SARITHA M.

SOC ANALYST

Email:sarithachowdhary27@gmail.com|Mobile: 8919033514|Location: Hyderabad.

Career Objective:

To improve myself as a competent and committed professional in an organization in the field of security which gives me the opportunity and scope to apply my skills and knowledge and contribute to the success of organization and achieve personal growth along with professional growth.

Profile Summery:

- Good Knowledge in SOC (Security Operations Centre) Operations methodology such as Incident Handling, Threat detection, Network traffic monitoring, real time security event handling, log analysis, identifying and classifying attempted compromises to networks through heuristics identification of suspect traffic.
- Experience in device configuration for various devices and applications including Firewalls, IDS, IPS, Windows servers, Linux servers, Database servers and other applications as per the custom requirements and Analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks).

Working Knowledge:

- Monitoring and analysis of events generated by various security and network tools like firewalls, proxy servers, av, ips/ids, load balancer's database, system application, cloud (amazon, azure and google) windows and Linux servers etc. working as security analyst for SOC 24*7 environment.
- Security incident response: responsible for monitoring of security alerts. Analysis of logs generated by appliances, investigation, and assessment on whether the incident is false positive or false negative.
- Use SIEM tool (azure sentinel) to detect possible signs of security breaches and perform detailed investigation to confirm successful breach. Perform root cause analysis (RCA) and approprimately handle the incident as per defined incident management framework.
- Following end to end incident investigation and incident response process phishing & email security , ensuring to close the investigation within defined SLA escalation of security incidents to concerned teams and their management and follow-up for closure.
- Creating tickets in service now and tracking the status of the incidents.
- Analysis of daily and monthly reports for incident management and compliance. Coordinating with network team, server team regarding activities and technical issues.
- Creating vulnerability and remedy reports and reporting them to users. Finding the critical servers and application inventory from respective business owners and scheduling the scan weekly, monthly and quarterly basis.
- Knowledge sharing session with the team members whenever complex incident issues are raised and also lessons learned from other team members.
- Scanning the environment using Nessus tool and finding the vulnerabilities based on the business units and sending the report to respective business owners. Attending calls with business owners, windows and Linux team for scheduling the vulnerability management patching and remediation part without business disruption.

Technical Skills:

Course Complete: Cyber Security.

- Knowledge on Different types of Cyber Attacks, Cyber Kill Chain Process, MITRE ATTACK.
- Knowledge on OSI and TCP/IP Layers and Ports and Protocols.
- Knowledge on SIEM, EDR, FIREWALL, IDS, IPS, and PROXY.
- Knowledge on Vulnerability Management and Reporting.
- Knowledge on Incident Life Cycle Management (ITIL) and SDLC**.**
- Knowledge on DLP(Data Loss Prevention)Tool.

Ability Work in Tools:

- SIEM – Azure sentinel ,Splunk
- EDR- MS Defender
- VMDR – Nessus
- Network Security- Firewall, IDS/IPS, Proxy
- Email Security –MDATP
- Ticketing Tool - Service Now, Jira

Education:

- **Master of Computer Applications(MCA),** From Vaagdevi College of Enginering since 2021 to 2023.

Languages:

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

Declaration:

I hereby declare that the information furnished above is true to the best of my knowledge and correct."

Saritha M.
Hyderabad