KARTHIK PRADEEP C

+91 8606717326
Karthikpradeep006@gmail.com
Kerala, India
https://www.linkedin.com/in/
karthikpradeep-c-b 164a423a/

PROFILE SUMMARY

Motivated and detail-oriented SOC Analyst with hands-on experience in threat detec- tion, incident response, and security monitoring. Skilled in using advanced security tools like XDR to identify and mitigate cyber threats. Adept at conducting root cause analysis, producing detailed security reports, and implementing security protocols. Strong ability to work collaboratively within teams and adept to fast-paced, dynamic environments. Seeking to leverage expertise in cybersecurity to contribute to organi- zational security initiatives and enhance overall threat protection.

WORK EXPERIENCE

SECURITY OPERATION CENTER ANALYST (SOC) - 2024 TO PRESENT
MACOM SOLUTIONS, THRISSUR

- Conducted deep-dive analysis of triggered alerts using the XDR tool
- Monitored network traffic and security events, identifying and responding to potential threats in real-time.
- Utilized SIEM tools to analyze security logs and correlate events to detect, assess, and mitigate cyber threats.
- Investigated security incidents and escalated issues to senior security person- nel when necessary for further analysis and resolution.
- Performed vulnerability assessments and recommended appropriate actions to strengthen the organization's security posture.
- Assisted in the development and implementation of incident response proto- cols and procedures to ensure quick and effective mitigation of threats.
- Maintained and updated security documentation, ensuring compliance with internal policies and regulatory requirements.
- Worked closely with cross-functional teams to provide security support and resolve security-related incidents in a timely manner.
- Continuously stayed updated on emerging cyber threats and vulnerabilities, ensuring the security of organizational assets.

INTERNSHIP

SOC ANALYST TRAINEE - 2023 - REMOTE
CHAITANYA CYBER STRIX TECHNOLOGIES PVT LTD, HYDERABAD

- Assisted in monitoring security events and incidents, identifying potential threats using various security tools and platforms.
- Conducted initial triage of security alerts, providing detailed analysis and escalating issues to senior analysts for further investigation.
- Collaborated with the team to develop and implement security protocols, learning best practices for incident response and threat management.

ACADEMIC PROJECT

- A Cyber Security Methodology for a Cyber Industrial Control System Testbed Code

- Information with Aggregate Key Cryptosystem

EDUCATION

- **M.SC CYBER FORENSICS (MG UNIVERSITY) 2020-2022**
  School of Technology and Applied Science, Pathanamthitta

- **B.SC CYBER FORENSICS (MG UNIVERSITY) 2017-2020**
  School of Technology and Applied Science, Pathanamthitta

CERTIFICATION

- CERTIFIED PENETRATION TESTER (RED TEAM HACKER ACADEMY)
- CERTIFIED ETHICAL HACKER(CEH) V13 (EC COUNCIL)

TECHNICAL SKILLS

- IDS/IPS
- Security Event Management
- Endpoint Detection andResponse (EDR)
- MDR Tool
- XDR Tool (Stellar Cyber)
- Seqrite
- Threat Analysis
- Malware Analysis
- Kali Linux
- Vulnerability management
- SIEM Tool (Splunk)Microsoft
- Defender XDR
- Excel
- SentinelOne

SKILLS

- Communication
- Problem-Solving
- Team Collaboration
- Time Management
- Adaptability
- Critical Thinking
- Conflict Resolution
- Leadership
- Emotional Intelligence

LANGUAGES

- English
- Malayalam
- Tamil
- Hindi