K PREMA TEJA

CYBER SECURITY ANALYST

CONTACT

+91 9440703172
premateja.karangula@gmail.com

EXPERIENCE

Network Engineer Intern
Pi Data Centers, Vijayawada
May 2024 - Present

It Recruiter
Elabs Infotech, Hyderabad
March 2023 - August 2023

SKILLS

- IBM Qradar, Splunk
- Fortigate & Paloalto Firewall
- Email Gateway
- IDS/IPS
- Vulnerability Management
- Nessus
- Service Now
- Cyber Kill Chain & MITRE Framework
- OSI, TCP/IP Layers, Ports & Protocols, OWASP Top 10 Attacks
- Java Full Stack

EDUCATION

B. Tech (CSE)
Sai Spurthi Institute Of Technology
June 2018 - July 2022

SUMMARY

- As Security Analyst for SOC 24*7 environment . Monitoring and analysis of events generated by various security and network tools like Firewalls, Proxy servers, AV, IPS/IDS, load balancer's, database , System Application etc.
- Solid understanding of common network services and protocols.
- Good knowledge on cyberattacks and attack vectors.
- Working level knowledge on security solutions like Antivirus, Firewall, IPS,IDS, Email Gateway, Proxy, IAM, Threat Intelligence, VA Scanners, WAF etc.
- Exposure to using frameworks and compliances like MITRE ATT&CK. CIS Critical Controls, OWASP, ISO 27001 etc.
- Drafting shift hand-overs.

SOC ANALYST SKILLS

- Deep dive analysis of triggered alerts using SIEM, SOAR and other analysis tools.
- Acknowledging and closing false positives and raising tickets for validated incidents.
- Follow-up with incident response team for remediation.
- Following end to end Incident Investigation and Incident Response process, ensuring to close the investigation within defined SLA.
- Research, compile and organize monthly vulnerability reports.
- Participate in weekly SOC meetings to discuss about raised incidents.
- Involved in creating phishing awareness campaign.
- Knowledge on Incident Investigations like Malware, Phishing Email, and Ransomware.
- Track threat actors and associated tactics, techniques, and procedures (TTPs).
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs, client meetings, report walk throughs, bridge calls, RFPs, etc.
- Keeping updated with the latest developments in the cyber security landscape.

CERTIFICATION

- Certification Completed on Cyber Security by Codetech IT Solutions.
- Certification Completed on Networking by Microsoft.