Mahesh Babu Pentapati.

Security Analyst L1

Pune MH | maheshbabu.soc7@gmail.com | 7670866926

CAREER OBJECTIVE :

Result-oriented professional with experience Information technology and proven knowledge of Information security. Aiming to leverage my skills to successfully fill the **Information Security Analyst** role at your company

---

SUMMARY :

Overall 2.5 years of IT experience with information security and currently working as **Information Security Analyst** with SOC. Hands on experience on security monitoring, analysis and ticketing tools.

SKILLS :

- SOC(Security Operation Center)
- Phishing Email Analysis.
- Monitoring and reporting .
- DLP & Guardium
- Ticketing Tools (*Service Now*).
- SIEM (*Qradar, Splunk*).
- Malware analysis (*VT, Wireshark*).
- Endpoint Detection and Response. (*Crowdstrike, Microsoft Defender*).
- Preparing security advisories.

EXPERIENCE :

Mastercard| Pune | Sep 2022 – Present.

- Working in **SOC** (24x7), monitoring SOC events, detecting and preventing **intrusion** attempts.
- Hands on experience on **Threat Analysis**, **Security Monitoring** and Operation.
- Experience on **SIEM** (Security Information and Event Management) tools and Monitoring real-time events using **Qradar and Splunk**.
- Generating tickets on ticketing tools (**Service Now**) and taking the necessary followup.
- Hands on experience on EDR tools (Crowdstrike, Microsoft Defender, Fortinet).
- Performing in depth **Malware analysis** using multiple tools.
- Hands on work experience on Symmantec DLP and Guardium.
- Investigating and creating case for the Security Threats, Threat analysis and forwarding it to Onsite SOC team for **further investigation** and **action**.
- Experience on performing log analysis, malware analysis, DLP and analyzing the critical alerts at immediate basis and Recognizing attacks based on their **signatures**.
- Experience and knowledge in investigating incidents, remediation, tracking and follow-up for incident closure with concerned team.
- Technical knowledge on security tools (**Anti-virus/malware, IDS/ISP, Firewalls, proxies, vulnerability**, etc) and infrastructure (**Network, OS, Database**)

TechOwl Infosec — SOC Analyst

06/2025 – Present | Surat, Gujarat

- Responsible for end-to-end SOC operations and incident response.

- Worked on FortiSIEM for custom correlation rule creation, parser optimization, and log normalization.
- Integrated FortiSOAR for automated alert enrichment and ticketing workflows.
- Handled firewall log monitoring, alert triage, and threat containment.
- Developed detection rules for SQLi, XSS, DNS anomalies, and Powers-hell-based attacks.
- Supported onboarding of multiple BFSI clients with tailored SIEM content and dashboards.

Responsibilities :

- Working in Security Operation Centre (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts Responding to various security alerts, incidents for various clients.
- Responding to various security alerts, incidents for various clients.
- Monitoring real-time events using **SIEM** tools like **IBM Qradar, Splunk.**
- Microsoft Azure Sentinel threat collection, detection, response, and investigation efforts.
- Microsoft defender malware protection, web protection, real-time security notifications, and security tips.
- Crowd strike falcon protect endpoints and workloads from cyber threats.
- Configured and managed security tools including User and Entity Behaviour Analytics (UEBA) with Securonix, Data Loss Prevention (DLP) solutions, and Zscaler.
- Performed independent assignments such as RIN installations, system upgrades, and DLP policy configurations to enhance security posture
- Created, maintained, and updated detailed design documents, diagrams, and Standard Operating Procedures (SOPs) to ensure clarity and consistency in security operations.
- Monitoring, analysing and responding to infrastructure threats and **vulnerabilities**.
- Collecting the logs of all the network devices and analyse the logs to find the suspicious activities.
- Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
- Analysing daily, weekly and monthly reports
- Monitoring **24x7** for Security Alerts and targeted **phishing** sites by using **SIEM** tool.
- Analysing daily, weekly and monthly reports.
- Creating the tickets in ticketing tool.
- Actively collaborated with fellow team members, contractors, and vendors on bridge calls to prevent or resolve incidents, ensuring effective communication and rapid issue resolution
- Create, maintain and update documentation of detailed design documents, Sop's, for client requirement.
- Having Good communication skills, both verbal and written, with the ability to express complex.

EDUCATION :

- Graduate in **B.Tech –Mechanical Engineering - KIET –2022 - JNTUK -7.15 CGPA**.
- Diploma – Mechanical Engineering –KIET -2019 -65%
- SSC from Surya High School – 2015.

INTERESTS :

Reading | Movies

Place:

Mahesh Babu Pentapati