SRIDHAR V

Security Analyst (SOC)

sridharvachar@gmail.com
Ph No : 7975069288
Bengaluru

SUMMARY

Dedicated and result driven **SOC ANALYST with 3 years of hand on experience in cyber security operations**. Good understanding on common network services and protocols. Familiarity with Cyber-attacks, Cyber Kill Chain, Mitre attack framework, malware and phishing analysis. Working knowledge on security solutions like Anti-virus, Firewall, IPS, IDS, Proxy and EDR etc. Meticulous, detailed-oriented and able to thrive in fast paced environments.

Actively looking for **SOC ANALYST** role to provide a situational awareness using combination of technology to properly identify, analyse, investigate, communicate, respond and report cyber security incidents.

TOOLS AND TECHNOLOGIES

- SIEM Tools: **IBM QRADAR**
- Firewall: **PALO ALTO**
- Email analysis: **MS 365 DEFENDER, MX TOOL BOX**
- Threat Intelligence: **URL SCAN, VIRUS TOTAL**
- Malware analysis: **ANY.RUN (Sand box)**
- TICKETING TOOL: **JIRA**
- EDR : **SENTINELONE**

TECHNICAL SKILL

- knowledge on servers like **DHCP, DNS, PROXY SERVER, ACTIVE DIRECTORY etc**
- knowledge on **MALWARE** and Different types of attacks such as **DDOS, DNS POISONING, PHISHING AND MITM.**
- Good knowledge of security concepts **(CIA TRAID, CYBER KILL CHAIN)**
- Good understanding of **OSI MODEL, IP ADRESSES AND CLASS OF IP ADRESSES**

ACADAMIC QUALIFICATION

Bachelor of Engineering
(ECE) at SJMIT - 2020
Chitradurga

ROLES AND RESPONSIBILITIES:

- Monitoring and analyzing the logs, triggered alerts 24/7 and raise tickets for validated incidents by following run book.
- Collection of necessary logs that could help in the incident containment and security investigation.
- Triage security events and incidents, detect anomalies and report remediation actions.
- Recognize and investigate intrusion attempts differentiate false Positives from true intrusion attempts.
- Escalate validated and confirmed incidents by raising tickets which includes all information about the offenses
- Analysis of phishing emails reported by internal end users and finding the legitimacy of emails using different tools and technology like MX tool box and so on.
- Conducting basic malware analysis on suspicious files detected on end points.
- Maintaining proper sop's and processes.
- Regularly checking mails and taking follow up in a timely manner.
- Assist in incident remediation.
- Attending weekly meeting on ticket review.
- Draft shift handover.

WORK EXPERIENCE:

Company **: SANEMI TECHNOLOGIES PVT LTD**
Date **: From 2021 to NOV 2024**
Designation **: Security Analyst (SOC) L1**

DECLARATION

I hereby declare the information furnished above is true to the best of my knowledge.