SMART INDIA HACKATHON 2024

SMART INDIA HACKATHON 2024

Team- TechCiphers

SMART INDIA
HACKATHON
2024

Team Member Details

Pavni AggarwaL - 2023UEE4669

Alan Sajith - 2023UCA1943

Kratika Sinha - 2023UBT1103

Rishav Shah - 2023UCS1543

Aakanksha - 2022UCI8060

Ayush Chauhan - 2023UIT3134

SMART INDIA HACKATHON 2024

Problem Statement ID – **1744**

Problem Statement Title**- Creating a cyber triage tool to streamline digital forensic investigation**

Theme- **Blockchain & Cybersecurity PS**

Category- **Software**

Team ID-

Team Name- **TechCiphers**

SMART INDIA HACKATHON 2024

Problem Statement

To design and develop an innovative digital forensics and incident response tool with an intuitive interface that streamlines importing evidence, automated analysis, and detailed report generation. The tool should support:

- Automated data collection from forensic images and other formats.
- Automated scanning and analysis of files, system logs, registry entries, and network activity.
- Identification of indicators of compromise (IOCs) and suspicious activities
- AI/ML-driven anomaly detection with a scoring system and recommendation engine.
- User-friendly review options with interactive timelines, graphical summaries, and exportable reports in formats like PDF, JSON, and CSV.

Need of the Solution

- As the number of cases increase, **streamlining evidence import**, **automating analysis**, and efficiently generating reports is vital to **saving manpower and time** .
- Real-time **data visualization** is essential in digital forensics for quick insights and **faster decision-making.**
- **Machine Learning** will help **anomalies** and prioritize the most important evidence, making the investigation easier and faster.
- Review of the evidence using interactive visuals, like timelines, and **generate detailed reports** that can be exported in different formats (like **PDF** or **CSV**).
- Integrating **Artificial Intelligence** and **Blockchain** for identifying and **flagging** known **cyberattack patterns** or behaviors, ensuring enhanced security.

TECHNICAL APPROACH

- Develop an **AI-driven cyber triage tool** that **automates** key tasks like data collection, **analysis**, and **reporting.**
- Implement **Machine Learning algorithms** to identify and **prioritize threats** based on severity, using **behavioral analysis** and **anomaly detection techniques**.
- Incorporate **real-time evidence management,** ensuring that all data is securely stored, indexed, and easily retrievable.
- Include **user-friendly dashboards** and **automated reporting features** to assist investigators in making informed decisions quickly, reducing manual workloads and investigation time.

TECHNOLOGY STACK

EVIDENCE REPORT

AUTOMATE DATA COLLECTION

IOC IDENTIFICATION AND SUSPICIOUS ACTIVITY DETECTION

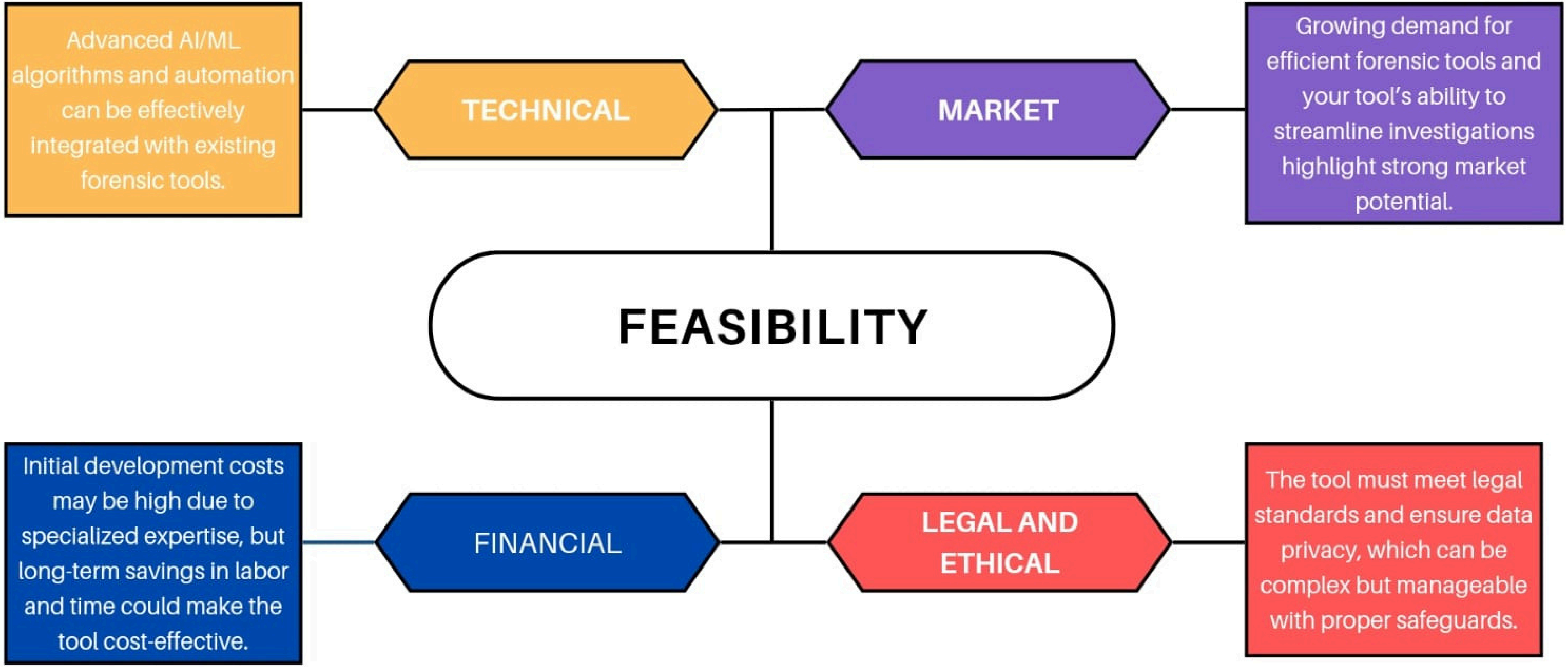
SCORING SYSTEM AND RECOMMENDATION SYSTEM

INTERACTIVE TIMELINES AND GRAPHICAL SUMMARIES

COMPREHENSIVE EXPORTING REPORTS

SMART INDIA
HACKATHON
2024

FEASIBILITY OF THE IDEA



FEASIBILITY

TECHNICAL

Advanced AI/ML algorithms and automation can be effectively integrated with existing forensic tools.

MARKET

Growing demand for efficient forensic tools and your tool's ability to streamline investigations highlight strong market potential.

FINANCIAL

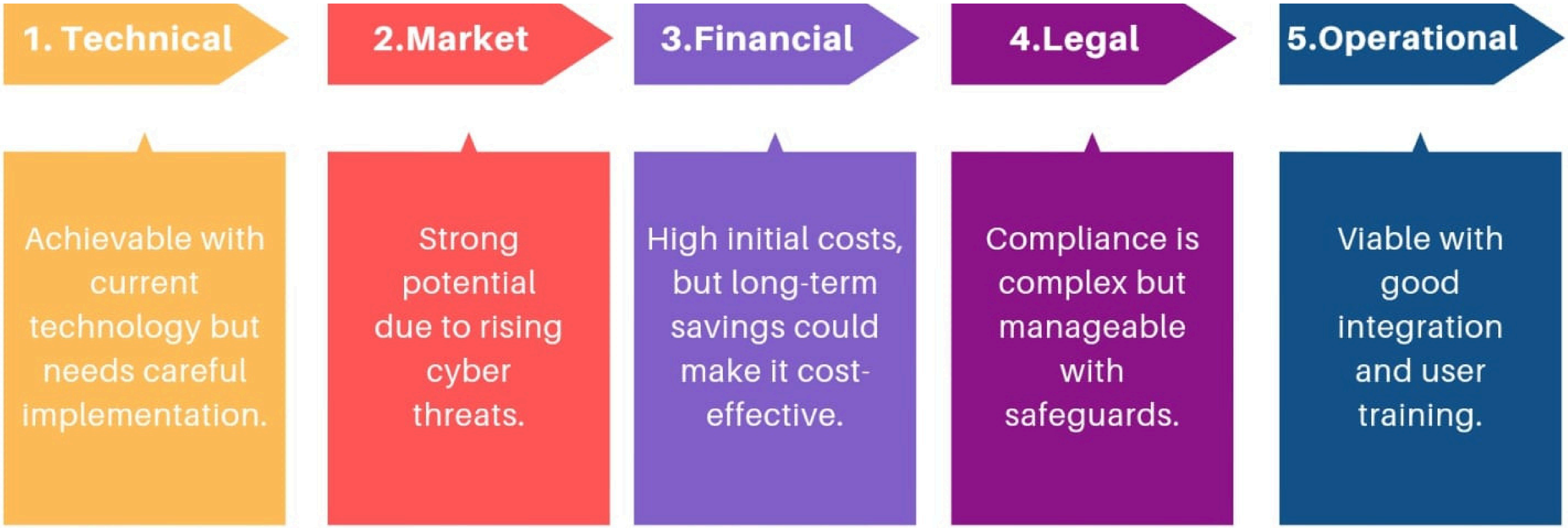
Initial development costs may be high due to specialized expertise, but long-term savings in labor and time could make the tool cost-effective.

LEGAL AND ETHICAL

The tool must meet legal standards and ensure data privacy, which can be complex but manageable with proper safeguards.

SMART INDIA HACKATHON 2024

VIABILITY OF THE IDEA



1. Technical

Achievable with current technology but needs careful implementation.

2.Market

Strong potential due to rising cyber threats.

3.Financial

High initial costs, but long-term savings could make it cost-effective.

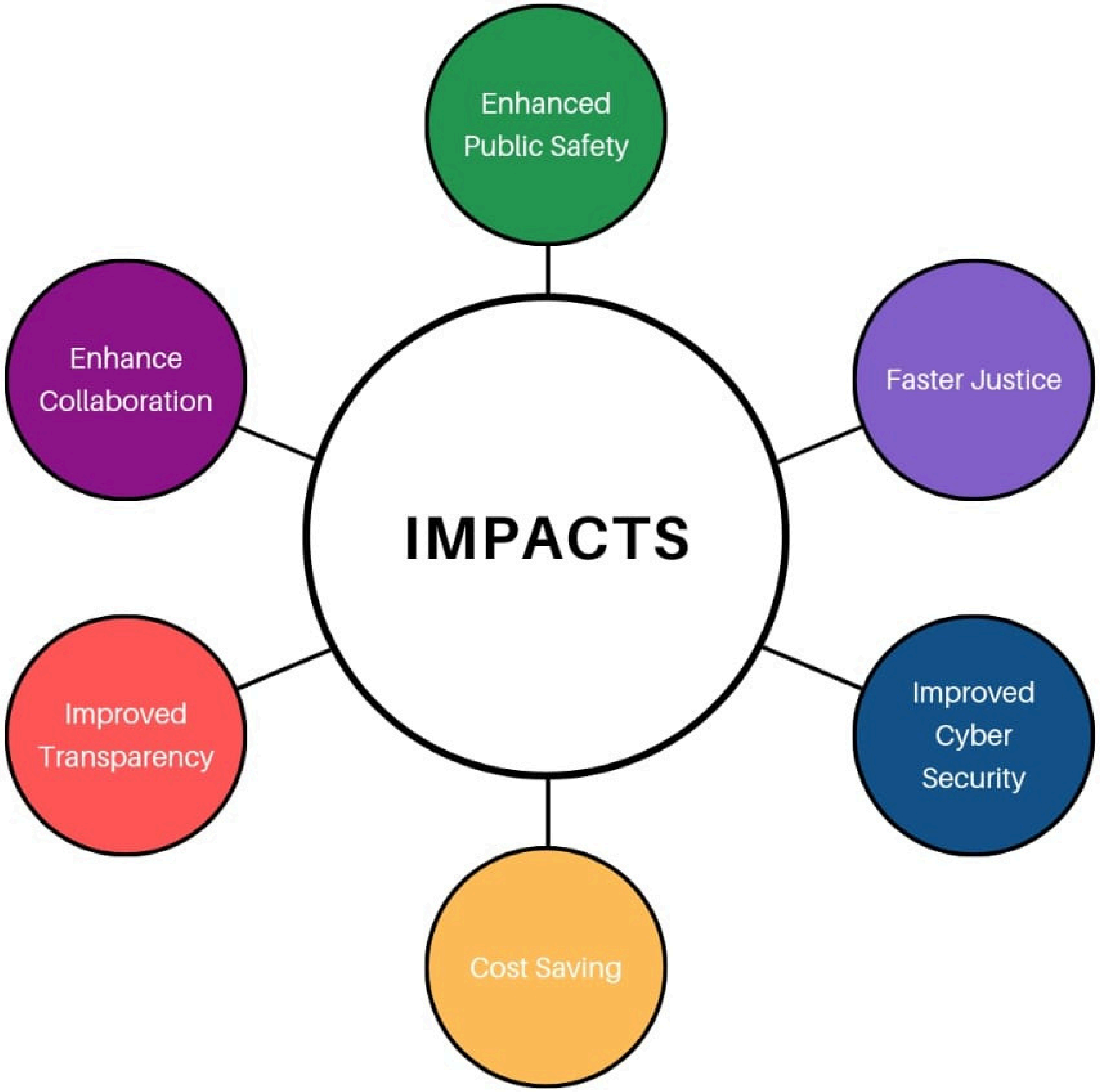
4.Legal

Compliance is complex but manageable with safeguards.

5.Operational

Viable with good integration and user training.

IMPACT AND BENEFITS



IMPACTS

Enhanced Public Safety

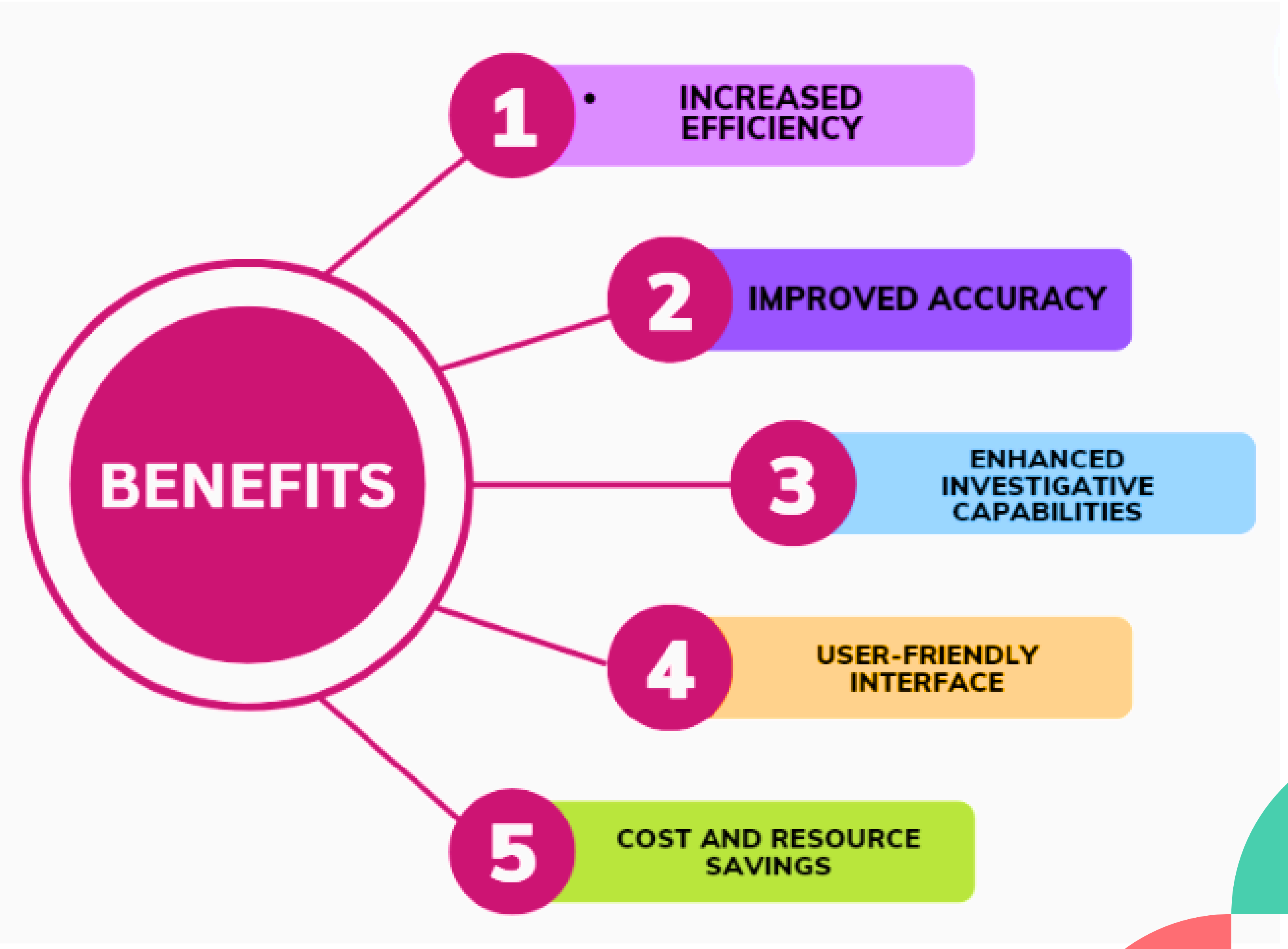
Faster Justice

Improved Cyber Security

Cost Saving

Improved Transparency

Enhance Collaboration



BENEFITS

1 INCREASED EFFICIENCY

2 IMPROVED ACCURACY

3 ENHANCED INVESTIGATIVE CAPABILITIES

4 USER-FRIENDLY INTERFACE

5 COST AND RESOURCE SAVINGS

BUISNESS MODEL

- Focus on key **sectors** like **law enforcement**, **corporate security**, **educational institutions** and **legal firms.**
- **Collaborate** with **cybersecurity firms** and consultants to reach a **broader audience**.
- Build **partnerships** with **government** and **private** sectors, offer free trials, participate in industry events, and provide strong support and maintenance.
- Offer **solutions** that scale with the **needs of the organization**, from small teams to large enterprises.
- **Affordable pricing**, localized features, user-friendly interface, and **comprehensive reporting capabilities.**