KARTHIK MOHARE P R

SOC ANALYST

karthickmohare20@gmail.com +91-9380650330

Davanagere, Karnataka

linkedin.com/in/karthick-mohare-8a4070331

OBJECTIVE

To build my career as a successful security analyst in a major global organization, where I can best utilize my skills to accomplish the organization's goals and objectives, at the same time get an opportunity to expand my knowledge.

SOC ANALYST SKILL

- Good Knowledge on Security alerts generated by SIEM.
- Knowledge on creating Reports, Dashboards and Alert.
- Analyzing SIEM alerts by following runbooks and using various tools.
- Well verse knowledge on generating tickets for validating incidents.
- Well known knowledge about malware like Virus, Trojans, Worms, Ransomware, Botnets etc..

INTERNSHIP

- Cybersecurity fundamentals: Basics of networking, cryptography, and security protocols.
- Vulnerability assessment: Identifying weaknesses in systems and networks.
- Security tools: Familiarity with SIEM, IDS/IPS, and antivirus software.
- Incident response: Ability to analyze and respond to security incidents.
- Risk management: Understanding risk assessment and mitigation strategies.

CERTIFICATIONS

- Intro to splunk (eLearning)
- Foundations of operationalizing MITRE ATT&CK
- Soc fundamentals course

LANGUAGES

- English
- Hindi
- Kannada

EDUCATION

STJIT College ,Private college , Ranebennur

• Bachelor of engineering in **information science** (2021- 2024)

• CGPA-**6.5**

SKILLS SUMMARY

- Good Understanding of **OSI Model, IP addresses and Classes of IP Address, 3-way Handshake.**
- Well Knowledge on **DNS, DHCP, ARP, IPS, IDS, Proxy server, Active Directory etc.**
- Having good knowledge on **Cyber kill chain** and its phases.
- Good Knowledge of security concepts like **CIA triad, MITRE-ATTACK.**
- Understanding on common networking services like **Web, Mail, FTP.**
- Understanding of concepts like **Encryption, Decryption, Hashing.**
- Familiar with different types of attacks like **DOS/DDOS, Crosssite scripting, SQL injection, Phishing** and **Bruteforce** attacks.
- Good knowledge on IP ports and protocols well known about components of **SIEM and Architecture of SPLUNK**.
- Solid understanding of architecture of IBM Qradar.
- Knowledge on network & security concepts.
- Knowledge on security solutions like **Antivirus, Firewall, IPS, WAF,..etc.**
- Knowledge on analyzing the malicious IP address, URL, by using open- source Threat Intel tools (like Virus-total, IP-Void, URL Void).

TOOLS EXPOSURE

- **SIEM:** SPLUNK ES, IBM QRADAR.
- **FIREWALL**: PALO-ALTO
- **EDR:** CISCO AMP
- **VULNERABILITY:** NESSUS
- **ESA:** MS 365 DEFENDER
- **TICKETING TOOL:** JIRA

AREA OF INTEREST

- Alert Analysis
- Threat Intelligence
- Malware Analysis
- Vulnerability Management
- Phishing Analysis
- Network Security
- End Point Security