

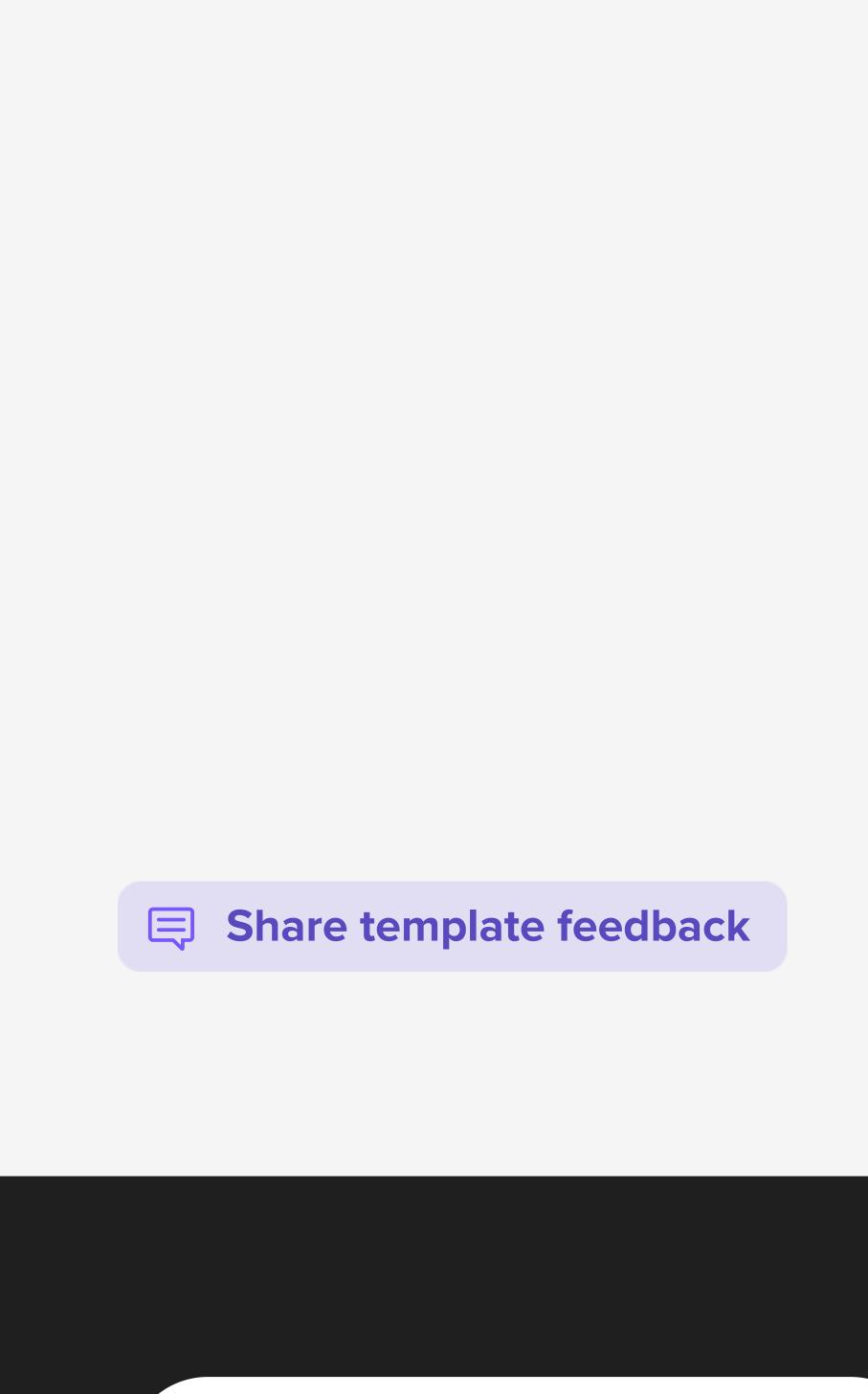
# Empathy map canvas

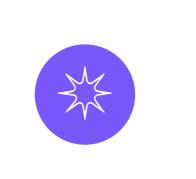
Use this framework to empathize with a customer, user, or any person who is affected by a team's work.

Document and discuss your observations and note your assumptions to gain more empathy for the people you serve.

Originally created by Dave Gray at







## Develop shared understanding and empathy

Summarize the data you have gathered related to the people that are impacted by your work. It will help you generate ideas, prioritize features, or discuss decisions.



### WHO are we empathizing with?

We are empathizing with the people who are using web servises and softwares and get attacked by the malware.

What Do

they

Hear

Web users
are
requiredd to
be safe

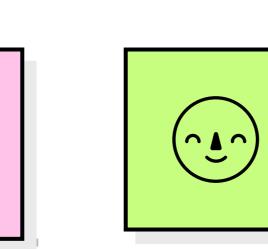
Malware detection systems alert users of potential threats, providing specific names, classifications, and severity ratings. They may also offer action recommendations, date and time of detection, affected files, and potential impact. However, they can generate false positives, disrupting

legitimate operations.



**GOAL** 

PAINS



GAINS

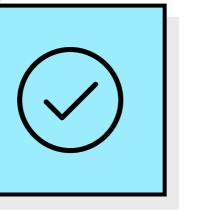
On of the drawbacks of this project are we are very exposed to malware itself so we need to check our own systems.

1. While Designing
the project we
wont be able to
detect most of the
malware in the file,
Database,
Network and App's
etc.,

The impact of the project is to detect malware and classify it.
 We can use Al and python to build this Tool.

3. Our Projects helpss in detecting the malware and classify them.

What other thoughts and feelings might influence their behavior?

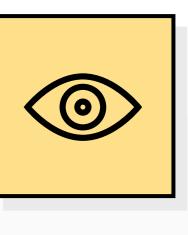


## What do they DO? Type your paragraph...

Malware detection methods include Signature-Based Detection, Behavior-Based Detection, Heuristic Analysis, and Machine Learning and Al, which compare files or network traffic with known malware patterns

Malware classification aids cybersecurity professionals in identifying threats, including viruses, worms, Trojans, ransomware, spyware, adware, rootkits, and others, considering propagation method, target, and sophistication level.

Anti-virus software detects and removes malware, while sandboxing analyzes suspicious files. Networkbased intrusion detection systems monitor traffic for malware activity, while endpoint detection and response solutions provide visibility and control.



#### What do they SEE?

Administrators of systems:
They constantly receive alerts
and logs, making it challenging
to differentiate between safe
and dangerous conduct. They
also recognize the possible
consequences of a malware
assault, which might include
data breaches, monetary
losses, and reputational harm.

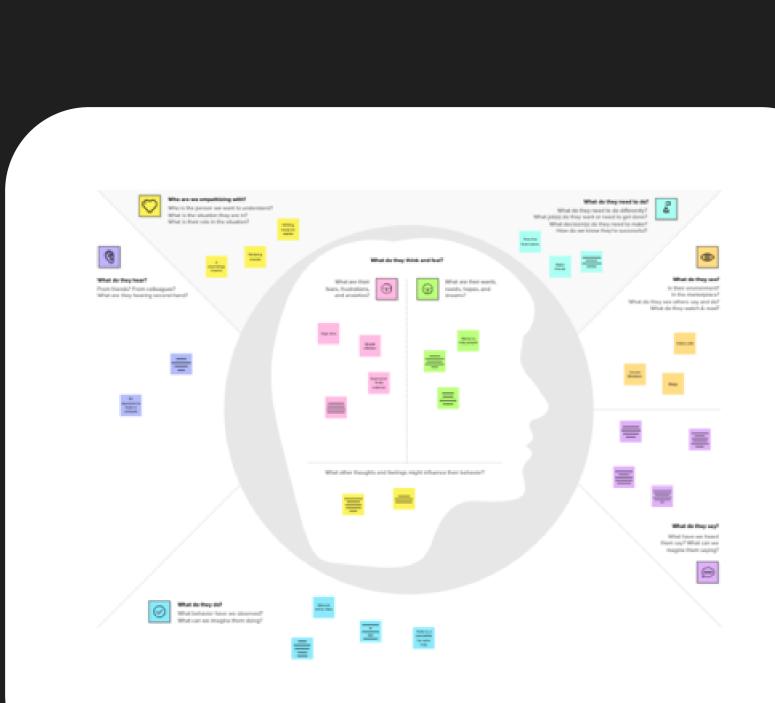
Users: They consider malware to be a threat to their security and privacy. They might not be knowledgeable about all the various varieties of viruses that exist or how to defend themselves against them.

Additionally, methods for malware detection that produce false positives or hinder productivity may irritate them.



## What do they SAY?

Malware detection systems use a variety of techniques, such as pop-up messages, email alerts, quarantine reports, severity information, recommendations, database updates, and false positive notifications, to notify users and administrators of possible risks.



Need some inspiration?

See a finished version of this template to kickstart your work.

Open example





