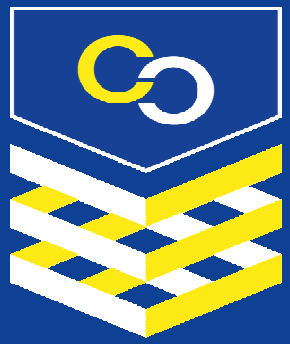


Cyber Security for Europe

EaP connect II CyberSecurity Workshop

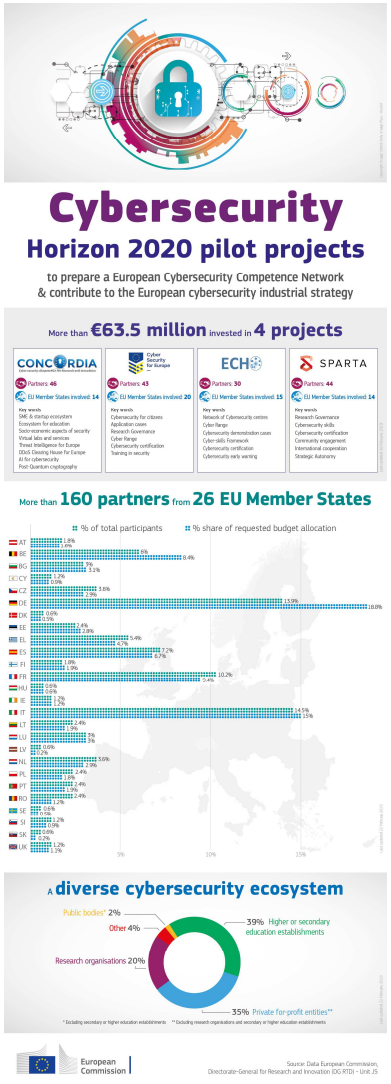
9-10 February 2022

Pierre-Henri Cros

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Working together towards a common objective



ECHO

CONCORDIA

SPARTA

Cyber Competence Network

Cyber Security for Europe

A European network of cybersecurity centres of excellence

Changing Europe' cybersecurity research and innovation landscape

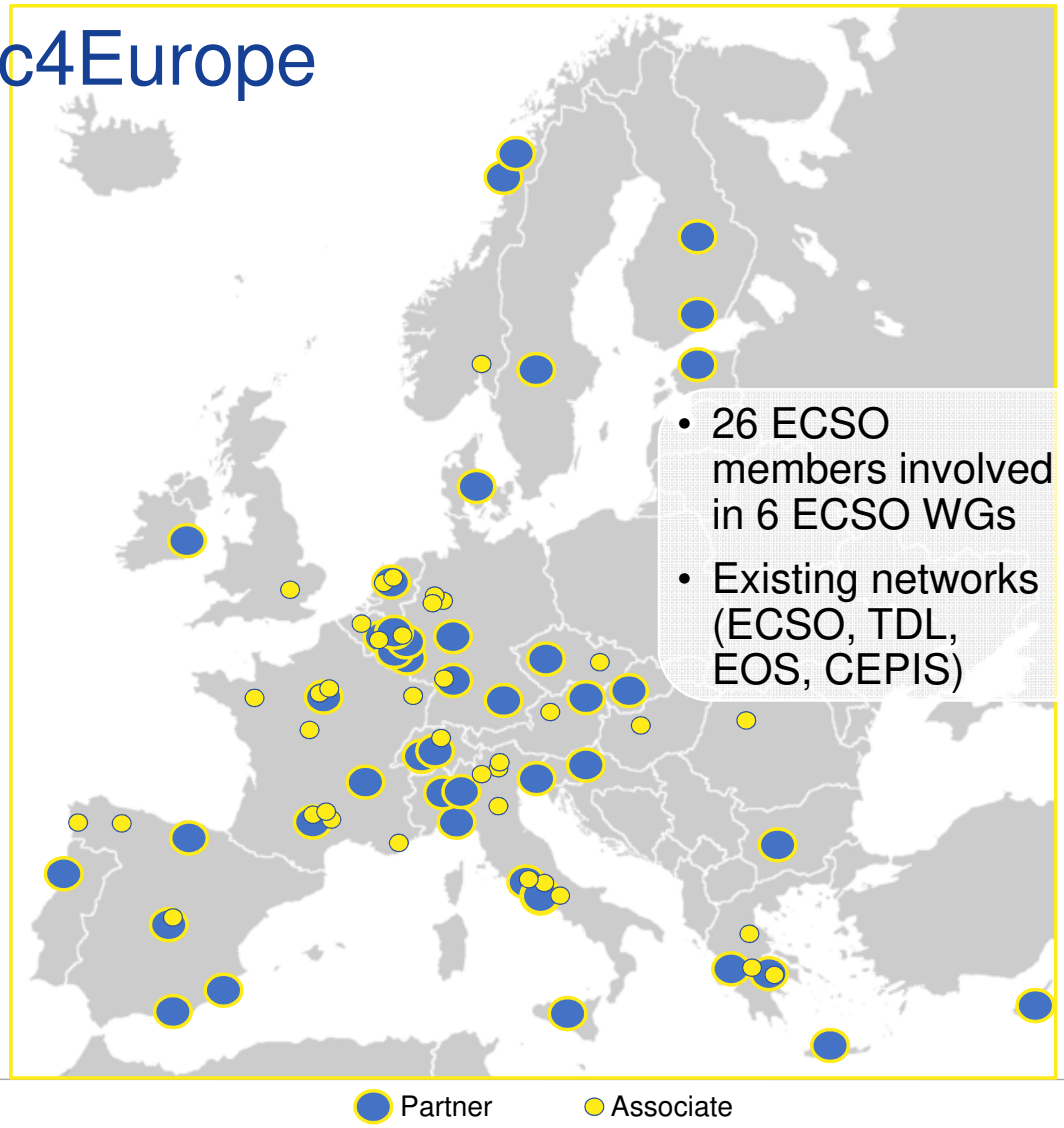
Cyber Security for Europe

Strong academic performers
Insufficient critical mass

Intensified partnerships
World-leading capacities

Who Are CyberSec4Europe

- Centres of Excellence / Universities / Research Centres / Enterprises (small and larger)
- 43 members in 22 countries
- 40 associates in 16 countries
- 11 technology/application elements and coverage of nine vertical sectors
- Experience from over 100 cybersecurity projects in 14 key cyber domains
- Funding period: 02/2019 – 07/2022



Consortium Participants

Project Lead

Goethe University Frankfurt (DE)

WP Leaders

TU Delft (NL)

University of Murcia (ES)

FORTH (EL)

NEC Labs Europe (DE)

Trento University (IT)

Masaryk University Brno (CZ)

Cybernetica (EE)

Trust in Digital Life (BE)

Conceptivity (CH)

Associates

Inclusion during the project

Partners

ABI Lab (IT)

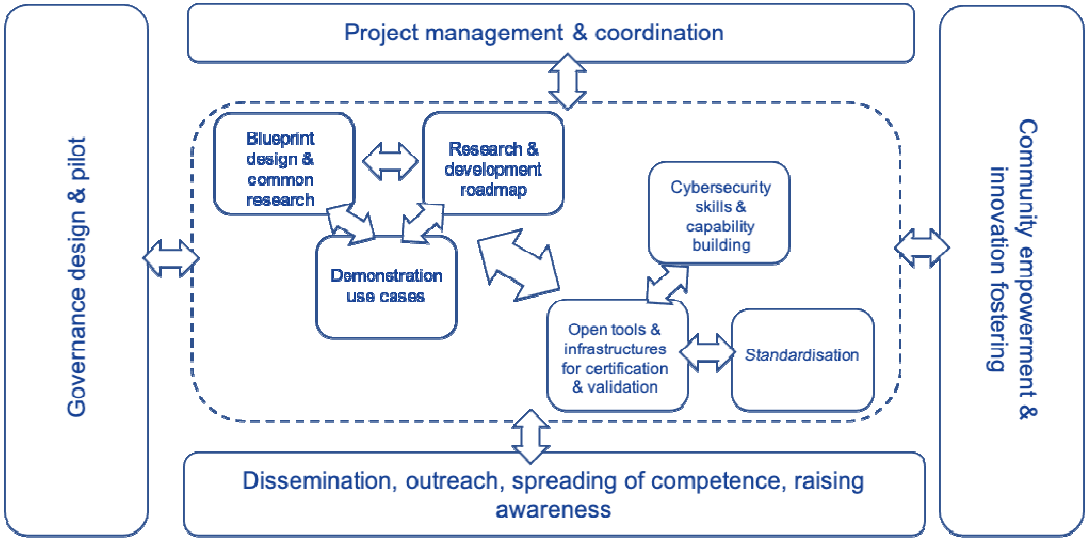
AIT (AT)

Archimede Solutions (CH)

ATOS Spain (ES)

Banco Bilbao Argentaria (ES)
University Porto (PT)
CNR (IT)
CTI “Diophantus” Patras (EL)
DAWEX (FR)
Denmark Technical University (DK)
Engineering Spa (IT)
Comune di Genova (IT)
Banque Populaire (FR)
International Cyber Investigation Training Academy (BG)
Intesa Sanpaolo (IT)
JAMK University of Applied Sciences (FI)
Karlstad University (SE)
KU Leuven (BE)
Norwegian University of Science and Technology (NO)
Open & Agile Smart Cities (BE)
Politecnico de Torino (IT)
Siemens AG (DE)
SINTEF (NO)
Time.Lex (BE)
University College Dublin (LERO) (IE)
University of Cyprus (CY)
University of Maribor (SI)
University of Malaga (ES)
University of Luxembourg (LU)
University of Piraeus (EL)
Université Paul Sabatier Toulouse (UPS-IRIT) (FR)
VaF (SK)
VTT (FI)

What is CyberSec4Europe?



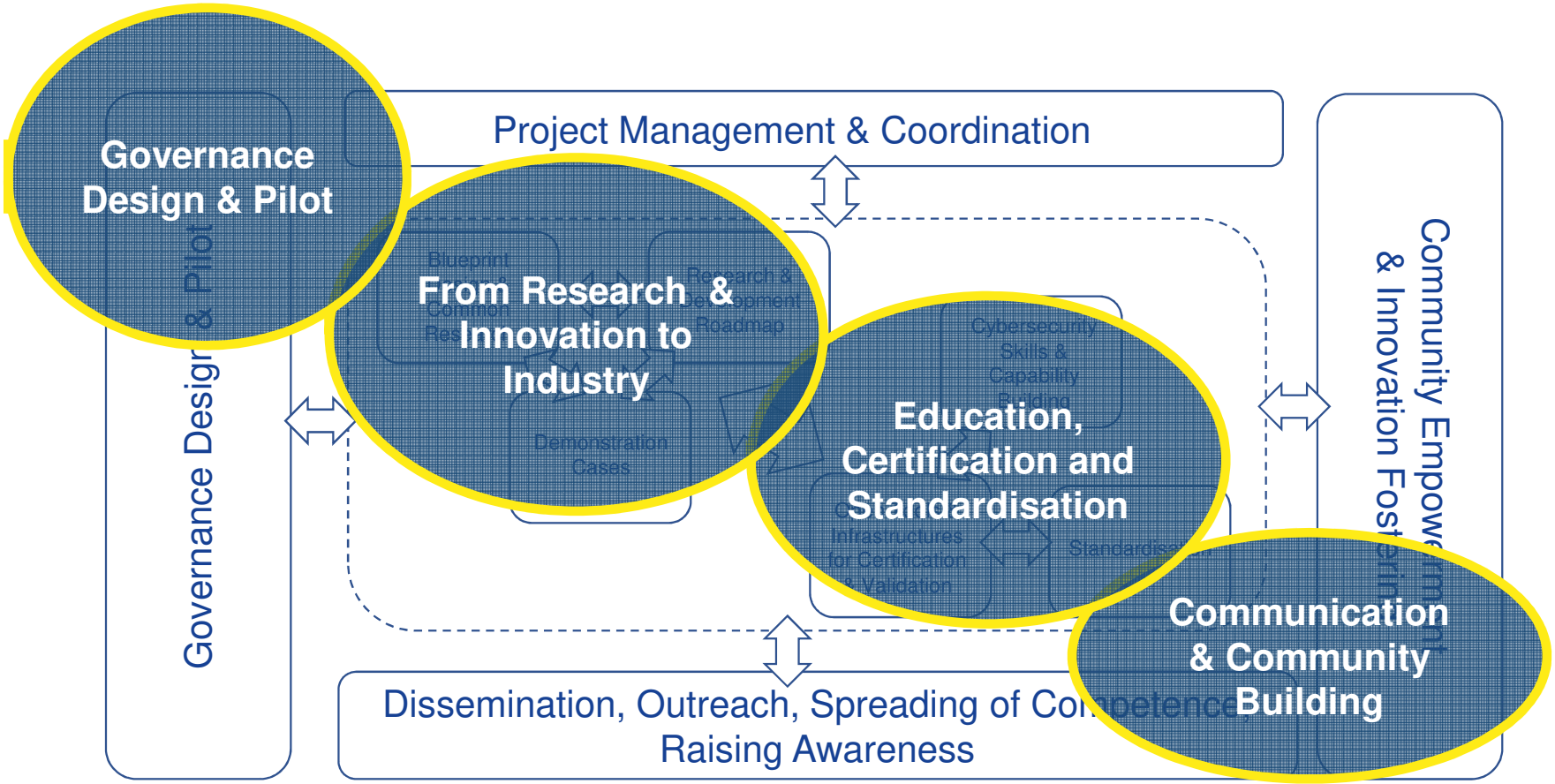
- Ensure the adequacy and availability of cybersecurity education and training as well as common open standards
- Communicate widely and build communities

CyberSec4Europe is a research-based consortium working across four different but inter-related areas with a strong focus on openness and citizen-centricity in order to:

- Pilot a European Cybersecurity Competence Network
- Design, test and demonstrate potential governance structures for the network of competence centres
- Harmonise the journey from software componentry identified by a set of roadmaps leading to recommendations

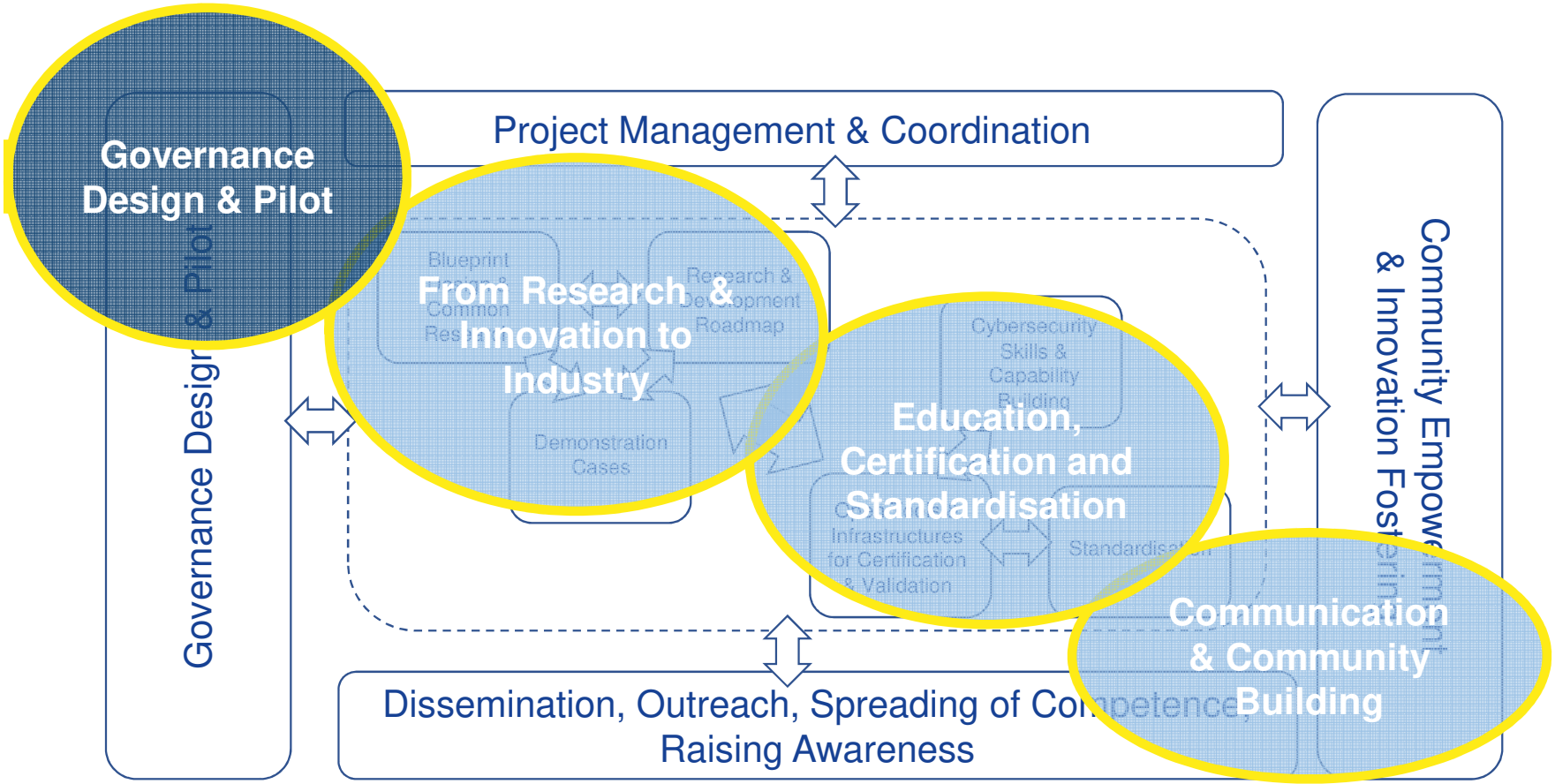
Project Architecture

Cyber Security for Europe



Project Architecture

Cyber Security for Europe



Pillar I: Governance, Design & Pilot (WP2)

Cyber Security for Europe

Goal:

- WP2, within Pillar I, aims to design a governance model based on the ambition to give the cybersecurity research community a common European goal.

Means:

- Validation of the assumptions on the governance structure in D2.2
- Further development of the governance model in D2.3
- **Research into the case studies of establishment of CHECKs (France, Spain) and the role of touching points in the European cybersecurity ecosystem development**
- Up-to-date and ongoing legal analysis and interpretation of the Regulation (proposal) and other relevant high-level legislature and legal requirements, ensuring a holistic approach to the governance design process
- Cross-pilot Governance Coordination Group

Solution: CHECKs (Community Hubs of Expertise and Cybersecurity Knowledge)

We developed and started testing a bottom-up governance structure that has the potential to address urgent cybersecurity challenges through capitalising on the community-derived capabilities and ensuring robust cooperation.

Cyber Security for Europe

IRIT 30 ans 1990-2020

CHECK-T

1er NOEUD du réseau européen DE CYBERSECURITE

dans le cadre du projet pilote

CyberSec4Europe

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

Université Fédérale Toulouse Midi-Pyrénées

UFTMIP - CM du 24 Juillet 2020

Objectif

Develop the conditions for the creation of the 1st node of the future European CHECK-T network

CHECK-T (**Community Hubs of Expertise and Cybersecurity Knowledge of a Territory)** should enable its members to :

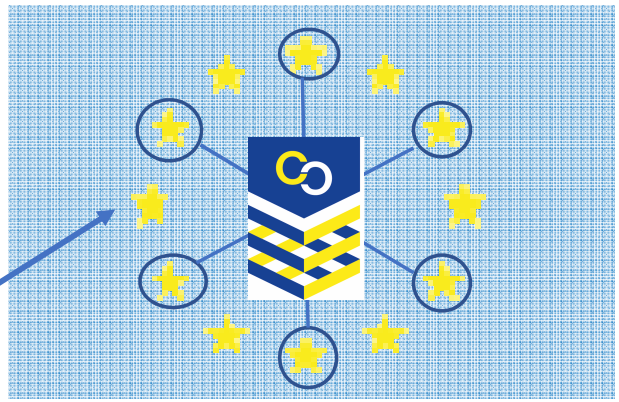
- Obtain human and financial resources to develop innovative projects
- To accompany the rise in skills of all by a personalised watch
- Become visible and credible on their high levels of expertise
- Anticipate and influence political interventions at national and European level

Two workshops have been set up:

1- Consult the public and private communities of a territory that are concerned by cybersecurity on the needs and expectations expressed.

2- Identify the governance structure that will allow them to work together on a roadmap.

Vision: CHECK-T and its context



Funding of European projects

Services

Skills development

ROI, Access to new markets / partnerships

End users (large groups, SMEs / Startups, citizens' groups

Demande

Offer

Shows the value

Facilite

CHECK-T

Use cases, Demonstrators, Simulation platforms

node of the network

Connect

Investors / financing actors

Connect

Eco Development Actors
Poles and Clusters, Dev. Eco Agencies, Local Authorities...

Poles and Clusters, Economic Development Agency, Local Authorities

Facilite

Technology Centres, Solution Providers

Technical Solution Providers

CHECK-T

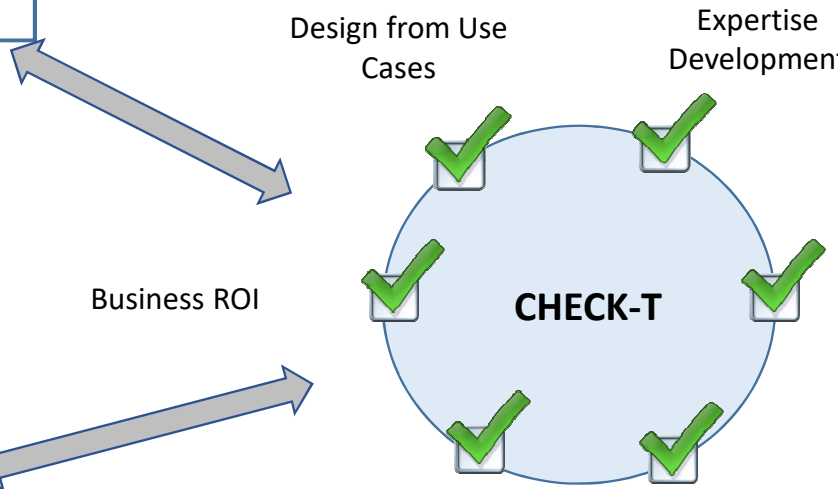
Bringing together the competences of a territory around cybersecurity needs and expectations

Cyber Security for Europe

Cybersecurity end-users

Essential sectors (Transport, Finance, Health, Energy, Agri-Agro...)

Cybersecurity Solution Providers
Experts in Cyber Security, Experts in Digital Transformation and Security



Economic development accelerators
Local authorities, Economic Development Agencies, Competitiveness Clusters, Thematic Associations...

Technology Centres
Academic and industrial research laboratories, higher education, Continuing Education

Methodology (1)

Elicit cybersecurity needs and expectations

Interview campaign with 50 stakeholders from 4 communities

Method :

- Production of a presentation to guide the interviews
- Selection of method to capture expectations
- Drawing up a list of prospects
- Conducting interviews
- Processing and analysing the information collected
- Integration of proposals into an interaction matrix
- Presentation at a plenary meeting involving all interviewees

Methodology (2)

Reminder of the questions :

1- In which community would you like to invest yourself in priority?

- Cybersecurity Users College: industry players (transport, health, energy, etc.)
- Technology Centre College: Research, Development & Innovation players, research and academic laboratories
- Industry College: Cybersecurity service providers, SOC
- Economic Development College: institutional and economic development players.

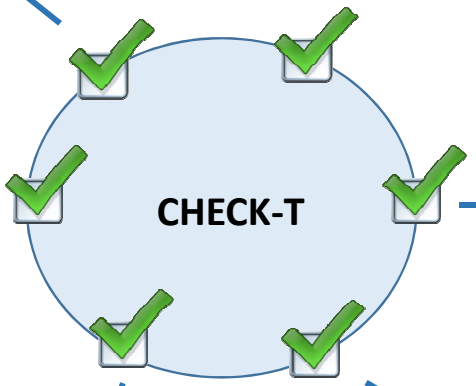
2 - For each mission :

Imagine, with regard to your activity, the potential that you will be able to draw thanks to the community to achieve your objectives and face the pressure of performance

Express the benefits expected from contributing to the platform in terms of :

- Convenience: funding, infrastructure, etc.
- Reach: market access, new partners...
- Value gain

Synthèse des besoins et attentes



Conception à partir de Cas d'Usages

- Thématiques et Capture des exigences
  - Anoymisation, RGPD
  - Cloud
  - Identité Digitale
  - Lutte contre les fraudes
  - …
- Réseautage
  - Prospective (nouveaux marchés, nouveaux métiers…)
  - Veille
  - Ateliers et conférences Expert
- ROI, Accès marché
  - Nouveaux partenariats
  - Nouvelles relations d'affaires
  - Co-innovation (produit/service)
- Opportunités de financement
  - Projets de R&D&I
  - Financement européen
  - Financement local complémentaire
  - Investisseurs (publics/privés)

ROI des entreprises

Développement d'Expertise

- Partage d'Information
  - Connaissance Cyber, threat intelligence
  - Etat de l'art
  - Interprétation des textes juridiques Cybersecurité
  - …
- Coopetition, alliances stratégiques sur des projets

Transfert d'Usages, Mutualisation de Coûts de R&D&I

- Partage d'Information
  - Cross-fonction /problèmes cross-filières
  - Capitalisation d'expériences, déploiement de processus /méthodes
  - Benchmark de fournisseurs de solutions

Leadership Technologique

- Lobbying
  - Influence de la feuille de route européenne en Cybersecurité
  - Influence auprès des autorités politiques nationales
  - Développement de crédibilité et de légitimité via un Label CHECK-T
- Montée en compétences
  - Identification/Prospection (stages, alternance, thèses etc.)
  - Nouveaux modules de formations adaptés aux besoins en emplois

Construction de la Confiance

- Cadre éthique de coopération
  - Charte commune / NDA
  - Règlement intérieur
  - Benchmark juridique
  - Gestion de la propriété intellectuelle

Partners

Arterris	Continental	Atos
Banque Postale	BPOC	Institut de droit privé
EasyMile	Cemoi	LAAS / INSA
IDETCOM	Collins Aerospace	Epitech
IMS Network	Thales Group	AD'OCC (Cyber'Occ)
Pôle Optitec	Apsys Airbus	MIPIH
Thales Group	Pole Star	SOCODIT
Pôle EuroBioMed	Sogeti Cap Gemini	Digital 113
Great X	CGI	CNES
BoostAeroSpace	Pierre Fabre	Tisseo DIH Move2Digital
Orange CyberDefense	Sopra Steria	
Pôle AgriSOI	IBP	
LAAS / INSA	Occitanie Data	
Pôle Aerospace Valley	Lyra Network	

With the support of:
ANSSI – Délégation Occitanie
DISSE Occitanie (rattaché au SGAR et à la DIRECCTE)
Région Occitanie, Toulouse Métropole

A first milestone in the implementation of CHECK-T

L'Institut de Cybersécurité d'Occitanie (ICO)

The ICO focusses on Research and Development, having at its core the three leading labs in Occitanie, namely IRIT, LAAS, and LIRMM.

It's primarily academic, with strong links to the industrial ecosystems nurtured by the composing labs. Its initial funding is majorly public and invites partnerships with private actors for the co-funding of research positions like PhD students and post-docs.

The ICO will participate in the implementation of Check-T and the inclusion of our territory in the European cybersecurity competence network.

Université Fédérale
Toulouse Midi-Pyrénées

Lessons learned and being learned: Participation and trust essential

Synergy between **top-down** and **bottom-up** structures
→ **integrating stakeholder** groups (**including citizens**)
→ efficient stakeholder **engagement** on **all societal levels**

- Industry groups, local governments, CERTs → not all the same level of formality as representatives of the EC and Member States
- May be different per country (so regulation must allow this, e.g. sectoral vs regional)

Key elements of **trust** into an **organisation**

- Secured participation
- Organisational transparency

Agile, trustful, and **lively exchange** in and between **Cybersecurity Communities**

Summary

- CyberSec4Europe is a **vibrant pilot community.**
- **Agile** to spontaneous EU requests – contributions to EC strategy and JRC Atlas cybersecurity roadmap
- Spearheaded the design of **a distributed governance model**
- Progressed research and research planning based on **real** application requirements
- Progressed education, certification and standardization initiatives
- Integrated **all** pilots and ECSO in a single **comprehensive event**:
  - **CONVERGENCE NEXT, 1-3 June 2022 Brussels, hybrid**
- Intensive *contribution* to and interaction with **ECSO**
- Implemented **principles** in **practice**

Cyber Security for Europe

Thank you!

pierre-henri.cros@univ-toulouse.fr

cybersec4europe.eu