Empathy Map

Who are we empathizing with?

- *Security Analysts:* Cybersecurity professionals responsible for monitoring and protecting their organization's digital assets.
- *IT Managers:* Individuals overseeing the IT infrastructure and security within organizations.
- *End Users:* Employees or individuals using digital devices and systems for work or personal purposes.

Where can it be used?

- *Work Environment*: Security analysts and IT managers operate within organizational security teams, often located in SOC's.
- *Digital Landscape:* Malware threats can infiltrate through various online channels,including emails, web downloads, and network vulnerabilities.
- *Global Reach:* Malware threats affect organizations worldwide, transcending geographical boundaries.

Why this project?

- *Security*: Protecting the organization's data, systems, and reputation from cyberattacks.
- *Compliance*: Adhering to regulatory requirements and industry standards is essential for avoiding penalties and reputational damage.
- *Business* ***Continuity***: Ensuring that malware threats do not disrupt operations and revenue generation.
- *User Confidence*: Providing end users with the assurance that their digital activities are safe and reliable.

When is it Implemented?

- *Continuous Vigilance:* Maintaining an ongoing, round-the-clock watch for potential malware intrusions.
- *Immediate Response:* Swift action is crucial upon detecting malware to prevent damage or data breaches.
- *Regular Updates*: Consistently updating malware detection databases and software to keep pace with evolving threats.

WHAT ARE OUR CONCERNS?

Worries about malware compromising sensitive information, disrupting operations, and causing financial losses

WHAT ARE OUR OBJECTIVES?

Proactively identify and mitigate malware threats, ensuring the continuity of operations.

WHAT ARE OUR REQUIREMENTS?

Efficient malware detection tools, comprehensive threat classification, and real-time monitoring for rapid response.

WHAT ARE OUR CHALLENGES?

Staying up to date with emerging threats, ensuring user compliance with security protocols