



Cyber Security Engineer

Job Description

Cyber security engineers, sometimes referred to as data security engineers or IT security engineers are cyber security professionals who create, develop, and implement extremely secure network solutions for businesses to guard against hacking attempts and other online dangers. They collaborate with other departments to identify and address any hiccups and/or security dangers brought on by security gaps. They are members of the IT team in any firm.

Key Responsibilities

- Determining the business's security needs and developing plans and backup plans if necessary.
- Creating, managing, implementing, and updating security networks and systems to safeguard all of an organization's sensitive data.
- Assisting in the creation of cybersecurity strategies to protect the organization in the event of a network system breach or incursion.
- Establishing safety measures, such as firewalls and encryption methods
- Addressing and resolving any internal security breaches that occur.
- Carrying out penetration testing to identify network weaknesses and openings.
- Taking the necessary actions to protect the current infrastructure and data.
- Taking care of basic duties like reporting and interacting with other departments to make problem-solving simple.
- taking part in the organization's change management process.

Qualifications Needed

- Degree in systems engineering, computer science, or a related discipline.
- Professional experience in forensics, incident detection and response, and other cyber security-related tasks.
- Knowledge of how firewalls work, how to maintain them, and how to use different endpoint security measures.
- Expertise with tools/languages like C++, Java, Node, Python, Ruby, Go, or Powershell.

- The capacity to perform in a fast-paced setting, frequently under pressure.
- A keen eye for detail and excellent problem-solving abilities.
- Up-to-date understanding of current hacker techniques and cyber security trends.