1. Problem Statement:

As the use of web applications continues to grow across industries, the security of these applications has become a critical concern. Web applications often contain sensitive data and business-critical information, making them prime targets for cyberattacks. Despite advancements in security technologies, many organizations still struggle to adequately identify and address vulnerabilities within their web applications.

Current cybersecurity measures often fall short due to evolving attack techniques, lack of comprehensive vulnerability scanning, and insufficient application security assessments. This project aims to address the growing challenge of securing web applications by systematically identifying vulnerabilities through industry-standard scanning tools and ethical hacking methodologies. The lack of proactive and thorough security assessments exposes organizations to potential data breaches, financial losses, and reputational damage.

The research focuses on providing actionable insights into vulnerability types, their business impacts, and effective mitigation strategies, contributing to a more secure and resilient digital environment for businesses.

2. Brainstorming:

2.1 **Holistic Security Integration (“Shift Left”)**

- Integrate security testing early in the development lifecycle (e.g., code reviews, automated SAST/DAST in CI/CD pipelines).
- Provide developer training and code scanning tools so they can identify and fix vulnerabilities before production.

2.2 **Automation & Tooling**

- Automated vulnerability scanning tools that run regularly on staging or production environments.
- AI-driven anomaly detection tools to spot unusual traffic patterns or user behavior.
- Container security scanning (if using Docker/Kubernetes) to identify known vulnerabilities in images.

2.3 **Continuous Penetration Testing / Bug Bounties**

- Ongoing penetration tests rather than annual or quarterly—simulate real-time threats.
- Encourage responsible disclosure and bug bounty programs to leverage the ethical hacker community.

2.4 **Threat Modeling Workshops**

- Regular cross-team workshops (developers, QA, security, product owners) to map out potential threats and attack vectors.
- Use standardized frameworks like STRIDE or PASTA to guide the discussion and identify likely weaknesses.

2.5 **User Awareness & Training**

- Security training not only for technical teams but also for non-technical staff who handle sensitive data.
- Create easy-to-digest documentation or e-learning modules for developers about common web vulnerabilities (OWASP Top 10).

2.6 **Policy and Governance**

- Establish clear security policies and guidelines that are easy to understand and follow.
- Enforce compliance checks and audits to ensure security standards are met consistently.
- Have an escalation matrix for reporting and addressing vulnerabilities quickly.

2.7 **Security by Design**

- Encourage designing features with security in mind from the start, rather than adding it as a patch later.
- Leverage secure coding practices and frameworks that minimize common vulnerabilities (e.g., using prepared statements for SQL, parameter validation, etc.).

2.8 **Risk-Based Approach**

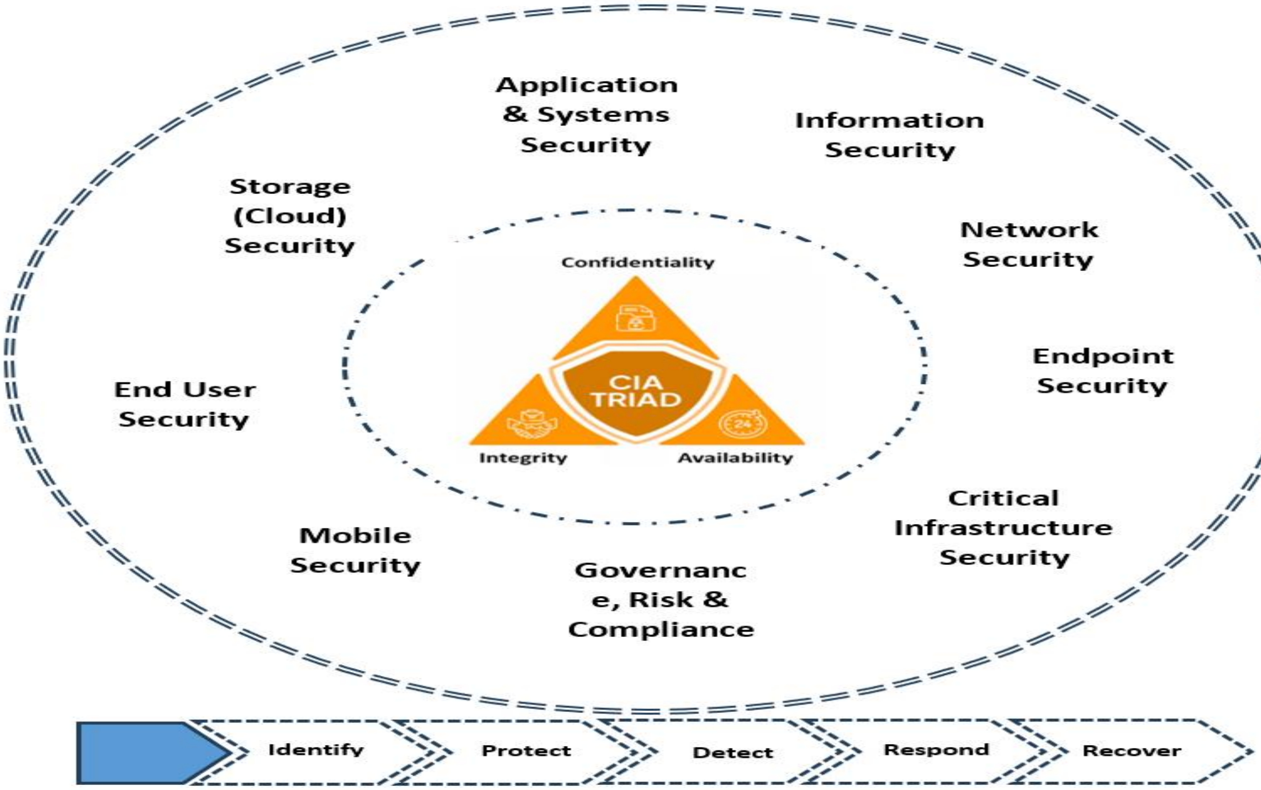
- Categorize vulnerabilities based on their impact and exploitability to prioritize remediation.
- Align business goals with security posture by identifying critical assets that need the highest level of protection.

2.9 **Incident Response & Disaster Recovery**

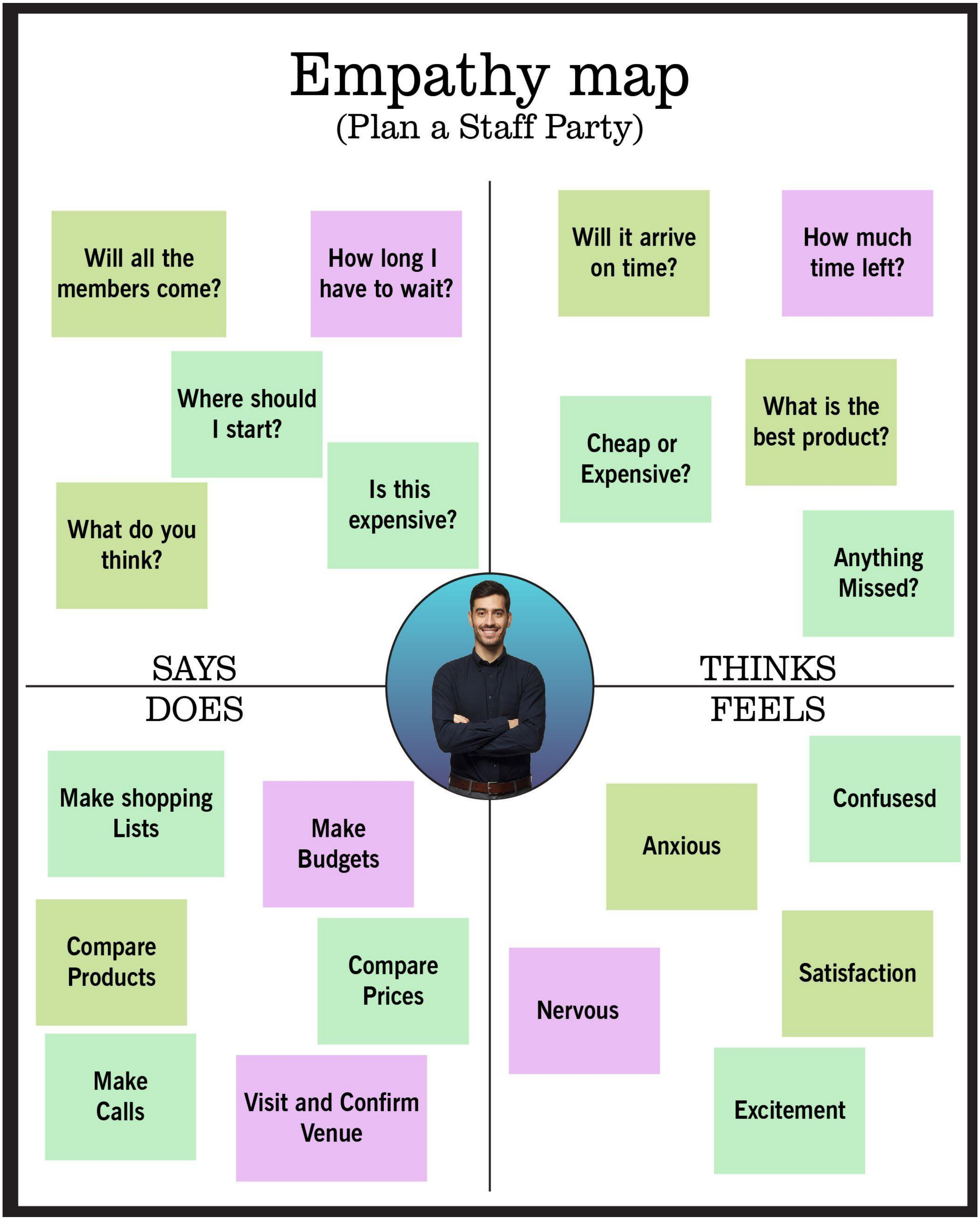
- Develop clear incident response playbooks to ensure quick, coordinated responses to security incidents.
- Regularly test incident response plans with simulated breaches or tabletop exercises.
- Have robust backup and recovery processes to mitigate data loss.

2.10 **Proposed Cybersecurity Architectures**

A coordinated effort is vital in maintaining a good cyber security posture as organizational assets are comprised of various platforms. The web of cybersecurity measures working together to protect a system is called cybersecurity domains.
The proposed cybersecurity architecture makes use of the NIST framework (Identify, Protect, Detect, Respond, Recover) "GOALS" as the foundation (these are further discussed in Section 5.1) and utilises the pillars from the CIA triad (Confidentiality, Integrity, Authenticity) at the CENTER (discussed in Section 5.2) and finally offer nine (9) subdomains as the core of the architecture (discussed in Section 5.3)



3. **Empathy Map :**



Empathy map

(Plan a Staff Party)

SAYS

Will all the members come?

How long I have to wait?

Where should I start?

What do you think?

Is this expensive?

THINKS

Will it arrive on time?

How much time left?

Cheap or Expensive?

What is the best product?

Anything Missed?

DOES

Make shopping Lists

Make Budgets

Compare Products

Compare Prices

Make Calls

Visit and Confirm Venue

FEELS

Confusesd

Anxious

Nervous

Satisfaction

Excitement

Empathy Map – Short Overview

- **Definition**: A visual tool to understand a user’s mindset, needs, and challenges by categorizing what they **Think & Feel**, **Hear**, **See**, **Say & Do**, **Pains**, and **Gains**.
- **Purpose**:
    1. **User-Centric Insight** – Helps teams design or improve solutions based on real user motivations.
    2. **Identify Obstacles & Motivations** – Highlights frustrations and desires, guiding better user experiences.
    3. **Foster Alignment** – Ensures everyone shares the same understanding of the user’s perspective.

Key Sections

- **Think & Feel**: Inner thoughts, worries, motivations.
- **Hear**: Influences from peers, management, media.
- **See**: Observations in the user’s environment.
- **Say & Do**: Public statements and behaviors.
- **Pains**: Frustrations or obstacles.
- **Gains**: Positive outcomes or benefits the user wants.