Ideation Phase
Empathize & Discover

Date	12 October 2023
Team ID	Team-593479
Project Name	Malware Detection and Classification
Maximum Marks	4 Marks

Team Members:

Ramar Priya Maha Lakshmi

Chevala Syam Sai

Panchada Varun

Mulumudi Prabhas

Empathy Map Canvas:

An empathy map is a simple, easy-to-digest visual that captures knowledge about a user's behaviours and attitudes. It is a useful tool to helps teams better understand their users.

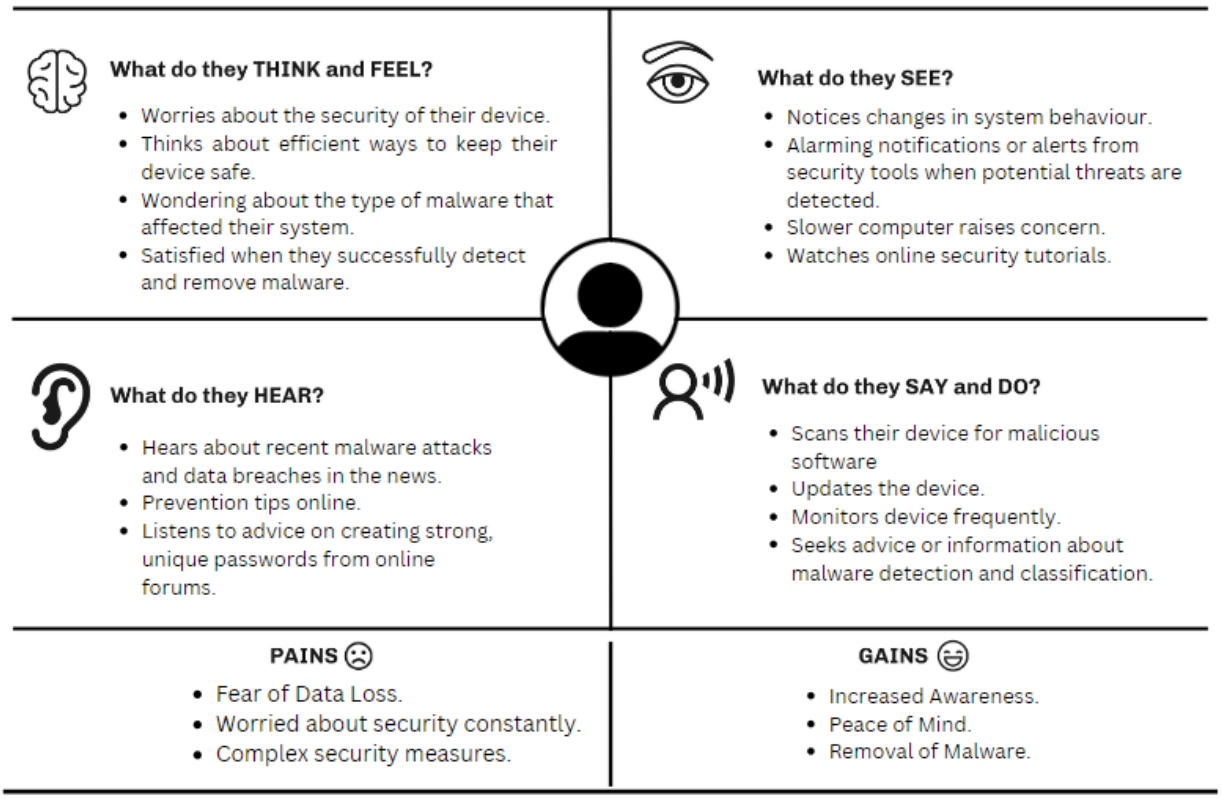
The empathy map for "**Malware Detection and Classification**" illuminates the multifaceted user perspective in the realm of cybersecurity. Users often find themselves navigating a landscape filled with concerns and complexities. They ponder the security of their valuable data, contemplating the best ways to identify and classify malware to ward off potential threats. Users hear advice from peers and experts, seeking insights on protection. They engage in discussions about security and encounter visual cues from security software. This collective experience guides the development of user-centric solutions.

They fear data loss, grapple with device security, and struggle with the intricacies of security measures. Uncertainty about the ever-evolving malware landscape adds an extra layer of stress. However, there are gains in the journey as well. Effective malware detection provides peace of mind, quick and accurate alerts empower proactive responses, and streamlined security measures simplify the process. Users also benefit from increased awareness, which enhances their knowledge of emerging threats and best practices. These pains and gains guide the design of user-centric cybersecurity solutions, aiming to alleviate concerns and empower users with confidence in their digital interactions.

Empathy Map

Team ID -593479

Topic: Malware Detection and Classification



Conclusion:

Understanding the user perspective through the empathy map is pivotal for developing user-centric solutions in the realm of malware detection and classification. By recognizing their thoughts, feelings, actions, and experiences, we can design cybersecurity systems that alleviate their pains and deliver the gains they seek. This approach ensures that our efforts align with the real needs and emotions of the users, resulting in more effective and user-friendly tools and strategies to combat malware threats.