Cyber Security Roles

1. Chief Information Security Officer - CISO

A Chief Information Security Officer (CISO) is a senior-level officer who ensures the complete safety of information in an organisation. CISOs are responsible for developing and maintaining information security and risk management programs, and they are also required to interact with stakeholders and they brief them about the information security concerns. Usually, one becomes a CISO after having good experience in a few other cybersecurity job roles.

2. Security Architect

A Security Architect is responsible for designing robust security structures that are used to prevent malware attacks. They perform vulnerability tests and provide technical assistance to the other security team members.

3. Cybersecurity Engineer

Cybersecurity Engineers work on planning security measures to prevent the organisation from a cyberattack. They are responsible for protecting the organization’s networks and data. They design cybersecurity platforms and collaborate with the other teams to maintain overall security.

4. Malware Analyst

A malware analyst identifies and examines cyber threats such as viruses, worms, bots, and trojans to understand their nature. They develop malware protection tools, and finally, they document the methods to avoid malware threats.

5. Penetration Tester

A penetration tester, also commonly known as an ethical hacker, is a network security consultant who exploits a system’s vulnerabilities just like a hacker would. They design new penetration tools, and they also document the test results.

6. Computer Forensics Analyst

Computer Forensics Analysts work on cases to gather digital evidence and to retrieve data. They work on recovering deleted, manipulated, or stolen data.

This can be for private companies or law enforcement.

7. Application Security Engineer

The application security engineer is the one who creates, implements, and maintains the security of a company's applications. They are responsible for designing and implementing policies that will protect against both internal and external threats.

A typical day for an application security engineer starts with reviewing the previous day's findings and fixing any bugs or vulnerabilities found. After this, they will collaborate with other engineers to plan the next day's work.

8. Cloud Security Specialist

Because of the increased reliance on the cloud, cloud security specialists are in high demand and will remain so in the future. The role of a cloud security specialist is to protect data, systems, and networks from cyber-attacks. They do this by analysing threats and vulnerabilities, implementing safeguards, monitoring networks for intrusions, and overseeing compliance with regulations.

Cloud security specialists are responsible for ensuring the safety of data stored on a cloud server. They design and implement policies and procedures that protect data from unauthorised access, alteration, or disclosure.

9. Database Administrator

A database administrator is a person who manages and monitors the database. They are responsible for designing, creating, and maintaining the database. Database administrators also need to ensure data protection and security of the data in the database. Database Administrators are vital for the smooth functioning of any organization.

They are responsible for making sure that the databases are running efficiently and securely. Database administrators need to have a good understanding of databases, IT infrastructure, and programming languages.

10. Incident Manager

An incident manager is a person who is responsible for managing and resolving incidents.

They are called in when an incident arises, and they are the ones who will fix it. The most important aspect of this job is that they need to be able to handle all kinds of situations, which means they need to be able to think on their feet.