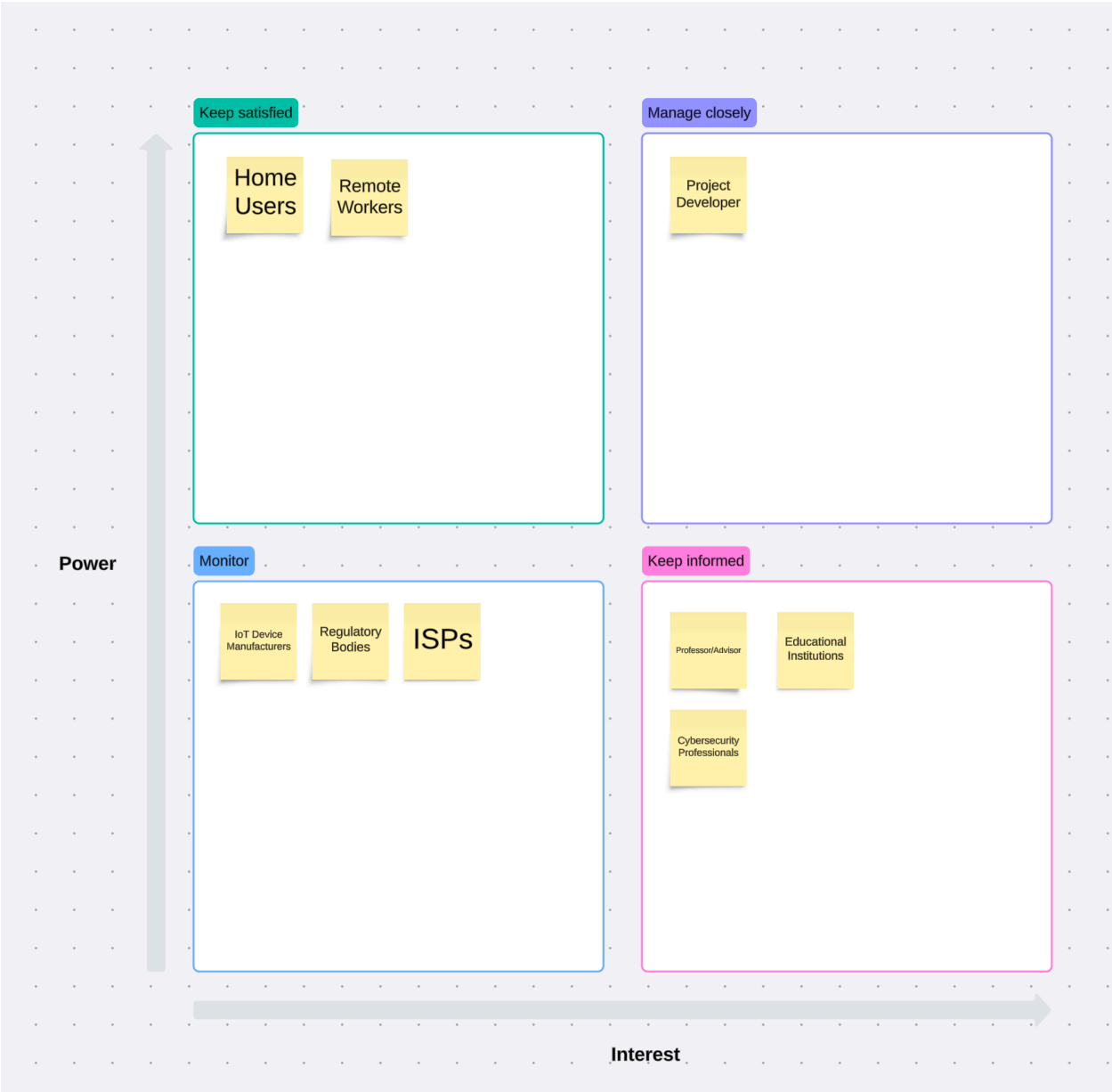
Stakeholder Map outline



1. Primary Stakeholders

Home Users:
Description: Non-technical individuals who own and manage home networks, including families, students, and IoT enthusiasts.
Influence: Their needs and preferences directly shape the tool's features and user interface. The success of the project depends on its ability to address their pain points and provide a seamless user experience.

Remote Workers:
Description: Professionals who rely on home networks for their work, especially those in industries requiring secure access to sensitive corporate data.
Influence: As frequent users of home networks for work-related tasks, their feedback ensures that the tool addresses vulnerabilities that could compromise professional activities or sensitive data. Their adoption of the tool is vital to preventing breaches that could impact both personal and corporate security.

2. Secondary Stakeholders
Cybersecurity Professionals:
Description: Experts in network security who may use the tool to provide services or training for home users.
Influence: Their feedback and best practices inform the technical design, ensuring the tool adheres to cybersecurity standards.
Internet Service Providers (ISPs):
Description: Companies that provide internet connectivity to home users.
Influence: ISPs could endorse or promote the tool to enhance customer satisfaction by addressing network security issues.

3. Tertiary Stakeholders

Educational Institutions:
Description: Schools, universities, or organizations providing cybersecurity education and awareness programs.
Influence: They may integrate the tool into training curricula, helping to raise awareness about home network vulnerabilities.

IoT Device Manufacturers:
Description: Companies producing smart devices commonly found in home networks.
Influence: Their cooperation could help ensure compatibility with the tool and encourage users to adopt secure practices for IoT device setup.
Regulatory Bodies:
Description: Government agencies or organizations focused on data privacy and cybersecurity regulations.
Influence: They set guidelines for cybersecurity best practices that inform the tool's recommendations and ensure legal compliance.

4. Development Team

Project Developer:
Description: The designer and developer of the tool.
Influence: Responsible for translating user needs into technical features, maintaining project scope, and ensuring timely delivery.

Professor/Advisor:
Description: Academic guide providing oversight and feedback on the project.
Influence: Offers critical insights and ensures the project aligns with educational and professional standards.

5. Indirect Stakeholders

Families of Users:
Description: Individuals who share home networks with primary users.
Influence: They benefit from enhanced network security, reducing the risk of breaches and protecting shared resources.

Stakeholder Influence Summary
The success of the Home Network Vulnerability Assessment Tool relies on aligning the needs and expectations of its stakeholders. Home users and remote workers dictate the tool's usability and effectiveness, while secondary and tertiary stakeholders provide essential support and resources to ensure the project's real-world application. Collaboration among these groups ensures the tool's relevance, sustainability, and impact.