# Synoptics Technologies Limited

**Job Profile – SOC Manager**

| | |
|---|---|
| **Position** | **SOC Manager** |
| **Reports to** | **Cyber Security Practice Head** |
| **Experience** | **8-12 Years** |
| **Location** | **Mumbai** |
| **Job Overview** | An experienced Security Operations Center (SOC) Manager with over 10 years of expertise in managing and optimizing security operational services. This role requires deep knowledge and hands-on experience with unified threat management, anti-virus solutions, Security Information and Event Management (SIEM), Distributed Denial of Service (DDoS) / Denial of Service (DoS) mitigation, threat and vulnerability management, cyber investigations, and cyber security forensic investigations. |
| **Responsibilities** | • **Leadership and Management:** Lead and manage the SOC team, ensuring efficient and effective operations. Develop and implement SOC strategies, policies, and procedures. Coordinate with other departments to align security operations with organizational goals. Mentor and train SOC staff, fostering professional growth and development.<br>• **Threat Management:** Oversee the implementation and management of unified threat management systems. Ensure effective deployment and maintenance of anti-virus and anti-malware solutions. Monitor and respond to security threats and incidents in real-time.<br>• **SIEM and Log Management:** Manage the deployment, configuration, and maintenance of SIEM solutions. Ensure effective log collection, correlation, and analysis to identify potential security incidents. Develop and maintain security use cases and correlation rules within the SIEM.<br>• **Incident Response:** Lead the SOC team in responding to security incidents, including DDoS/DoS attacks. Coordinate with relevant stakeholders during incident response and recovery. Conduct post-incident analysis and reporting to prevent future occurrences.<br>• **Threat and Vulnerability Management:** Oversee regular vulnerability assessments and penetration testing. Ensure timely patch management and remediation of identified vulnerabilities. Develop and implement threat intelligence programs to stay ahead of emerging threats.<br>• **Cyber Investigations:** Conduct cyber investigations to identify the root cause of security incidents. Gather and analyze digital evidence for forensic investigations. Prepare detailed investigation reports and present findings to senior management.<br>• **Continuous Improvement:** Regularly review and enhance SOC processes and technologies. Stay updated with the latest security trends, tools, and best |

| | |
|---|---|
| | practices. Conduct regular SOC performance assessments and implement improvements. |
| **Requirements** | • Bachelor's degree in Cybersecurity, Information Technology, or a related field.<br>• Over 10 years of experience in cybersecurity, with a focus on security operations.<br>• Expertise in unified threat management, anti-virus solutions, SIEM, DDoS/DoS mitigation, threat and vulnerability management, cyber investigations, and forensic investigations.<br>• Strong leadership and team management skills.<br>• Excellent problem-solving and analytical abilities.<br>• Certifications such as CISSP, CISM, CEH, GIAC, or equivalent are highly desirable.<br>• Strong communication skills, with the ability to convey complex technical concepts to non-technical stakeholders. |