Cyber Security Engineer Responsibilities:

* BCOM / BCA / BSC – IT / BE/ MCA / B.Tech.
* A certification in one of the following - CISA / CISSP / CISM / CRISC will be an advantage.
* Candidate should have Information Security background, preferably in banking Industry
* Should have excellent analytical, drafting, communication (English Language - spoken and written) and presentation skills
* Having 3 to 4 years’ experience in Security domain preferably in BFSI sector
* Planning, implementing, managing, monitoring, and upgrading security measures for the protection of the organization’s data, systems, and networks
* Troubleshooting security and network problems
* Responding to all security breaches to the network and associated systems
* Ensuring that the organization’s data and infrastructure are protected by enabling the appropriate security controls
* Participating in the change management process
* Testing and identifying network and system vulnerabilities
* Daily administrative tasks, reporting, and communication with the relevant departments in the organization
* Evaluating the organization’s security needs and establish best practices and standards accordingly
* Designing, implementing, maintaining, overseeing, and upgrading all security measures needed to protect organizations’ data, systems, and networks
* Troubleshooting all network and security issues and incidents
* Routinely conduct penetration testing
* Taking appropriate security measures to ensure that the organization’s infrastructure and existing data are kept safe
* Conducting testing and scans to identify any vulnerabilities in the network and system
* Taking an active role in the change management process.
* Protecting the systems and networks of an organization against potential threats from cyberspace adversaries.
* Performing assessments and conducting regular penetration testing.
* Developing and implementing secure network solutions.
* Architecting and engineering trustworthy, reliable, and secure systems.
* Managing audits, intrusion, and security technology systems.
* Identifying unauthorized access and offering corrective solutions.
* Collaborating and coordinating with other teams to establish security protocols across the organization.