Ideation Phase

1. Understanding the Problem

Before conducting security assessments, we need to define the **key cybersecurity challenges**:

- **What are the risks?** (e.g., web application vulnerabilities, data breaches, malware attacks)
- **Who are the stakeholders?** (Developers, security analysts, management)
- **What is the goal of the project?** (Identify vulnerabilities, enhance security, ensure compliance)

2. Brainstorming Solutions

To address the identified risks, multiple solutions were considered:

- **Manual Security Testing** – Penetration testing, source code review.
- **Automated Scanning** – Using tools like Nessus, Burp Suite, and OWASP ZAP.
- **Continuous Monitoring** – Implementing SIEM solutions for real-time threat detection.
- **Compliance Auditing** – Ensuring adherence to security frameworks (ISO 27001, PCI-DSS).

3. Selecting Key Features & Grouping Them

Based on feasibility and impact, the following areas were prioritized:

- **Web Security Testing** (SQL Injection, XSS, Authentication flaws).
- **Infrastructure Scanning** (Server misconfigurations, outdated software).
- **Incident Response & Threat Monitoring** (SOC & SIEM integration).

4. Prioritization

A **feasibility vs. impact matrix** was used to classify tasks:

- **High Impact, High Feasibility** → Automated scanning, patch management.
- **High Impact, Low Feasibility** → AI-based security automation.
- **Low Impact, High Feasibility** → Enabling security headers.
- **Low Impact, Low Feasibility** → Advanced forensic analysis.

5. Empathy Mapping

To better understand the concerns of stakeholders, an **Empathy Map** was created:

- **SAYS:** "How can we prevent security breaches?"
- **THINKS:** "Are our defenses strong enough?"
- **DOES:** Conducts vulnerability assessments and threat analysis.

- **FEELS:** Anxious about security gaps and compliance risks