SOC Manager / Lead - Information Security - MP - 26/06	
Post Code	MP - 26/06
Qualification	BE/B.Tech/MCA, CISSP, CISM, Certified Incident Handler (CIA), Certified SOC analyst (CSA), Experience with SIEM and EDR/XDR platform
Experience	Minimum 8+ years of experience in Cybersecurity, with 3+ years in SOC/Security Operations leadership
Remuneration	Commensurate with qualification & experience and comparable with the best in the industry.
Employment Type	On Contract
Job Location	The position will be based at either GIFT City, Gandhinagar/ GNFC Infotower, Ahmedabad. However, depending on the organizational requirements, the employee may be transferred or posted to any other office location of the Company.
Role Overview	We are looking for an experienced professional can look after Overall SOC operations, SOC strategy, governance, SLA, escalation, Management & Reporting
Key Responsibilities	> Manage day-to-day SOC operations and security monitoring. > Establish and maintain SOC processes, SOPs, playbooks, and escalation procedures. > Ensure effective L1/L2/L3 alert triage and investigation. > Define and monitor SOC SLAs, KPIs, and KRIs. > Oversee monitoring of SIEM, EDR/XDR, firewall, IDS/IPS, WAF, DLP, IAM, cloud and other security platforms. > Develop and continuously improve security monitoring use cases. > Review detection rules and reduce false positives. > Ensure appropriate log sources, log retention, correlation, and monitoring coverage. > Lead investigation and response to critical and high-severity security incidents. > Establish incident classification, severity, escalation and communication mechanisms. > Coordinate containment, eradication and recovery activities with IT and business teams. > Ensure post-incident reviews and root-cause analysis, lesson learned are incorporated into SOC controls and detection mechanisms. > Oversee the use of threat intelligence to enhance detection capabilities. > Monitor emerging threats, vulnerabilities, IOCs and relevant TTPs > Oversee SOC platforms including: SIEM, EDR/XDR, SOAR, Vulnerability Management, Threat Intelligence, Network Security Monitoring, Email Security, DLP > Evaluate and recommend new security technologies where required. > Ensure effective integration and automation between security tools > Ensure SOC activities align with organizational security policies and risk requirements. > Support ISO 27001, SOC 2, DPDP Act and other applicable regulatory/compliance requirements, as relevant. > Maintain appropriate evidence, logs, incident records and audit trails. > Support internal and external security audits. > Prepare periodic SOC dashboards and management reports.

	> Report significant incidents and security risks to the CISO/management > Track metrics such as: Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Alert volume, False-positive rate, Incident severity, SLA compliance, Detection coverage, Open/high-risk incidents
Interested candidates may fill-up the application form online through mentioned link as well as upload the detailed resume latest by 14/09/2026	