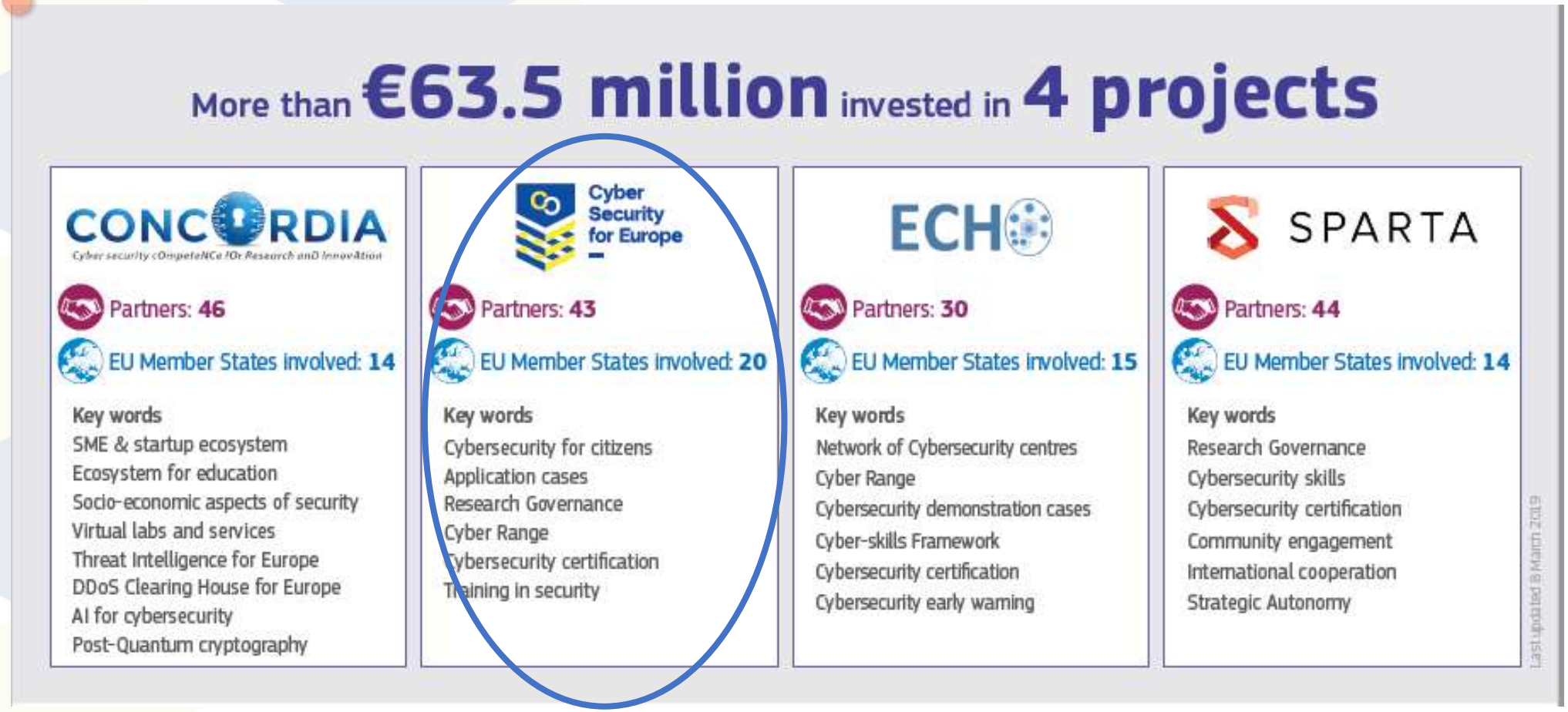
Cybersecurity

Horizon 2020 pilot projects

to prepare a European Cybersecurity Competence Network
& contribute to the European cybersecurity industrial strategy

Pierre-Henri CROS



CyberSec4Europe Overview

CyberSec4Europe will develop a governance model for the future European Cybersecurity Competence Network and will trial this model in several technology and innovation activities relevant for progressing Europe's cybersecurity capabilities, adopting a robust, evolutionary path based on five foundational pillars:

- Governance
- Cooperation
- Building future-oriented European capabilities
- EU leadership in cybersecurity innovation
- Supporting the complete industrial value chain

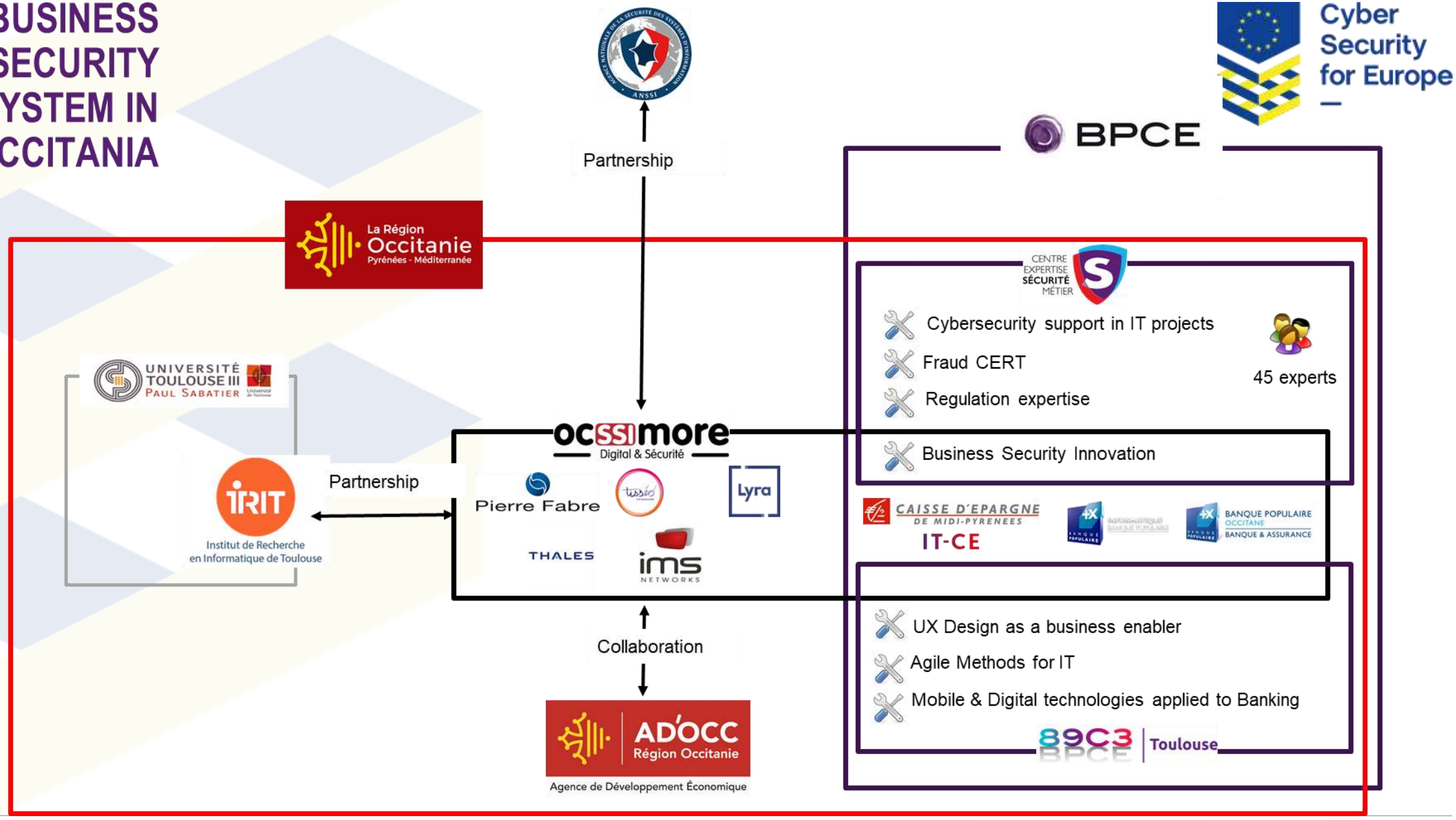
WP2: Governance Design and Pilot Tasks

- Assessing best governance practices
- Governance structure design
- Operation and testing of the governance structure
- Preparation for the future Cybersecurity Competence Network

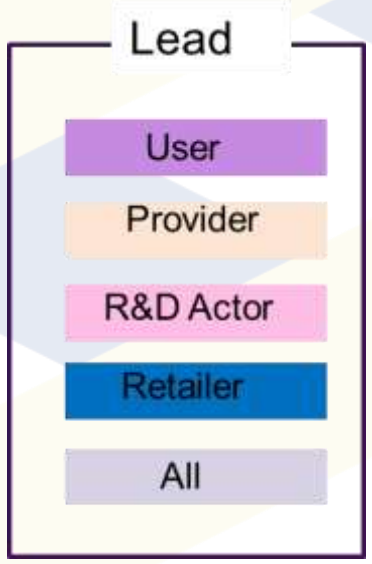
- **Task 2.4 Operation and Testing of the Governance Structure [M1-M36]**

Governance model V1.0 as described in D2.1 will be validated by applying the model to the regional cybersecurity expertise hub that is being established by **our partners in Toulouse**. The Toulouse hub will be **responsible for implementing the decision processes and policies proposed by the governance model**…… will be partially validated on a selection of cases from the Toulouse hub, as well as from others that may have been established by other partners in the meantime.

OUR BUSINESS SECURITY ECOSYSTEM IN OCCITANIA



POTENTIAL ACTIVITIES OF THE FUTURE CYBERSECURITY COMPTENCE CENTER



Identifying business innovation sources

- Backlog of user needs
- R&D breakthrough innovations

Demonstrating ROI on current and concrete use cases

- POC / Business Demonstrators
- Build & Test environments

Testing, Building and Validating appetence of target users

- Showrooms and specific events
- Publications/ white papers
- Field Trials

Designing the future product/service

Designing the sharing value model

Deploying widely Generating large adoption

Industrialization of participation to Europe's Cybersecurity call of proposals

- Distribution/Deployment networks
- Competence development / industrialization
- Business Model
- Contracting policies and intellectual property
- UX Design
- Product conception

Demonstration cases

- Finance and E-Commerce
- Supply Chain Security Assurance
- Privacy-preserving Identity Management
- Incident Reporting
- Maritime Transport
- e-Health and Medical Data Exchange
- Smart Cities

Incident reporting

The main problems and challenges identified by the stakeholders are:

- Lack of harmonised procedures
- Prove the efficiency of AI in cybersecurity events detection and incident responses
- Access to the information
- Facilitating the collection of incident and/or data leak
- Train people to manage security incidents
- Improve the economic model of CERT

Incident reporting

The main problems and challenges identified by the stakeholders are:

- Lack of harmonised procedures
- Prove the efficiency of AI in cybersecurity events detection and incident responses
- Access to the information
- Facilitating the collection of incident and/or data leak

- Train people to manage security incidents
  - Understand what constitutes a security incident, and what is not considered a security incident (e.g. spam, etc.).
  - Identify and correctly react to security incidents.
- Improve the economic model of CERT
  - Today, the economic model for sharing incident reports is based on a pricing system that is proportional to the wealth of information provided. This restricts the use of a full service to those who can pay for it.
  - SMEs should be supported, financially and from an organizational point of view (like a EU grant).

Thank you

pierre-henri.cros@irit.fr