

Chennuri Sai Deepthi

📞 +91-8008728020

✉ saideepthi.ch15@gmail.com

🌐 LinkedIn Profile

SUMMARY

A SOC L1 Analyst with a comprehensive understanding of cybersecurity principles, specializing in threat detection, incident response, and network monitoring. Proficient in utilizing SIEM tools, analyzing suspicious events, conducting log analysis, and correlating security events to identify potential threats. Skilled in investigating security incidents, performing deep dive analysis, and implementing remediation measures. Capable of effectively communicating with cross-functional teams and providing actionable insights to enhance the security posture of the organization.

PROFESSIONAL EXPERIENCE

• Associate Software Engineer

Tech Mahindra

June 2023-Present

– **Role:** SOC Analyst

– **Responsibilities**

- Working in Security Operation Centre (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts
- Conducted regular health checks to ensure system integrity and performance optimization.
- Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis.
- Analyzed and investigated security incidents, identifying indicators of compromise (IOCs) and potential security breaches.
- Conducted in-depth analysis of security events to determine the scope and impact of incidents, prioritizing response actions accordingly.
- Collaborated with cross-functional teams to share insights, and enhance detection capabilities.
- Participated in the Incident Response (IR) process and supported actionable incidents
- Responded promptly to security incidents, containing and mitigating threats to minimize impact and restore normal operations.
- Triaged security incidents based on their severity and priority, ensuring that critical incidents receive immediate attention.
- Monitoring IOC (Indicators of compromise).
- Working on assign ticket queue and understanding and exceeding expectations on all tasked SLA commitments.
- Escalating issues to L2 and management when necessary
- Making weekly, monthly reports and submitting to the team lead.
- Working on assign ticket queue and understanding and exceeding expectations on all tasked SLA commitments.
- Document all actions taken during incident investigations.
- Take follow ups and closing of the tickets based on client response.

TECHNICAL SKILLS

- **SIEM Tools:** IBM Qradar
- **Endpoint :** Trend micro
- **Scanning Tool:** Nmap
- **Incident Response:** Incident detection, analysis, containment, eradication, and recovery
- **Operating Systems:** Windows, Linux/Unix
- **Ticketing Tool:** Jira
- **Networking:** TCP/IP, DNS, DHCP, VPN, VLANs, routing and switching
- Phishing Email analysis
- **Programming:** Python, SQL

EDUCATION

• Bachelor of Technology in Computer Science

2018-22

Aurora's Technological and Research Institute, Hyderabad

CGPA: 7.03

CERTIFICATIONS

- Certified SOC Analyst (CSA) (EC council)
- Qradar Security information and event management (siem) from IBM
- SC200 certification by Microsoft
- Certified in Cyber security under Microsoft DSCI Project CyberShiksha conducted by RightWorkz Technology
- Endpoint Detection and Response certification issued by Qualys