🛡️ Cybersecurity Domains & Frameworks

1. Cybersecurity Domains

Cybersecurity is divided into multiple domains (areas of security).

🔷 Core Domains

1. Network Security
    - Protecting networks from unauthorized access & attacks.
    - Example: Firewalls, IDS/IPS, VPNs.
2. Application Security
    - Securing apps against vulnerabilities.
    - Example: OWASP Top 10, Secure Coding, WAF.
3. Endpoint Security
    - Protecting user devices (laptops, mobiles, servers).
    - Example: Antivirus, EDR (Endpoint Detection & Response).
4. Cloud Security
    - Securing cloud infrastructure & SaaS apps.
    - Example: IAM (Identity Access Management), Zero Trust.
5. Identity & Access Management (IAM)
    - Authentication + Access Control.
    - Example: MFA, SSO, RBAC.
6. Data Security
    - Protecting data in transit & at rest.
    - Example: Encryption, DLP (Data Loss Prevention).
7. Infrastructure & Physical Security
    - Protecting physical systems (servers, data centers).

- Example: CCTV, biometric locks.

8. Governance, Risk, and Compliance (GRC)
    - Ensuring security policies & laws are followed.
    - Example: GDPR, HIPAA, ISO 27001.
9. Incident Response & Forensics
    - Detecting, responding, and investigating attacks.
    - Example: SIEM, forensic tools (EnCase, FTK).
10. Security Awareness & Training

- Educating users about phishing, social engineering.

---

2. Cybersecurity Frameworks

Frameworks are structured guidelines & best practices for securing organizations.

🔷 Major Frameworks

1. NIST Cybersecurity Framework (CSF)
    - 5 Functions: Identify → Protect → Detect → Respond → Recover.
2. ISO/IEC 27001
    - International standard for information security management.
3. CIS Controls
    - 18 prioritized security controls for organizations.
4. COBIT (Control Objectives for Information & Related Technology)
    - Focus on governance & IT management.
5. PCI DSS (Payment Card Industry Data Security Standard)
    - Protects cardholder payment data.
6. GDPR (General Data Protection Regulation)

    - Data privacy law in Europe.
7. HIPAA (Health Insurance Portability & Accountability Act)
    - Protects medical & healthcare data (USA).
8. SOC 2 (Service Organization Control)
    - Security & trust framework for service providers.

---

3. Relationship Between Domains & Frameworks

- Domains → "What to secure" (areas).
- Frameworks → "How to secure" (guidelines & standards).

Example:

- Domain: Network Security
- Framework: Use CIS Controls + NIST Detect to secure networks.