SOC Operation Analyst - Information Security - MP - 26/14	
Post Code	MP - 26/14
Qualification	BE/B.Tech/MCA, CEH, Strong understanding of SIEM and EDR/XDR platforms, Incident response and forensic investigation fundamentals
Experience	Minimum 3+ years in Cybersecurity / SOC / SIEM / Detection Engineering
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	SOC Analyst (L1, L2)- Alert Monitoring, Initial Investigation, Advance Investigation, Incident Handling
Key Responsibilities	> Monitor SIEM, EDR/XDR, firewall, IDS/IPS, WAF, DLP, email security and other security tools. > Review and acknowledge security alerts within defined SLAs. > Monitor dashboards and security events for suspicious activity. > Identify anomalies and potential Indicators of Compromise (IOCs). > Identify attack patterns and potential lateral movement. > Investigate suspicious user, endpoint, and network and application activity. > Conduct detailed investigation of security incidents. > Determine incident scope, impact and severity. > Investigate compromised accounts, endpoints and network activity > Identify affected systems and potential attack paths. > Recommend blocking malicious IPs/domains/hashes where appropriate. > Coordinate endpoint isolation and account suspension according to approved procedures.
Interested candidates may fill-up the application form online through mentioned link as well as upload the detailed resume latest by 14/09/2026	