**2)Ideation Phase:**

2.1)Various Ideas from each group members:

**Siddique Sanadi:**

* Explore the role of emerging technologies in cybersecurity, including the use of artificial intelligence for threat detection and the vulnerabilities associated with IoT devices. Understanding these technologies is crucial for developing effective security measures.
* Focus on various types of cyber threats, including malware, phishing attacks, and insider threats. Emphasize the need to understand how these threats operate and their potential impact on both individuals and organizations.
* Discuss various cybersecurity solutions, such as firewalls, encryption techniques, and multi-factor authentication. Highlighting practical solutions can help organizations better protect themselves against cyber threats

**Swapnil Patil:**

* Emphasize the importance of human factors in cybersecurity. Explore topics like cybersecurity awareness training and social engineering tactics, as these are critical in preventing breaches caused by human error.
* Highlight the significance of having a robust incident response plan. Include best practices for incident response and disaster recovery strategies to help organizations recover from cyber incidents effectively.
* Investigate future trends in cybersecurity, such as the growing demand for cybersecurity professionals and the challenges of securing remote work environments. This will provide insights into the evolving landscape of cybersecurity.

**2.2)Features:**

**Threat Identification**

* Tools and methods to recognize different types of cyber threats, such as malware, phishing, and ransomware.

**Risk Assessment**

* Evaluating the potential risks associated with various cyber threats to determine their impact on an organization or individual.

**Preventive Measures**

* Basic security practices, such as using strong passwords, enabling two-factor authentication, and keeping software updated to prevent attacks.

**Incident Reporting**

* A straightforward process for reporting suspected cyber incidents or breaches to the appropriate authorities or IT teams.

**User Education**

* Simple training sessions or materials that teach users about common cyber threats and safe online behaviors.

**Data Protection Strategies**

* Techniques for safeguarding sensitive information, including encryption and secure data storage solutions.

2.3) Empathy Map

[Thinks 💭]

[Says 🗣️]

- "I’m worried about breaches." - "Is my data safe?"

- "How can I protect my data?" - "What are the latest threats?"

- "I don’t know which tools to use." - "Is investing in cybersecurity worth it?"

Target Audience: Students, Professionals, etc.

Needs: Awareness, Solutions, Best Practices

[Feels ❤️]

[Does 🏃‍♂️]

- Uses antivirus and firewalls. - Fear of being hacked.

- Follows strong password rules. - Frustrated with complex solutions.

- Attends cybersecurity training. - Empowered when learning protection.