Mahesh Babu Pentapati

SOC Analyst

maheshbabu.soc7@gmail.com +91 7670866926

CAREER OBJECTIVE

SOC Analyst with **2 years** of hands-on experience in identifying and mitigating security threats. Seeking a challenging role in a dynamic organization where I can leverage my expertise in threat detection, incident response, and security best practices to enhance the cyber security posture. Committed to continuous learning and professional growth to stay at the forefront of evolving security challenges and technologies while contributing to the organization's security goals.

PROFILE SUMMARY

- **2 years of** hands-on IT Experience in securing the network environment Experience in Information Security with emphasis on security operations, incident management, intrusion detection, and security event analysis using SIEM tool Splunk, Qradar and Azure Sentinel
- Experience in Monitoring & Investigating the incoming
- Events Experience of working in 24x7 operations of the SOC team, offering log monitoring, security information management, and global threat monitoring.
- Experience in generating Daily, Weekly & Monthly Reports
- Experience on performing log analysis analyzing the crucial alerts at immediate basis through SIEM
- Handling critical alerts from Symantec Endpoint Protection and working for resolution.
- Handling alerts from Crowd strike EDR and investigation.
- Responsible for triage of a variety of alerts stemming from Malware
- Responsible for monitoring the Phishing attempts.
- Exposure to Ticketing tool like Service Now.
- Strong knowledge on Incident management life cycle.
- Good communication, problem solving skills and the ability to acquire new skills in a timely manner.
- Strong in team coordination and managing tasks.

PROFESSIONAL EXPERIENCE

Mastercard (SOC Analyst)
09/2022 – present - **pune**

- Having **2 Years** of Monitoring the incoming security alerts in Splunk & Qradar
- Working in Offshore SOC team. Monitoring of SOC events, detecting and preventing the Intrusion
- attempts.
- Ad hoc report for various event sources customized reports and scheduled reports as per
- requirements.
  Collecting the logs of all the network devices and analyses the logs to find the suspicious activities.
- Investigate the security logs, mitigation strategies and Responsible for preparing generic security
- incident report
- Handling Alerts from multiple Security Log sources such as Proxy, Anti-Virus and EDR
- Deep dive Investigation through Falcon EDR
- Monitoring, analysing and responding to infrastructure threats and vulnerabilities.
  Phishing and Spam Email Analysis
-

Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.

Responsible to preparing the root cause analysis reports based on the analysis.

- Analyzing daily, weekly and monthly reports.
- Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
- Website Anti-Malware and Defacement monitoring and real-time alerting based on anomalies detected.
- Analyzing daily, weekly and monthly reports.
- Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Investigating the events based on particular criteria by creating an Active Channel.
- Handling the failed logins issues from the different systems.
- Handling the different issues like Phishing, Spam and Malicious email.
- Using Service now to handle & track al kind of incidents.
- Working on security related threats and Incidents.
- Coordinates with all the teams to Mitigate/Remediate the issue.
- 24/7 rotational shifts.

SKILLS

- Security Operation Center **(SOC)**
- **SIEM Tool:** Qradar, Azure sentinel, Splunk,
- **End point security:** Symantec & Trend Micro.
- **Ticketing Tool:** Service Now,Jira
- **Vulnerability Management:** Nessus & Qualys
- **DLP, Crowd Strike,CarbonBlack**
- **Trend Micro,IDS,IPS**
- **Email Security:** Proof point & Symantec

EDUCATION

B.TECH from Kakinada Institute Of Engineering & Technology, Korangi in **2022.**

DECLARATION

I hereby declare that the above-mentioned details are true to the best of my knowledge.

(Mahesh babu pentapati)