HEMANTH MELAM

☎: +91-8341229771 HTTPS://WWW.LINKEDIN.COM/IN/HEMANTH-MELAM/ ✉:HEMANTH3247@GMAIL.COM

Associate Engineer- SOC

Innovative and results-oriented Cyber Security Analyst with 3+ years of experience in Investigating, analyzing security incidents, and providing suitable counter measures. Combines technical skills with strong analytical and problem-solving abilities. Quick learner in mastering new systems and functions to be a high-impact contributor.

SUMMARY OF QUALIFICATIONS

- Do real time log analysis from different network devices e.g., Firewalls, IDS, IPS, Operating Systems, Proxy Servers, Linux Servers, Active Directory Servers, System Applications, Databases, Web Servers etc.
- Performs Real time log monitoring, Security incident handling, investigation, escalation of security incidents with recommendations to mitigate the threat
- Track the security investigations to resolution. Recognize cyber-attacks based on their signatures and if the alert is Suspicious then raise the Ticket, otherwise close the Alert.
- Integrate and share information with the related teams as appropriate with the documentations or reports. Assist customers with security related issues.
- Handling ADHOC request and Preparing Daily, Weekly, Monthly and Quarterly Reports for customers.
- Worked with wide range of customer from Medical, Insurance, Real- Estate Firm and, food tech management and Banking and Financial background.
- Researching the latest information security trends to understand the latest vulnerabilities and threads.
- Responding to clients ad hoc request which varies from deeper investigation for a given incident to proving
- Log searches for an audit purposes.
- Performing threat analysis using 3rd party tool like virus total, abuseipdb and hybrid analysis etc.
- Internal SIEM admin tasks-monitoring Log Stoppage, whitelisting, and health check
- Knowledge on basic security, SIEM for logs monitoring and analysis and networking concepts.
- Good understanding of different types of firewalls, proxies, Antivirus.
- Basic knowledge on CrowdStrike, SentinelOne, Symantec EDR.

TECHNICAL SKILLS /TOOLS

1. SOC (Security operation center)
2. Incident response/handling
3. AISAAC MDRTM
4. Arcsight
5. Service now Ticketing tool
6. Microsoft 365 Defender
7. Azure Active directory
8. security incident management and response
9. Dark trace
10. EDR Tool – SentinelOne XDR ,SYMANTEC,Crowdstrike

CERTIFICATIONS

- NSE 1 Network Security Associate
- Testing Applications for CompTIAPenTest+ from pluralsight
- Conducting Passive Reconnaissancefor CompTIA PenTest+
- Information Gathering and VulnerabilityIdentification for CompTIA PenTest
- Conducting Active Reconnaissance for CompTIA PenTest+

PROFESSIONAL EXPERIENCE

ATOS GLOBAL IT SOLUTIONS – Bangalore
Associate Engineer –SOC | Sep 2021- FEB 2025

Role : Associate Engineer
Sep 2021- SEP 2024

Worked as an Associate Engineer in an MSSP SOC project, handling a wide range of customers across various industries, including Medical, Insurance, Real Estate, Food Tech Management, and Banking & Financial sectors.

Role : Incident Handler
Project: SBI LIFE | Sep 2024- Feb 2025

Responsibilities:

- Daily Collaboration with multiple vendors teams to resolve the Logstoppages with in SLA.
- Log searches for an audit purposes.
- Handling adhoc request and Preparing Daily, Weekly, Monthly and Quarterly Reports for customers.
- Sharing threat intelligence (ioc) to the customer teams.
- Collaborating with cross-functional teams to identify deinducted and newly inducted devices, and documented their status for accurate tracking and reporting
- Supported the implementation team in device onboarding and use case simulation, ensuring seamless integration and optimal performance
- Supporting soc team to reduce the false positives and automation of the alerts and improving response efficiency by collaborating with customer teams and different vendor teams.
- Appreciated by customers for reducing overall security operations budget by 5-10% through efficient resource allocation and process optimization.
- Supported the implementation team in identifying and onboarding 20% of new devices, enhancing SOC visibility and threat detection capabilities.

- Reduced incident response time by 20% through efficient log analysis and collaboration with cross-functional teams.

EDUCATION

Bachelor of Technology – Computer Science

Kallam Haranadhareddy Institute of Technology, JNTU Kakinada, India
2015-2019