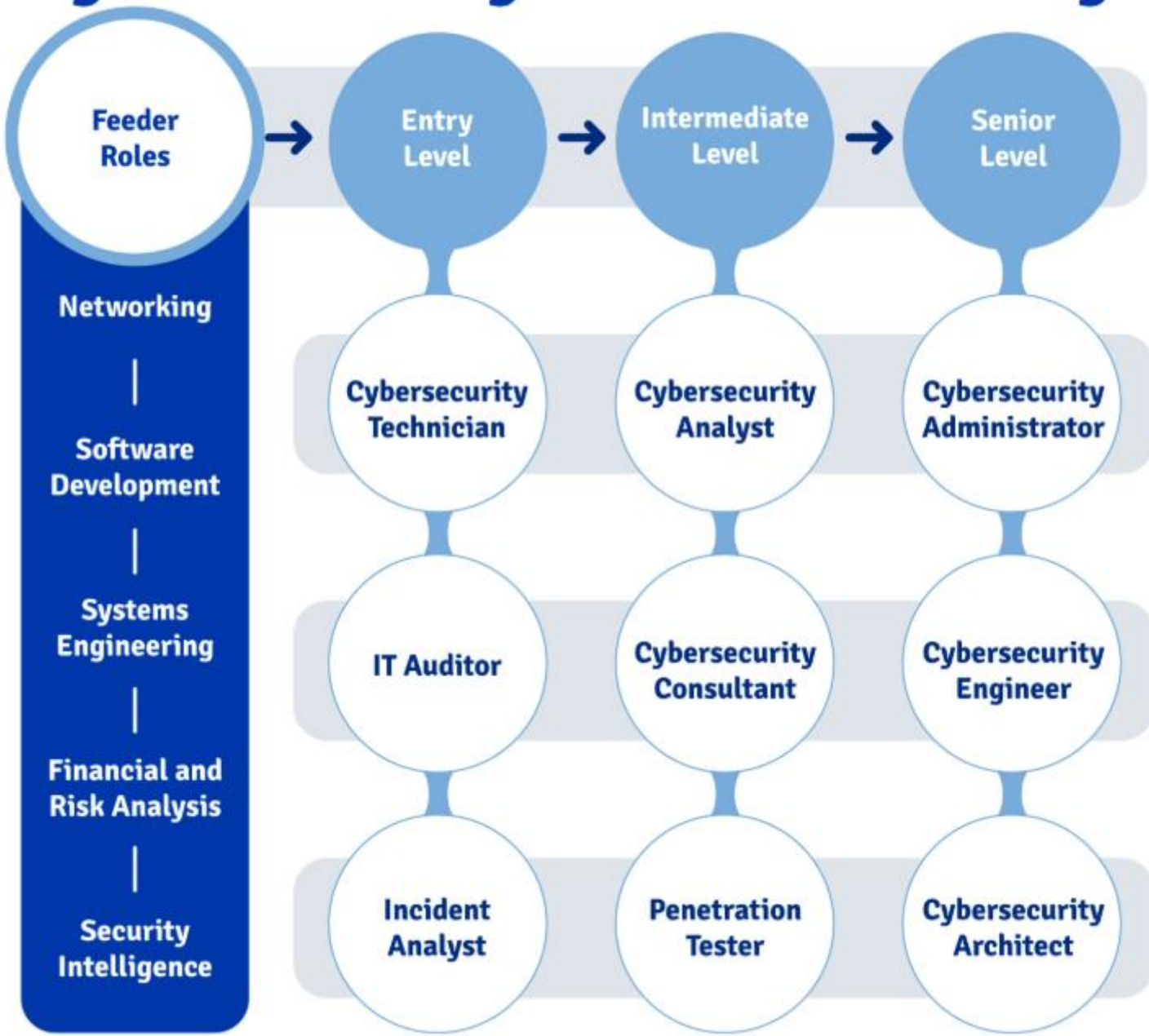
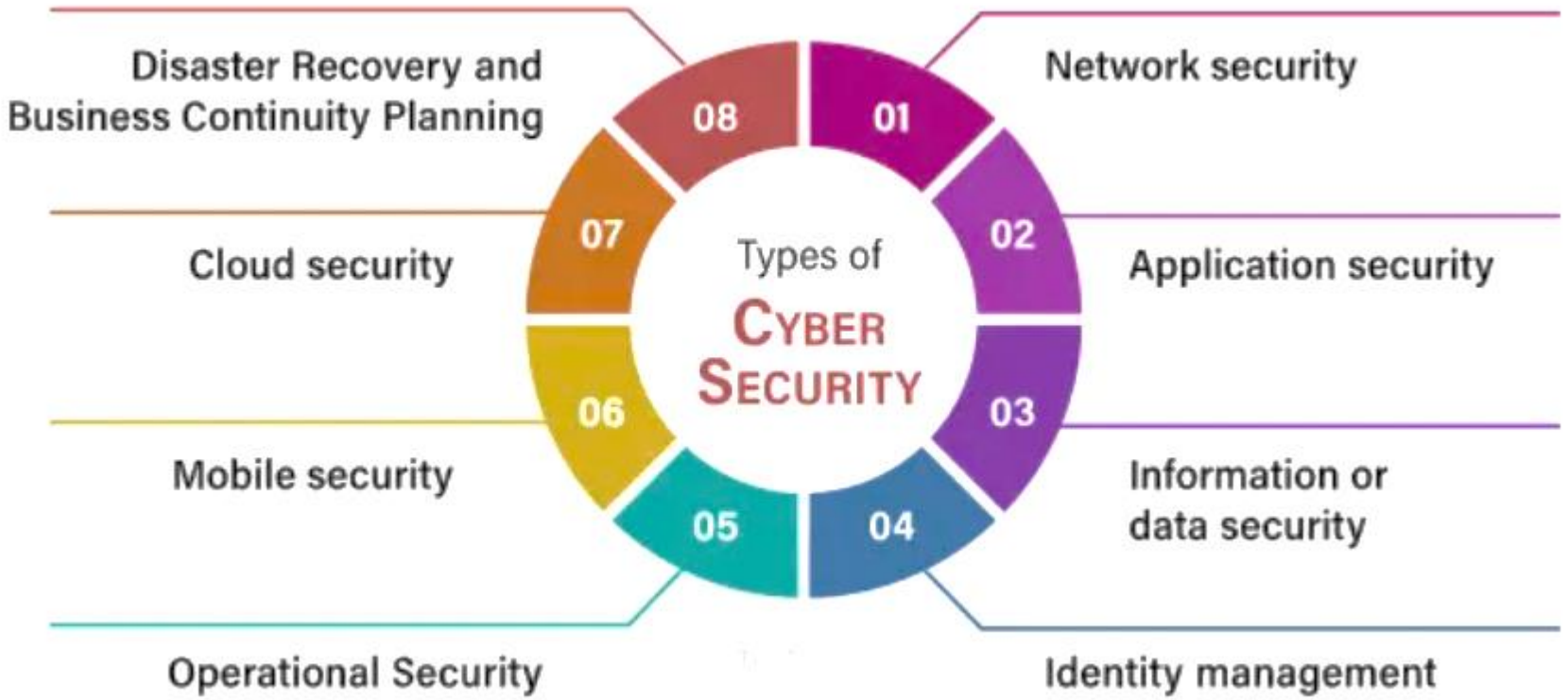
Cybersecurity Career Pathway

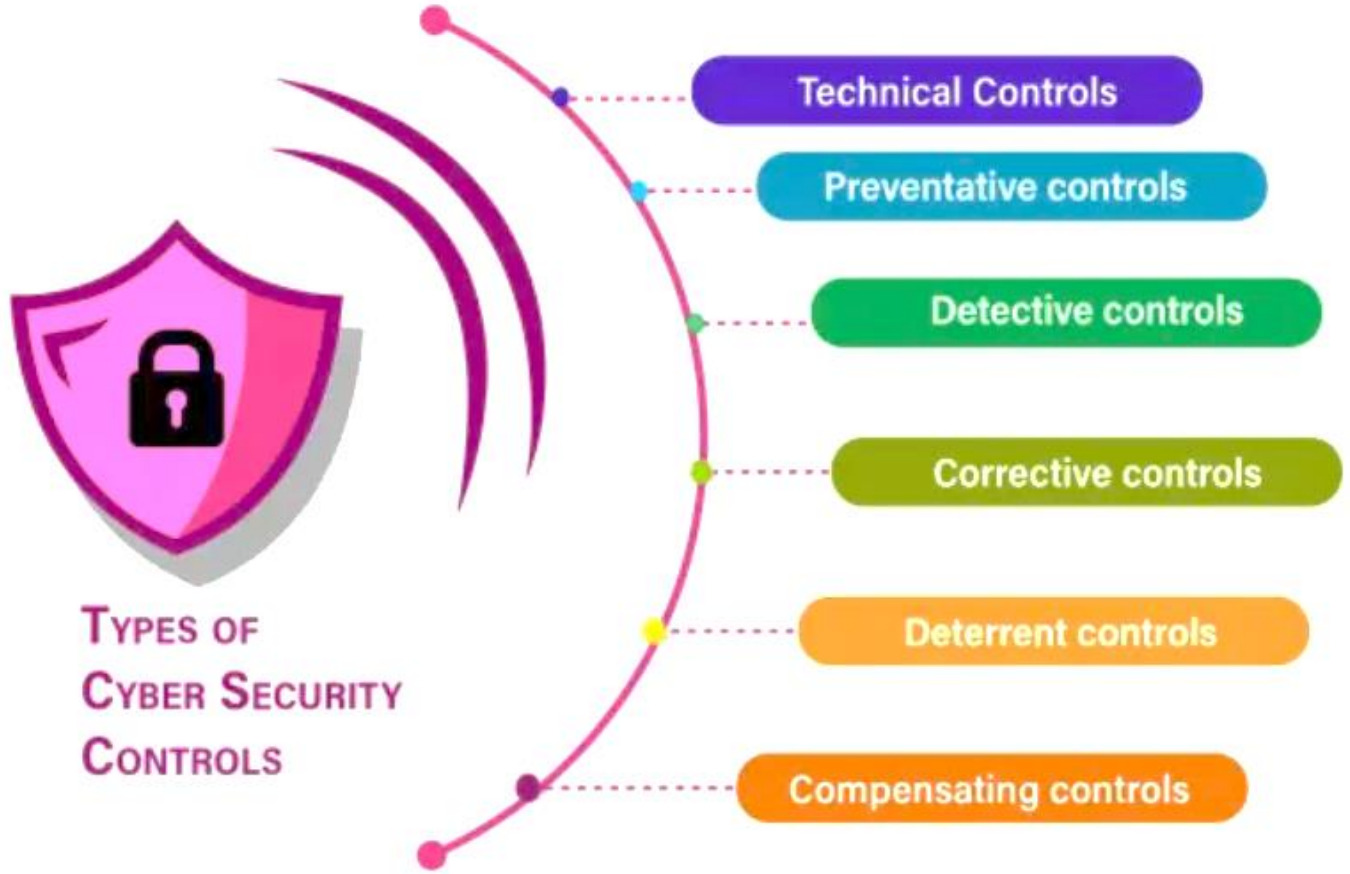


Cyber Security

Types


Types of
CYBER
SECURITY
01
Network security
02
Application security
03
Information or
data security
04
Identity management
05
Operational Security
06
Mobile security
07
Cloud security
08
Disaster Recovery and
Business Continuity Planning

Types of CS Controls



Tere
Papa
Detective
C
D
Chaman

Technical/Logical Controls

- Encryption
- Antivirus and anti-malware software
- Firewalls
- Security information and event management (SIEM)
- Instruction Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Technical Control Implementation Methods

- Access Control Lists (ACL)
- Configuration Rules
- Administrative controls like policies

Preventive Controls

- Hardening: It’s a process of reducing attacks and tightening security controls.
- Security awareness training: is the process of providing formal cyber security education to employees and stakeholders about security threats and the organization's policies and procedures.
- Change management: Measures taken by an organization to describe and implement changes both internally and externally in the system that include preparing and supporting employees to take the necessary steps for change.
- Account disable policy: This policy will disable the account when an employee leaves the organization.

Detective Controls

- Log monitoring – analyzing real-time data.
- SIEM- A set of tools and services are offered to analyze various system operational logs.
- Trend Analysis – Identifying the pattern from an application’s log output, to gather relevant information.
- Security Audits- set of measures that focus on cyber security standards and guidelines.
- Video Surveillance - Digital images and videos that are sent over communication networks are monitored.
- Motion Detection – Sensors are attached to detect nearby motions.

Corrective Controls

- IPS: detection of anomalies in traffic flow to quickly prevent malicious activity.

- Backups and system recovery: the Process of creating and storing data copies that can be used as backups when data is lost.

Other Controls

- **Management controls**: This control is used to mainly focus on risk management and information security management.

- **Operational controls**: The security controls that are primarily implemented, like technical and managerial controls executed by people, are saved by operational controls.

- **Physical controls**: Physical security controls in cyber security are implemented based on cyber measures in a defined structure. That is used to detect or prevent unauthorized access to sensitive data.

- **Deterrent controls:** Deterrent controls are used to reduce deliberate attacks, which are usually in the form of a tangible object or person.

- **Compensating controls:** Compensating control is an alternative method that is used to satisfy the requirement for security.