work field for cyber security department

Various work fields for Cybersecurity department:

- Application Security Officer: Ensuring the safety of software and applications
- AI Security Expert: Using AI to combat cybercrime
- Automotive Safety Engineer: Protecting cars from cyber-attacks
- Blockchain Developers/Engineers: Developing coding for the future of secure transactions
- Blue Team Members: Defending the most stringent defensive indicators/operating systems
- Bug Bounty Hunter: Detecting vulnerabilities and errors in electronic systems due to errors
- Network Security Scrum Master: Monitoring and protecting all data
- Chief Information Security Officer: Head of Information Security Department
- Senior Security Officer: Head of Personal Security/Information/Cybersecurity Department
- Cloud Security Architect: Protecting applications and cloud data
- Counterespionage Analysts: Thwarting cyber espionage in hostile countries
- Encryption: Decrypting encrypted mail without the encryption key

- Cryptographer: Developing a system to encrypt confidential and sensitive information
- Cyber Insurance Policy Expert: Consulting on cyber risks
- Network Intelligence Expert: Analyzing cyber threats and protecting the system from threats.
- Network Operations Experts: Integrating and implementing cyber attack procedures simultaneously against enemy activities and capabilities; They also perform defensive work to protect data, networks and electronic systems
- Cybercrime Investigator: Solve cybersecurity crimes
- Network Security Engineer: Develop security for computers.
- Cybersecurity Lawyer: Defend cybersecurity and cybercrime
- Network Security Software Developer/Engineer: Develop security settings in applications
- Data Privacy Officer: Ensure legal compliance with data protection
- Data Recovery Expert: Recover leaked data from digital devices
- Data Security Analyst: Protect information on computers and networks
- Digital Forensics Analyst: Examine data containing evidence of cybercrimes
- Disaster Recovery Expert: Plan and handle disasters and system disasters
- Governance, Risk, and Compliance Manager (GRC): Oversee risk management
- Industrial Internet of Things (IIoT) Security Expert: Protect industrial control systems

- Incident Responders: Initial response to cyber hacking and data theft
- Information Assurance Analyst: Identify information system risks
- Information Security Analyst: Plan and implement information security measures.
- Information Security Manager: Supervises the IT security team
- IT Security Engineer: Design, build and supervise the implementation of network and computer security systems for organizations; create complex security structures and ensure their operation; In addition to dealing with the defensive equipment dedicated to these networks (such as testing for vulnerabilities, installing firewalls, etc.) and responding (for example: responding to cybersecurity threats), they usually create a security infrastructure, provide technical guidance, assess costs and risks, and formulate security policies and procedures.
- IoT Security Experts: Protect network equipment
- Intrusion Detection Analyst: Use security tools to find targeted attacks.
- Mobile Security Engineer: Responsible for protecting mobile systems and equipment
- Network Security Officer: Protect computer networks from internal and external threats
- Penetration Tester: Conduct cyber attacks by simulating external network attacks

- Public Key Infrastructure Analyst: Manage the secure transmission of digital information
- Red Team Members: Participate in simulated cyber attacks
- SCADA (Supervisory Control and Data Acquisition) Security Analyst: System for protecting and protecting critical infrastructure