REWIRE

CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE

Speaker/Presenter: Julia Sánchez Rodriguez

Role in the Organisation: Undergraduate Program Coordinator and Researcher

Organisation: La Salle BCN - URL

ENISA Cybersecurity Skills Conference

Athens, 20-21 September 2022

ABOUT REWIRE PROJECT

- The REWIRE Alliance represents more than **160 partners** from the four pilot projects (i.e. SPARTA, ECHO, CONCORDIA, CyberSec4Europe) and EU entities and organisations, including big companies, SMEs, universities and cybersecurity research institutes, from **26 EU Member States**

- The **project aims** to provide concrete recommendations and solutions that would lead to the **reduction of skill gaps** between industry requirements and sectoral training provision and **contribute to support growth, innovation and competitiveness** in the field of Cybersecurity

- The partnership **objective** is to work together for developing a new sectoral **strategic approach** to cooperate on cybersecurity skills, and support a **better matching between skill needs** of the market **and skills provided** by the relevant education and training organisations

RESULTS OVERVIEW (I)

- **EUROPEAN CYBERSECURITY BLUEPRINT**
  - Address skills gaps in the cybersecurity sector
- **CYBER RANGE PLATFORM**
  - Based on **open-source components** with the following elements and features:
    - Range platform which provides **machine, container and network virtualisation** with an option to use public cloud infrastructure
    - **Orchestration capabilities** for scenario provisioning and automated, semi-automated or manual scenario execution
    - Components and tools for more **realistic and automated scenario execution**: traffic generator, attack generator, event detector
    - Management interface and **dashboard**
    - Infrastructure for conducting secure access
    - Allowance for baselined **documentation** for trainers and trainees
    - **Ability for scenario packaging** in order to enable standardised scenario building and exchange

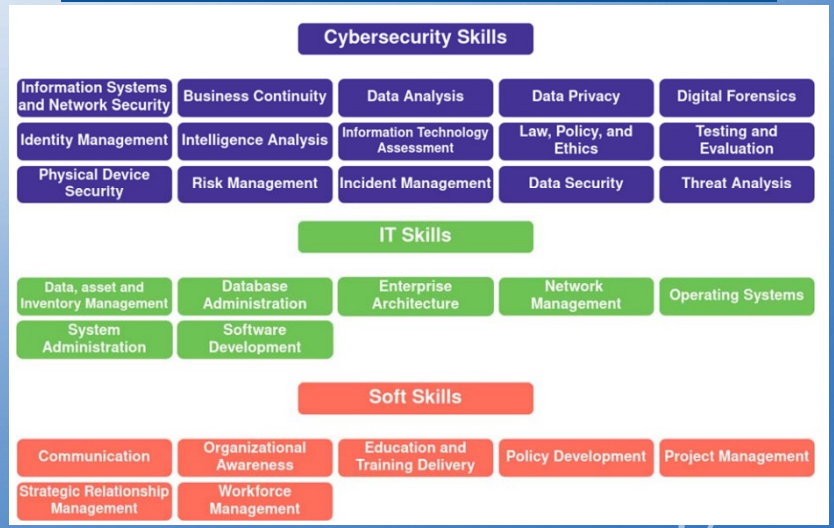
RESULTS OVERVIEW (II)

- **CERTIFICATION SCHEMES**
  - Cover specific areas of cybersecurity following international best practices
  - Produce a core set of documentation covering the certification schemes' common points and procedures
- **CyberABILITY**
  - A digital on-line publicly accessible **European Cybersecurity Skills Digital Observatory** which will provide **up-to-date information** regarding the job market, competences, training courses, certification schemes and a career roadmap
- **ONLINE COURSES**
  - Offer trainings and relevant certification schemes on selected occupational profiles in the form of four VOOCs (Vocational Open Online Courses) based on the REWIRE Curricula and Training Framework
  - The VOOCs will be hosted in a tailor-made Virtual Learning Environment (VLE)

STATUS QUO AND EUROPEAN CYBERSECURITY SKILLS STRATEGY (WP2) (I)

- **PESTLE Analysis (R2.1.1)**
  - European- and Country-level point of view - Factors impacting cybersecurity education from 6 different angles
  - 31 different factors affecting cybersecurity education and skills development and areas to be addressed in the future
- **Cybersecurity Skills Needs Analysis (R2.2.2)**
  - Identifying cyber security skills needs is challenging due to **a lack of reliable sources of direct information and a lack of a unified terminology** across different industry sectors
  - Three methodologies for obtaining a high-level understanding of the cybersecurity skills needs
    - Global cybersecurity skills frameworks
    - Pilot projects
    - NLP (Natural Language Processing) model (job ads)
  - Approach allows to **automate the analysis of skills needs** and can be adjusted to include new skills
  - NIST NICE cybersecurity competencies framework can be exchanged for the **European Cybersecurity Skills Framework**

31 skills **based on the NICE framework**



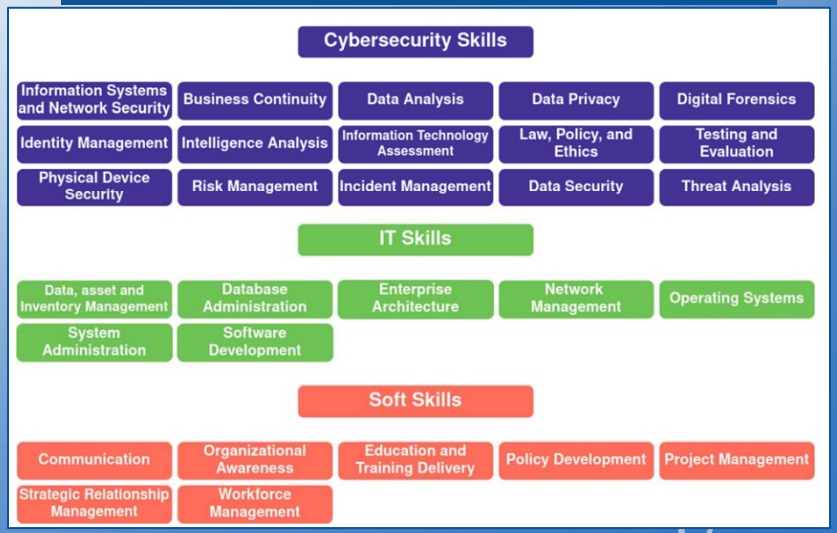
STATUS QUO AND EUROPEAN CYBERSECURITY SKILLS STRATEGY (WP2) (I)

- **PESTLE Analysis (R2.1.1)**
  - European- and Country-level point of view - Factors impacting cybersecurity education from 6 different angles
  - 31 different factors affecting cybersecurity education and skills development and areas to be addressed in the future
- **Cybersecurity Skills Needs Analysis (R2.2.2)**

Rank	Skill	Small dataset (Occurrence)	Medium dataset (Occurrence)
1	Communication	26	61
2	Information Systems and Network Security	20	52
3	Threat Analysis	24	50
4	Operating Systems	21	48
5	Data Security	23	46
6	Risk Management	18	46
7	Testing and Evaluation	18	45
8	Incident Management	18	44
9	Information Technology Assessment	20	41
10	Enterprise Architecture	15	36

liable sources of direct information

31 skills **based on the NICE framework**

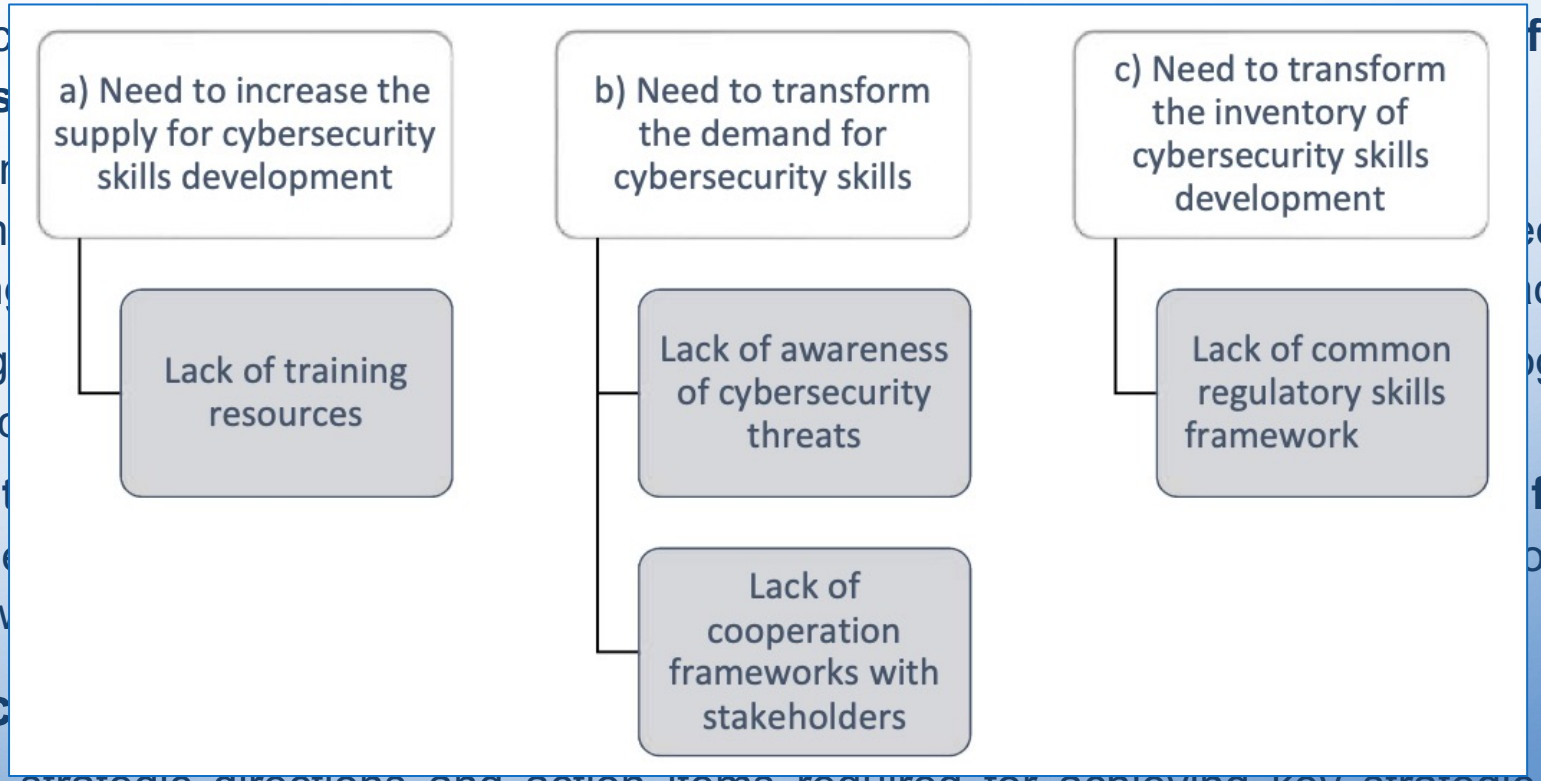


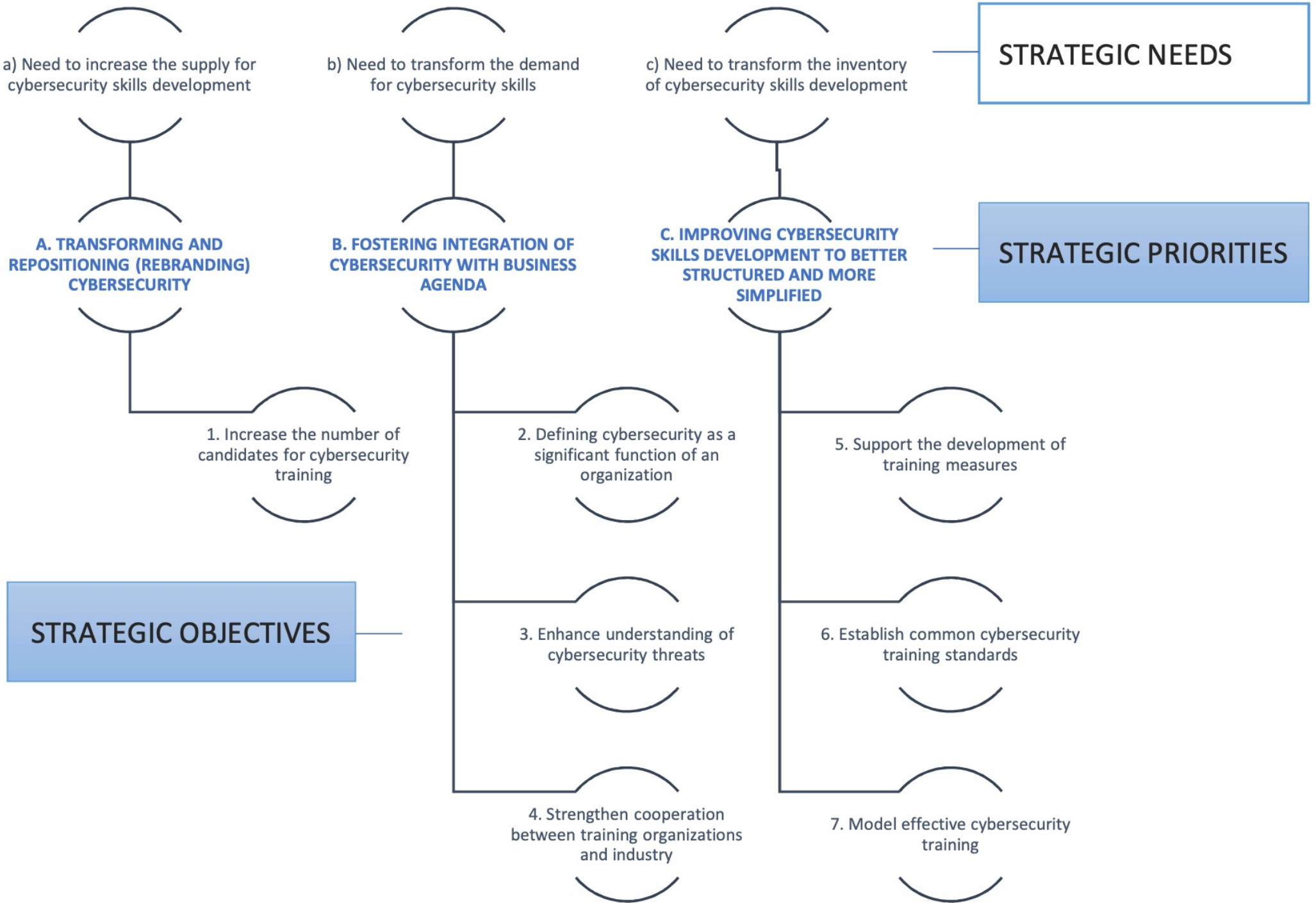
STATUS QUO AND EUROPEAN CYBERSECURITY SKILLS STRATEGY (WP2) (II)

- **Methodology to anticipate future needs (R2.2.3)**
  - Obstacles to the development of skills needs methodology → A **missing unified framework of cybersecurity roles and skills**
  - Combining **previous work** (4 pilots) with a newly created **stakeholder survey** (market view from industry and educational institutions) and **automated job ads analysis** based on machine learning, methodology for anticipating future needs will also be adjusted to reflect actual needs
  - Having a **shared vision** is essential to develop long-lasting model and methodology to forecast future cybersecurity skills needs
  - **Essential element → Co-operation with ENISA in the development of a unified framework** of cybersecurity roles and skills and ensuring aligning of future research based on the unified framework
- **Cybersecurity Skills Strategy (R2.3.1)**
  - Define strategic directions and action items required for achieving key strategic objectives in order to address skills demand and foster supply in the cybersecurity field

STATUS QUO AND EUROPEAN CYBERSECURITY SKILLS STRATEGY (WP2) (II)

- **Methodology to anticipate future needs (R2.2.3)**
  - Obstac… **framework of cybers…**
  - Combi… (market view from in… …d on machine learnin… …ctual needs
  - Having… …gy to forecast future …
  - **Essent… framework** of cyberse… …on the unified framew…
- **Cybersec…**
  - Define strategic directions and action items required for achieving key strategic objectives in order to address skills demand and foster supply in the cybersecurity field




a) Need to increase the supply for cybersecurity skills development
b) Need to transform the demand for cybersecurity skills
c) Need to transform the inventory of cybersecurity skills development
STRATEGIC NEEDS
A. TRANSFORMING AND REPOSITIONING (REBRANDING) CYBERSECURITY
B. FOSTERING INTEGRATION OF CYBERSECURITY WITH BUSINESS AGENDA
C. IMPROVING CYBERSECURITY SKILLS DEVELOPMENT TO BETTER STRUCTURED AND MORE SIMPLIFIED
STRATEGIC PRIORITIES
1. Increase the number of candidates for cybersecurity training
2. Defining cybersecurity as a significant function of an organization
5. Support the development of training measures
STRATEGIC OBJECTIVES
3. Enhance understanding of cybersecurity threats
6. Establish common cybersecurity training standards
4. Strengthen cooperation between training organizations and industry
7. Model effective cybersecurity training

DESIGN OF THE EUROPEAN CYBERSECURITY BLUEPRINT (WP3) (I)

R3.3.1. Cybersecurity Skills Framework

The REWIRE project plans to release shortly the R3.3.1. Deliverable, that describes the activities carried out from the project partners regarding the ECSF v.0.5.

The deliverable provides:

- Definitions (in relation to the ECSF)
- The methodology followed to identify Role Profiles (to be included in the ECSF)
- The methodology followed to make suggestions and improvements on the contents of the Role Profiles
- A proposal on the structure of the Roles and on the way to express the Tasks | Skills | Knowledge

DESIGN OF THE EUROPEAN CYBERSECURITY BLUEPRINT (WP3) (II)

Further work

R3.4.1 Mapping the framework to existing courses and schemes

This deliverable describes the method and results of the work performed by the project to map courses and certificates (skills) to the roles of the ECSF.

R3.5.1. Cybersecurity career pathway analysis

This deliverable describes the method and results of the work performed by the project to correlate the roles of the ECSF.

Both of these deliverables represent key inputs in the design of the **CyberABILITY platform**.

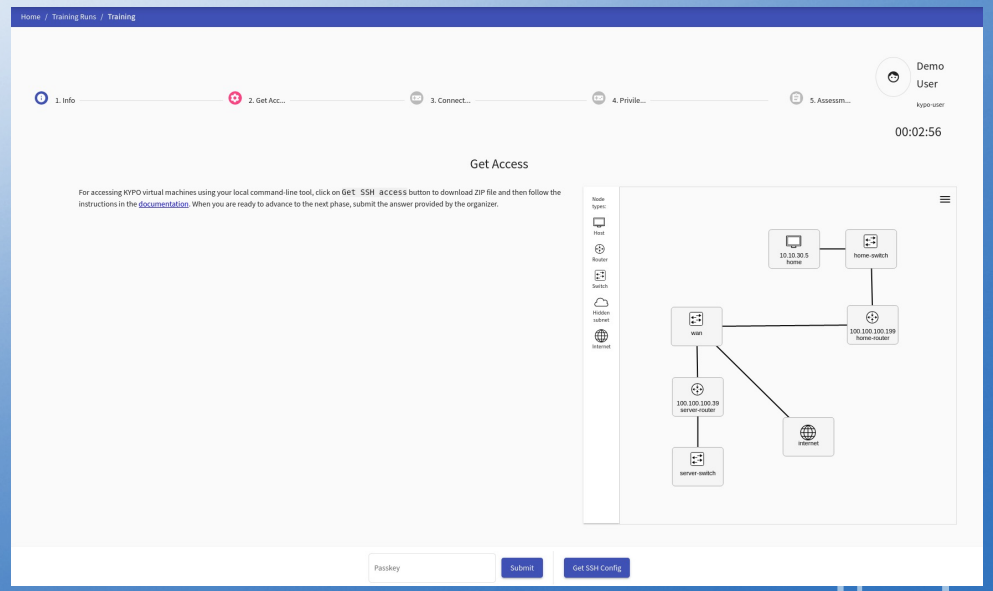
TOOLS DIRECTLY CONNECTED TO EDUCATION, TRAINING AND CERTIFICATION (WP4)

- **Setting up a Cyber Range**
  - **Methodology and Roadmap (R4.1.1, release available in November)**
    - From partners and pilot projects experience
    - Roadmap for the design, implementation and maintenance of a cyber range
  - **REWIRE Cyber Range (R.4.2, implemented by Feb 2023)**
    - Open-source components to make the design, exchange and implementation of cyber-exercises affordable

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

KYPO Cyber Range Platform

MUNI CERIT FI



FURTHER WORK

- **Design and development of the REWIRE Curricula and Training Framework**
  - Cybersecurity Skills Framework – 4 occupational profiles (training and validation mechanisms)
- **Scenario Sharing Platform**
- **Development of the REWIRE Virtual Learning Environment (VLE)**
- **Cybersecurity VOOCs delivery** (2 rounds, 3 month-long courses)
- **Design of Certification Schemes for Selected Cybersecurity Profiles**
  - Qualification Standards
  - Examination material
- **CyberABILITY Platform**

THANK YOU

More information:
https://rewireproject.eu/

Speaker/Presenter: Julia Sánchez Rodríguez

Role in the Organisation: Undergraduate Program Coordinator and Researcher

Organisation, Country: La Salle BCN – URL, Spain

E-mail address: j.sanchez@salle.url.edu

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE

REWIRE
CYBERSECURITY SKILLS ALLIANCE

AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B

Co-funded by the Erasmus+ Programme of the European Union