Brainstorming :-

1. Identifying Threats

- **Malware & Ransomware**: How attackers deploy malicious software and demand ransom.
- **Phishing & Social Engineering**: Tricks that manipulate human behavior.
- **DDoS Attacks**: Overloading systems to disrupt services.
- **Insider Threats**: Employees or partners leaking sensitive data.
- **Zero-Day Exploits**: Attacks targeting unknown vulnerabilities.
- **IoT Vulnerabilities**: Weak security in smart devices.

2. Analyzing the Impact

- Financial loss
- Data breaches and identity theft
- National security threats
- Reputation damage for organizations
- Disruption of critical infrastructure

3. Defensive Solutions

- **Encryption & Secure Communication**: Protecting data in transit and storage.

- **Firewalls & Intrusion Detection Systems (IDS)**: Monitoring network traffic.
- **AI-Powered Threat Detection**: Using machine learning to predict attacks.
- **Multi-Factor Authentication (MFA)**: Strengthening access control.
- **Zero Trust Architecture**: Verifying every access request.
- **Cyber Awareness Training**: Educating employees and users.

4. Emerging Technologies for Defense

- Blockchain for data integrity
- Quantum cryptography for unbreakable encryption
- Cloud security solutions
- Cyber threat intelligence platforms
- Ethical hacking and penetration testing

5. Future Trends

- The rise of AI-driven attacks
- Autonomous security systems
- Regulatory frameworks and compliance standards
- Global collaboration for threat intelligence sharing

6. Design Integration

- Visual representation of threat landscapes

- Interactive dashboards for real-time threat monitoring
- Gamified cybersecurity training modules
- Color-coded threat levels for intuitive understanding