Incident Response Specialist - Information Security - MP - 26/13	
Post Code	MP - 26/13
Qualification	BE/B.Tech/MCA, Certified Incident Handler, Certified Forensic Analyst, CEH
Experience	Minimum 4+ years in Incident Response / SOC / Cybersecurity. Minimum 3+ years of hands-on incident-response/security-investigation experience preferred, Experience handling high-severity cybersecurity incidents, Experience working with SOC teams and security technologies
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	Major Incident Containment (Malware/ransomware, Account compromise, data leakage, Business e-mail compromise, RCA 7 lesson learned, Co-ordinate with It-Infra, compliance, Legal, HR), Response co-ordination
Key Responsibilities	> Lead investigation and response for medium, high and critical cybersecurity incidents. > Assess incident severity, business impact and scope. > Coordinate incident containment, eradication and recovery. > Coordinate response activities across IT, Network, Cloud, Application and business teams. > Ensure appropriate escalation to management and relevant stakeholders > Investigate incidents involving: Malware and ransomware, Phishing and Business Email Compromise (BEC), Credential compromise, Privileged-account abuse, Insider-related security events, Data leakage/exfiltration, Unauthorized access, Lateral movement, Command-and-control activity, Suspicious cloud activity, Web/application attacks, Endpoint compromise > Perform or coordinate forensic analysis of compromised systems > Work with relevant technical teams to isolate compromised endpoints, Disable or reset compromised accounts, Block malicious IPs, domains, URLs and hashes, Remove malware and persistence mechanisms. > Prepare incident updates for SOC Manager/CISO. > Provide timely updates during critical 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	