

SNEHA.N.SATYARADDI

Security Analyst



+91 6361958896



snehasatyaraddi@gmail.com

SUMMARY

- Solid understanding of common network services and protocols.
- Good knowledge on cyberattacks and attack vectors.
- Working level knowledge on security solutions like Antivirus, Firewall, IPS, Email Gateway, Proxy, IAM, TI, VA Scanners, WAF etc.
- Basic knowledge on skills like Malware Analysis, Threat Hunting.
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs, client meetings, report walk throughs etc.
- Keeping updated with the latest developments in the cyber security landscape.

SOC ANALYST SKILL SET

- Deep dive analysis of triggered alerts using SIEM, SOAR and other analysis tools
- Acknowledging and closing false positives and raising tickets for validated incidents
- Assist IRT/SME teams in incident remediation by providing supporting data and recommendations
- Follow-up with incident response team for remediation
- Monitoring and troubleshooting Silent Log Sources
- Research, compile and organize monthly vulnerability reports
- Participate in weekly SOC meetings to discuss about raised incidents.
- Drafting shift hand-overs

TOOLS & TECHNOLOGIES

SIEM : Splunk

VA Scanner: Nessus

Malware Sandbox: Any. Run

Case Management: Cortex
XSOAR

EDR: Microsoft 365 Defender

OSINT Tools: Virus Total,
IPVoid, IBM XForce

Ticketing Tool: Service Now

CERTIFICATIONS

- ABCs of Malware Analysis
- SPLUNK fundamentals
- SOC Experts Certified Security Analyst
- Cortex SOAR Introduction

EDUCATION

Bachelor of Computer Application,
JSS Shri Manjunatheshwar
Institute of UG and PG
Studies, Dharwad 2025