Potential challenges and risks

- Restricted permissions on machines may limit the tool's ability to scan all areas of the system.
- AI-powered anomaly detection could flag non-critical issues, leading to unnecessary alerts.
- Scanning may consume significant system resources on low-end devices, impacting performance.
- Accessing and scanning sensitive system data could raise potential privacy and compliance issues.
- Relying on outdated databases may result in missing recent vulnerabilities or false security assessments.
- Storing scan logs on blockchain without proper encryption could expose sensitive system information.

Strategies for overcoming these challenges

- **False Positives**: Regularly refine AI models using real-world data and feedback to minimize incorrect alerts.
- **Performance**: Schedule scans during system idle times or run in small batches to reduce resource impact on low-end systems.
- **Privacy Concerns**: Ensure read-only operations with encryption and data masking to safeguard sensitive information.
- **Outdated Vulnerability Data**: Automate updates from trusted sources to keep vulnerability data current and relevant.
- **Blockchain Data Security**: Implement encryption for blockchain-stored logs to ensure tamper-proof records while protecting sensitive data.

SIH

SMART INDIA HACKATHON 2024

Code Breakers

Analysis of the feasibility of the idea

•***Technological***:

➢ The solution leverages proven tools like WMI, PowerShell, and vulnerability databases (e.g., ExploitDB).

➢ AI/ML for anomaly detection is supported by existing libraries, making real-time vulnerability assessments achievable.

➢ Additionally, blockchain technology ensures secure and immutable logging of scan results, preventing tampering or unauthorized modifications.

•***Operational***:

➢ The agent-less design simplifies deployment across Windows 10/11, reducing overhead and eliminating the need for additional software.

➢ The solution integrates smoothly with AV/EDR systems and scales easily for both individual and enterprise use.

➢ Blockchain enhances security by ensuring tamper-proof logs, adding an extra layer of trust and data integrity.

IMPACT AND BENEFITS

Potential impact on the target audience

SIH

SMART INDIA HACKATHON 2024

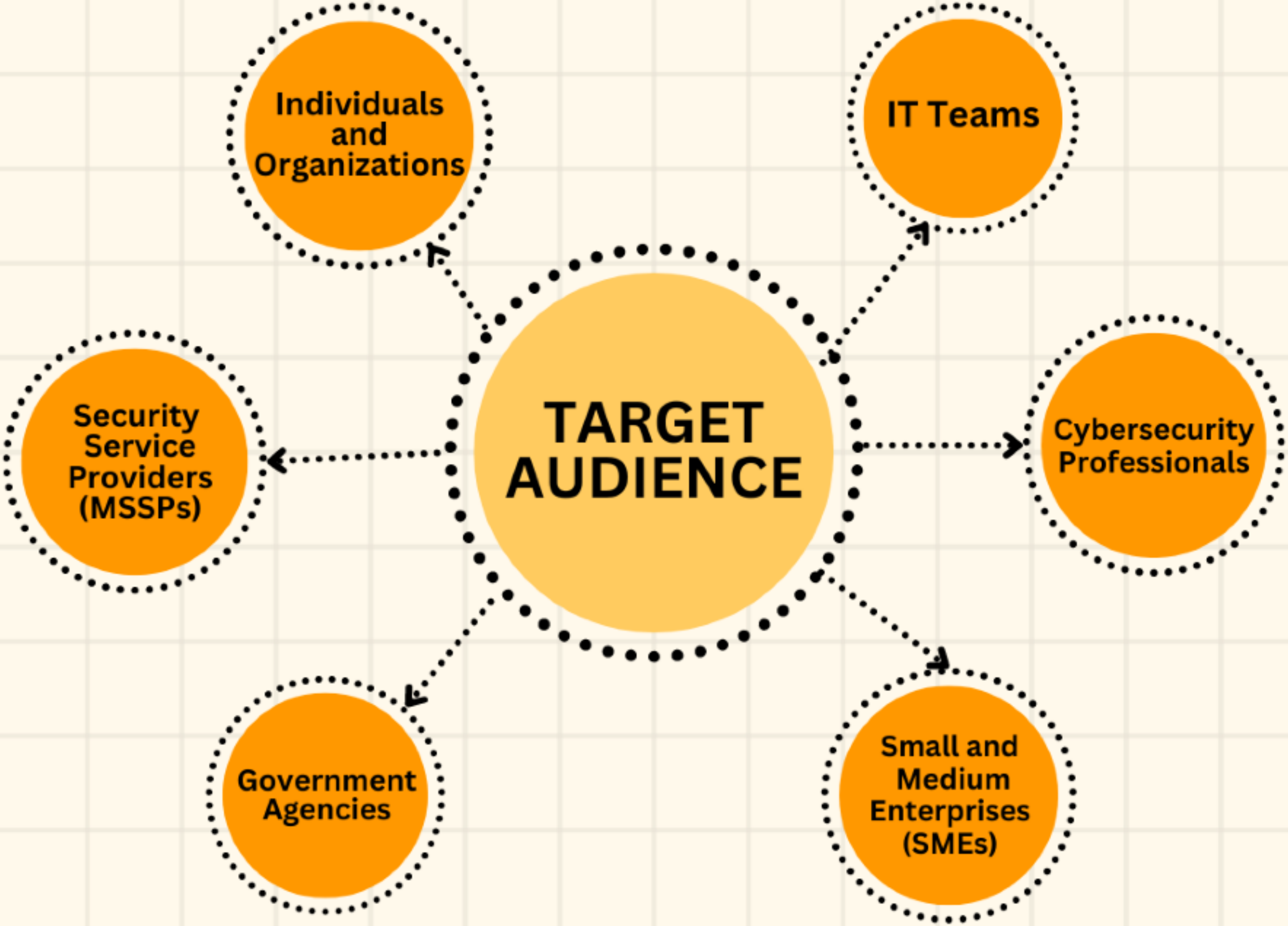
Code Breakers

Benefits of the solution (social, economic, environmental, etc.)

- **Social Benefits**: Enhances the security of personal and organizational data, reducing the likelihood of data breaches and protecting user privacy.

- **Economic Benefits**: Helps organizations avoid the high costs associated with data breaches, ransomware attacks, and other security incidents by identifying vulnerabilities early.

- **Environmental Benefits**: The agent-less nature of the solution ensures minimal system resource consumption, reducing energy usage and system strain, contributing to greener IT practices.



TARGET AUDIENCE

Individuals and Organizations

IT Teams

Security Service Providers (MSSPs)

Cybersecurity Professionals

Government Agencies

Small and Medium Enterprises (SMEs)