQLMap, identifying 15+ medium-to-critical vulnerabilities.
- Monitored and triaged 100+ SIEM alerts using Splunk and ELK, classifying phishing, brute-force, and malware activities.
- Produced remediation reports mapped to OWASP Top 10, supporting risk reduction and security posture improvement.

Cybersecurity Job Simulations - SOC & IAM, *Forage* 06/2025 – 07/2025 | Remote

- **Deloitte Australia:** Inspected 100+ server logs to detect automated scraping across API endpoints and recommended WAF rules that reduced attack surface.
- **Mastercard:** Investigated phishing campaigns affecting 5+ users, identifying 8 threat indicators that informed security training and reduced click-through rates by 45%.
- **Commonwealth Bank:** Built 5 Splunk dashboards processing 100+ transactions to detect fraud patterns, reducing detection time significantly.
- **TCS:** Documented IAM workflows for 20+ accounts and implemented RBAC policies that identified and remediated privilege escalation risks.

PROJECTS

AI-Powered Security Automation Tool

- Built an intelligent platform that automates Level 1 SOC analyst tasks, reducing alert fatigue.
- Configured Wazuh SIEM ingestion with ML-based alert classification and enrichment.
- Automated Jira ticket creation for high-severity incidents to accelerate response.

Automated Threat Intelligence Engine

- Deployed a modular platform to automate IOC extraction, enrichment, and AI-assisted threat analysis using Flask APIs.
- Integrated multiple threat intelligence services to classify alerts and generate actionable security reports.
- Implemented a scalable React-Flask architecture enabling real-time analysis and faster incident response.

SKILLS

Programming Languages: Python

Tools & Platforms: Splunk, Wazuh, CrowdStrike, ELK, Burp Suite, Nmap, SQLMap, Metasploit, Wireshark, Nessus, NetSparker

SOC & Security: SIEM Monitoring, Incident Triage, Threat Detection, Log Analysis, Vulnerability Assessment, Digital Forensics, OSINT

CERTIFICATIONS

Certified Ethical Hacker (CEH V13) — EC-Council

Google Cybersecurity Professional — Coursera

SOC Level 1 — TryHackMe

EDUCATION

Chalapathi Institute of Engineering and Technology, 10/2022 – 03/2026 | Lam, Guntur
B.Tech in Computer Science and Engineering (Cybersecurity)
GPA: 8.45/10