Meghana S Gopal

Address: Mundanthanathu, Othera East PO, Thiruvalla, 689546

Contact Number: 9387753400

Mail ID: meghanasgopal@gmail.com

Profile

Experienced SOC Analyst with a strong background in analyzing security alerts, conducting incident response, and mitigating cyber threats. Skilled in monitoring network traffic, identifying potential security breaches, and implementing security measures to protect sensitive information. Adept at working in fast-paced environments and collaborating with cross-functional teams to ensure the security and integrity of systems and data. Strong analytical and problem-solving skills with a passion for staying up-to-date on the latest cybersecurity trends.

Experience

SOC ANALYST | ADAPTIVE CYBER LABS, TRIVANDRUM | APRIL 2022- PRESENT

- Conducted daily monitoring and analysis of security events and incidents to identify potential threats and vulnerabilities
- Collaborated with cross-functional teams to investigate and respond to security incidents in a timely manner
- Security usecase creation, testing and implementation.
- Rule creation and Dashboard creation for Security monitoring.
- Reduced false alarms by fine-tuning intrusion detection system configurations based on historical analysis of incidents.
- Trained junior analysts in threat intelligence gathering techniques, improving overall team efficiency.
- Monitoring of client instance and alerts
- Preparation of reports for alerts triggered in the instance
- Served as an escalation point for difficult problems and complex enquiries
- Analyses all the attacks and come up with remedial attack analysis
- Conduct detailed analysis of incidents and create reports and dashboards
- Monitor for attacks, intrusions and unusual, unauthorized or illegal activity
- Maintained accurate documentation of all SOC activities, facilitating knowledge sharing across the organization.

SOC ANALYST INTERN | ADAPTIVE CYBER LABS, TRIVANDRUM | SEPTEMBER 2021-MARCH 2022

- Prepare Reports based on events analyzed
- Research and Implementation of Splunk in VM
- Researched on various cyber attacks
- Acknowledge, analyse and validate incidents received through other reporting mechanisms such as email, phone calls, management directions, etc
- Collection of necessary logs that could help in the incident containment and security investigation

- Escalate validated and confirmed incidents to SOC Analyst
- Undertake first stages of false positive and false negative analysis.

Education

PROVIDENCE COLLEGE OF ENGINERRING | MARCH 2020 | CHENGANNUR

- Electronics and Communication
- CGPA -7.9

Skills & Abilities

- Wireshark
- NMAP
- Vulnerability Research
- Network Traffic analysis
- Log Analysis
- Splunk
- Incident Response
- Cyberthreat Analysis
- SIEM
- Incident Management
- TCP-IP
- ISO/OSI
- DNS
- DHCP