Cybercrime Victimisation Barometer (CYBBAR)

Conceptual tool for digital reporting of cyber incidents

Objectives

BOLSTER EU'S RESILIENCE AGAINST CYBER THREATS

DEEPEN UNDERSTANDING OF CYBERCRIME'S SCOPE

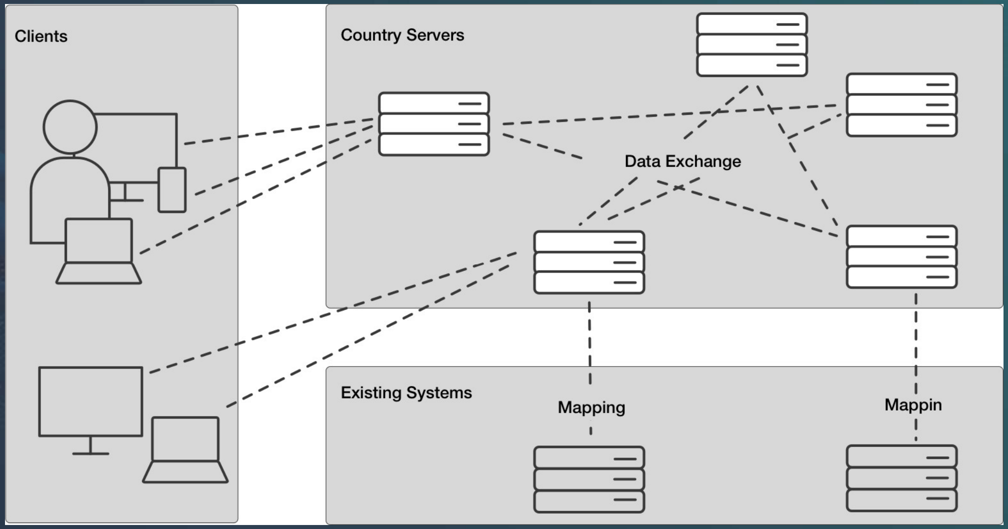
PROMOTE COLLABORATION BETWEEN LEAS AND PRIVATE ENTITIES

Beneficiaries

- National Law Enforcement Agencies
- EU agencies: ENISA, Europol
- Businesses and Citizens
- EU authorities and policymakers

Challenges

- Navigating international privacy laws
- Varying LEA methodologies
- Trust disparities among EU countries
- Motivation to use the reporting tool
- Compatibility with existing tools in EU member states



Technical Architecture

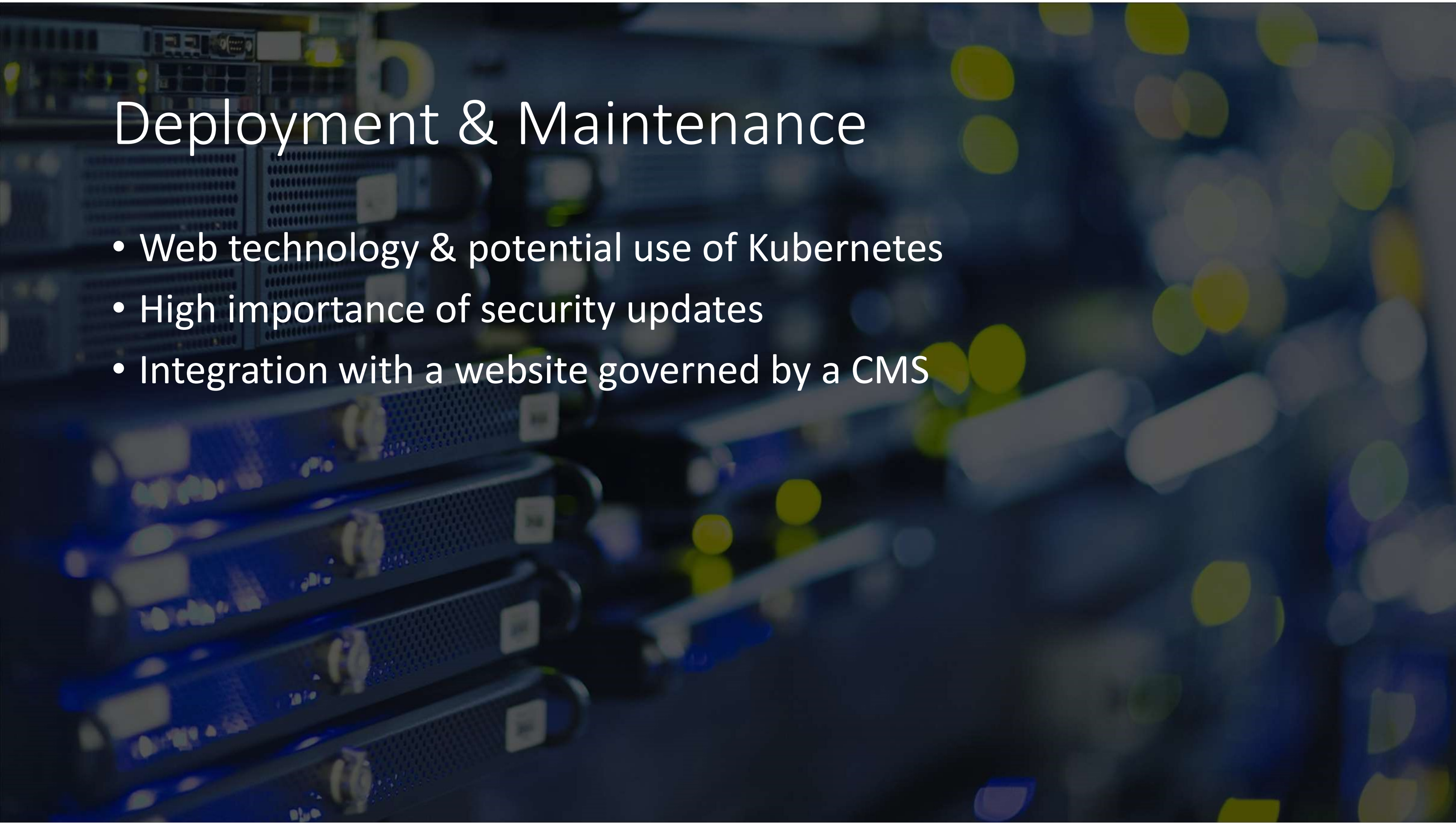
- Decentralized model: One server/country
- Selective data sharing & data uniqueness preservation
- Peer-to-peer synchronization of shared data

Open-source & Security

- Emphasis on open-source solutions
- Ensuring top-tier security measures
- Architectural measures & stringent policy rules
- Guard against cyber attacks & prevent sensitive data exchange

Development Approach

- Agile development process
- Active engagement of stakeholders
- Emphasis on prospective users' needs



Deployment & Maintenance

- Web technology & potential use of Kubernetes
- High importance of security updates
- Integration with a website governed by a CMS

Conclusion & Recommendations

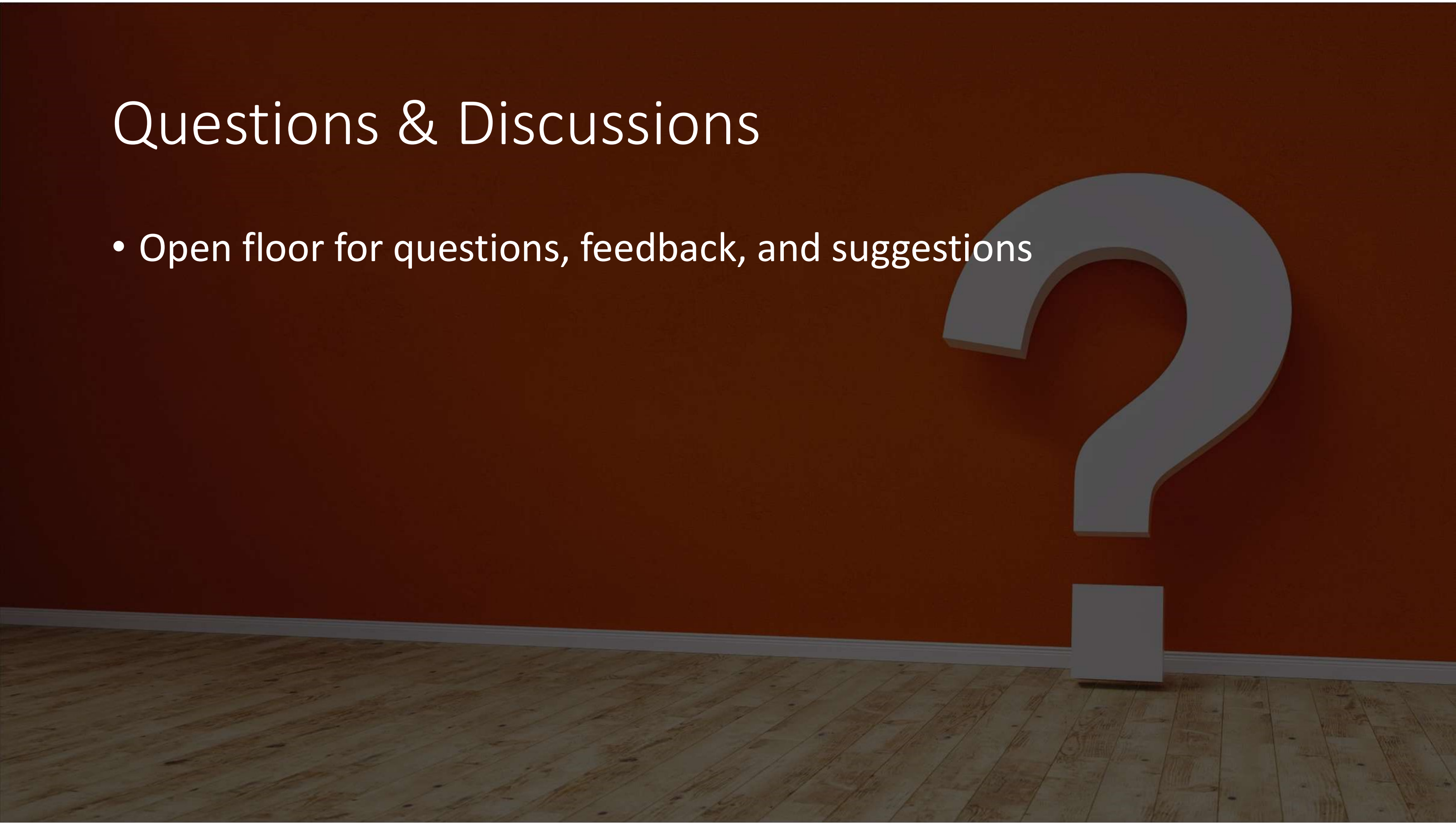
ADOPT A DECENTRALIZED, CUSTOMIZABLE APPROACH

FOCUS ON STAKEHOLDER ENGAGEMENT AND FEEDBACK

PRIORITIZE SECURITY AND REGULAR MAINTENANCE

The Digital Reporting Tool

- Link: https://cybbar.eu/reporting-tool/



Questions & Discussions

- Open floor for questions, feedback, and suggestions