Detection/ SIEM Engineer - Information Security - MP - 26/12	
Post Code	MP - 26/12
Qualification	BE/B.Tech/MCA, GCIA / GCIH / GCDA / GCED, CEH, CISA, Strong experience with at least one major SIEM platform
Experience	Minimum 4+ 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	We are looking for an experienced professional can Monitor SIEM, SOAR, EDR and security-tool administration, Proactive Detection, Threat Identification, False Positive analysis
Key Responsibilities	> Administer and maintain the organization's SIEM platform. > Onboard and integrate security and infrastructure log sources. > Configure log collection, parsing, normalization, and enrichment. > Develop and maintain correlation rules and detection logic. > Monitor SIEM health, data ingestion, performance, and availability. > Troubleshoot missing, delayed, or malformed logs. > Manage log retention and ensure appropriate security monitoring coverage. > Design and develop detection use cases based on: MITRE ATTACK, Threat intelligence, Security incidents, Vulnerability information, Industry threat trends > Develop detection rules for suspicious activities and known attack techniques. > Continuously tune existing rules to improve detection accuracy. > Reduce false positives while maintaining appropriate detection sensitivity. > Security Log Management > Threat Detection & Threat Hunting > Develop and maintain security automation workflows. > Integrate SIEM with EDR, SOAR, threat intelligence and ticketing platforms. > Incident Response support
Interested candidates may fill-up the application form online through mentioned link as well as upload the detailed resume latest by 14/09/2026	