Ideation Phase

Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age

Team Members:

1. Dhanraj Pawar
2. Balaji Patil
3. Kaushal Chougule
4. Atharv Pawar

Ideation Phase Overview

The Ideation Phase is where we brainstorm and define the core ideas, objectives, and scope of the project. This phase helps us understand the problem, explore potential solutions, and plan the next steps.

Key Objectives

- **Recognize Common Cyber Threats:**
  - Investigate the most widespread cyber risks in today's digital world (e.g., phishing, malware, ransomware, DDoS attacks).
  - Analyse the effects of these threats on individuals and businesses.
- **Examine Protective Measures:**
  - Study security tools, technologies, and methods to counter cyber threats (e.g., firewalls, encryption, SIEM, threat intelligence).
  - Assess the efficiency of these protective solutions.
- **Outline Project Scope:**
  - Identify key focus areas for the project (e.g., vulnerability analysis, threat detection, incident management).
  - Define specific objectives and expected outcomes for each focus area.

Brainstorming Questions

To guide the ideation process, we asked the following questions:

1. What are the most common cyber threats today?
    - Phishing attacks, malware, ransomware, insider threats, DDoS attacks, etc.
2. How can organizations protect themselves from these threats?
    - Implement firewalls, use encryption, train employees, deploy SIEM tools, etc.
3. What tools and technologies are available for cyber security?
    - Nessus (vulnerability scanning), Splunk (SIEM), Wireshark (network analysis), Metasploit (penetration testing), etc.
4. What are the key challenges in cyber security?
    - Lack of awareness, evolving threats, resource constraints, compliance requirements, etc.

Ideation Output

To facilitate the ideation process, we considered the following questions:

1. **What are the most prevalent cyber threats today?**
    - Examples include phishing scams, malware infections, ransomware attacks, insider risks, and DDoS incidents.
2. **How can businesses safeguard themselves from these risks?**
    - By deploying firewalls, utilizing encryption, educating employees, implementing SIEM solutions, and more.
3. **What cybersecurity tools and technologies are available?**
    - Some options include Nessus (vulnerability assessment), Splunk (SIEM), Wireshark (network monitoring), and Metasploit (penetration testing).
4. **What are the primary challenges in cybersecurity?**
    - Issues such as limited awareness, constantly evolving threats, budgetary limitations, and regulatory compliance hurdles.

Next Steps

1. Requirement Analysis:
    - Define functional and non-functional requirements for the project.
    - Identify tools, technologies, and resources needed.
2. Project Design:
    - Create a system architecture for the proposed solutions.
    - Design workflows for vulnerability assessment, threat hunting, and incident response.
3. Project Planning:
    - Develop a sprint plan with tasks, timelines, and assigned team members.
    - Estimate story points and prioritize tasks.
