REWIRE

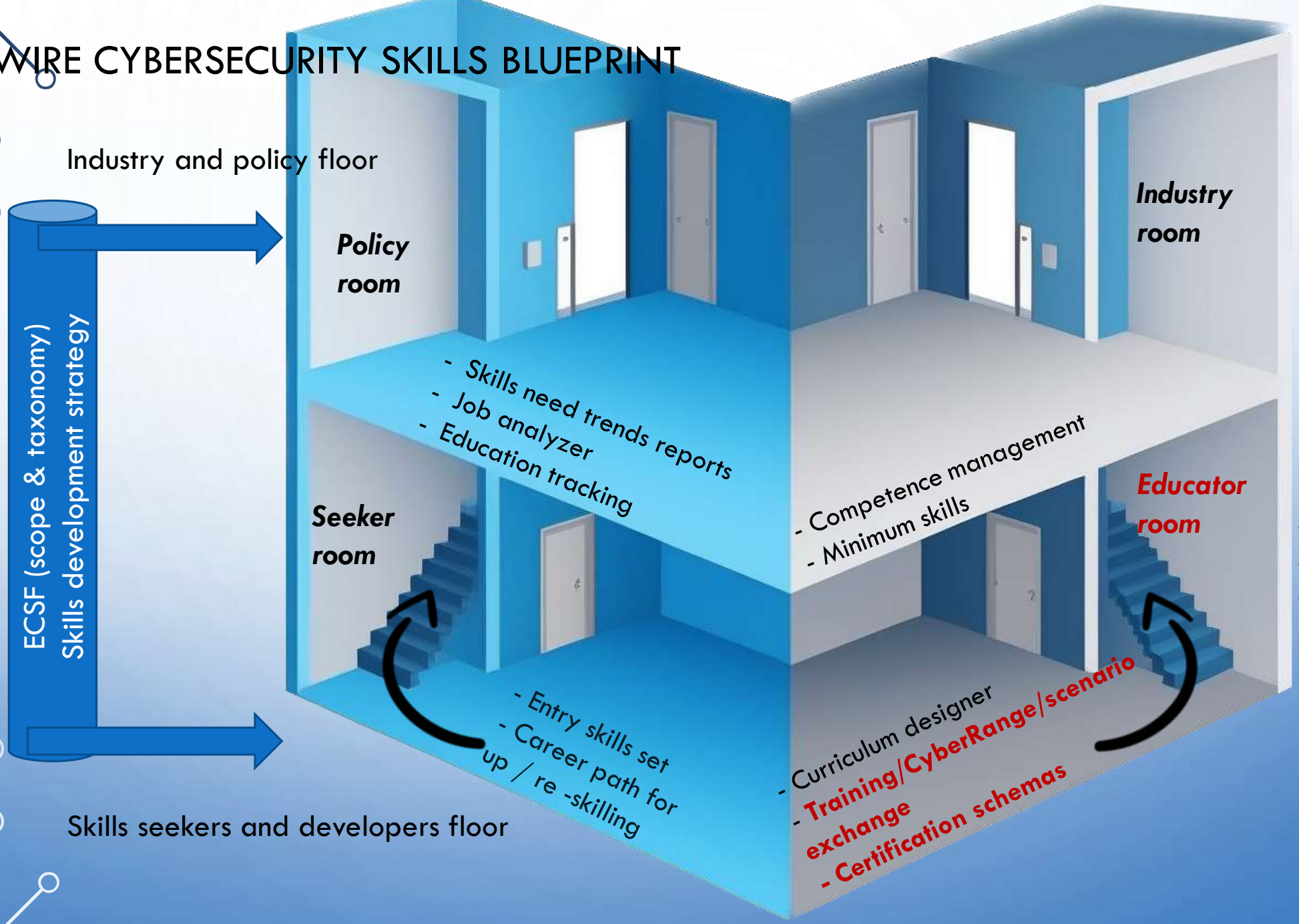
CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE

REWIRE COURSES - INFO DAY @ Lithuania

Author/presenter: Edmundas Piesarskas

Cybersecurity Skills Alliance – A New Vision for Europe (REWIRE) project has received funding from the European Union's Erasmus+ programme Cooperation for innovation and the exchange of good practices action under grant agreement No 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B.

REWIRE CYBERSECURITY SKILLS BLUEPRINT



Support terrace

- Job descriptions
- Best practice / examples

Support terrace

- Advertising materials
- Curriculum designer
- Best practice / examples

REWIRE BLUEPRINT TOOLBOX – *TOOLS DIRECTLY CONNECTED TO EDUCATION, TRAINING AND CERTIFICATION*

Objectives of the Toolbox:

- ✓Provide infrastructure and expert knowledge for activities utilizing **Cyber Ranges** (e.g. trainings, exercise implementation, examination, promotion, etc.)
- ✓Provide the **trainings** and relevant **certification** schemes on selected Occupational Profiles.

REWIRE COURSES SELECTION METHOD

6 Criterions proposed*:

(1) CRITERION A – Educational Levels of ENISA Occupational Profiles

(2) CRITERION B – Demand of The Job Market

(3) CRITERION C – Already Available Courses

(4) CRITERION D – Stakeholders' Input

(5) CRITERION E – Hands-on exercises on the Cyber Range

(6) CRITERION F – Certification

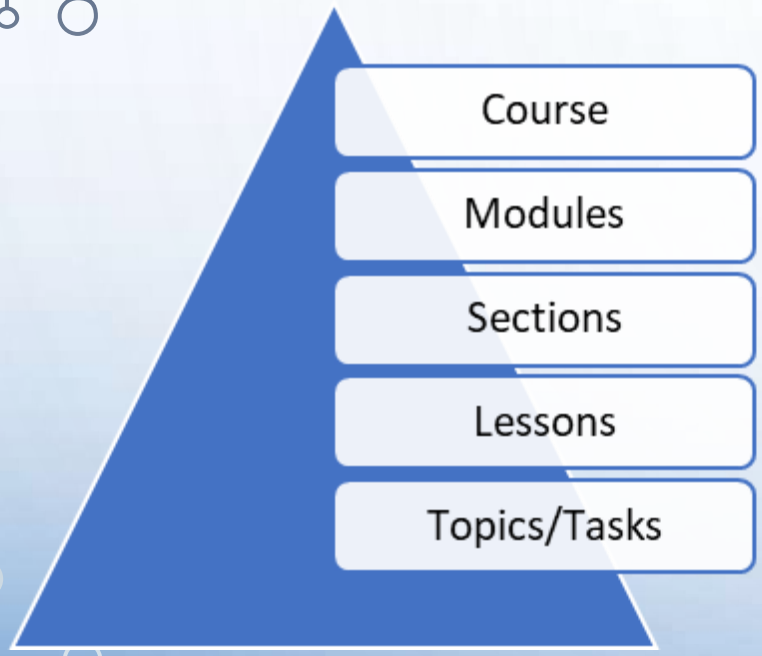
*R4.2.1 REWIRE Curricula and Training Framework [Available at rewireproject.eu]

REWIRE COURSES SELECTION

4 main Courses for each OP:

- CYBER THREAT INTELLIGENCE SPECIALIST
- CYBER INCIDENT RESPONDER
- PENETRATION TESTER
- CISO - CHIEF INFORMATION SECURITY OFFICER

STRUCTURE OF THE COURSES



REWIRE Courses are divided in Learning Modules (LM). Each **Module** is divided in one or more Sections to provide structure.
Each **Section** aims at teaching one or more lessons. Each **Lesson** is composed of topics/tasks that the students will need to complete, focusing on one or more concepts.

CISO COURSE- SYLLABUS

LM0: Introduction

- Overview of CISO program and market demand.

LM1: Risk Management

- Cyber Security Risk Management and risk assessments.

LM2: Security Strategy and Governance

- Information Security Governance, laws, regulations, and policy creation.

LM3: Incident Management

- Incident Management, team setup, response, and reporting.

LM4: Business Continuity and Disaster Recovery

- Business Continuity and Disaster Recovery concepts and planning.

LM5: Enterprise Architecture and Infrastructure Design

- Enterprise Architecture and Security by Design principles.

LM6: Audit & Information Security Controls Assessment

- Introduction to Security Audit and Assessment, vulnerability identification, and compliance

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B

CYBER INCIDENT RESPONDER COURSE - SYLLABUS

LM0: Introduction

Overview of the Cyber Incident Responder course, objectives, and market demand.

LM1: Risk Management

Fundamentals of Cyber Security Risk Management, risk assessment methodologies, and effective risk assessments.

LM2: Incident Management

Incident response terminology, understanding cyber attacks and threats, developing response plans, incident response procedures, malware analysis, and mitigation techniques.

LM3: Information Systems and Network Security

Knowledge of monitoring, logging, measurement, and evaluation processes and tools for information systems. Setting up logging functionality, collecting logs, operating SIEM systems, and practical labs.

LM4: Digital Forensics and Threat Analysis

Focus on digital forensics, digital evidence, forensics tools, and analyzing threat intelligence from external data sources. Insights into current cyber defense trends.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B

CYBER THREAT INTELLIGENCE SPECIALIST COURSE - SYLLABUS

LM0: Introduction

Overview of the Cyber Threat Intelligence Specialist course, objectives, and market demand.

LM1: Threat Intelligence Analysis

Fundamental concepts, tasks, and roles in cyber threat intelligence. Insights into CTI platforms, automation, and visualization. Real-world case studies for practical applications.

LM2: Threat Analysis

Cybersecurity tactics, techniques, and threat hunting. Organizing and streamlining the threat intelligence process.

LM3: Incident Management

Essential terms and definitions in incident response. Covers cyber attacks and threats, Cyber Incident Response Plan development, incident response procedures, malware analysis, and mitigation strategies.

LM4: Testing and Evaluation

Introduction to network ethical hacking, network cybersecurity tools, and the Cyber Kill Chain. Practical knowledge on testing and evaluating cybersecurity measures.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B

PENETRATION TESTER COURSE - SYLLABUS

LM0: Introduction

Overview of the Penetration Tester training program, core concepts, objectives, Penetration Tester profile, and market demand.

LM0: Basic Technical Knowledge

Establishing a foundational understanding of technical concepts. Preliminary knowledge, Cyber Ranges for practical exercises, and ethical and legal aspects in cybersecurity.

LM1: Threat Intelligence Analysis

Introduction to Cyber Threat Intelligence (CTI) terms, tasks, roles, CTI platforms, automation, and effective CTI visualization and interpretation.

LM2: Information Systems and Network Security

Information Systems monitoring, logging, measurement, evaluation processes and tools. Setting up logging functionality, collecting logs, operating SIEM systems, and hands-on labs.

LM3: Software Development and Vulnerability Assessment

In-depth knowledge of software for Web Penetration and OWASP TOP-10 vulnerabilities. Testing for SQL Injection (SQLI) and Server-side Request Forgery (SSRF) vulnerabilities.

LM4: Testing and Evaluation

Introduction to network ethical hacking, essential tools, and techniques for network cybersecurity. Exploration of the Cyber Kill Chain framework for systematic threat identification and mitigation.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B

REWIRE TOOLBOX – REWIRE CYBER RANGE

What is a Cyber Range?

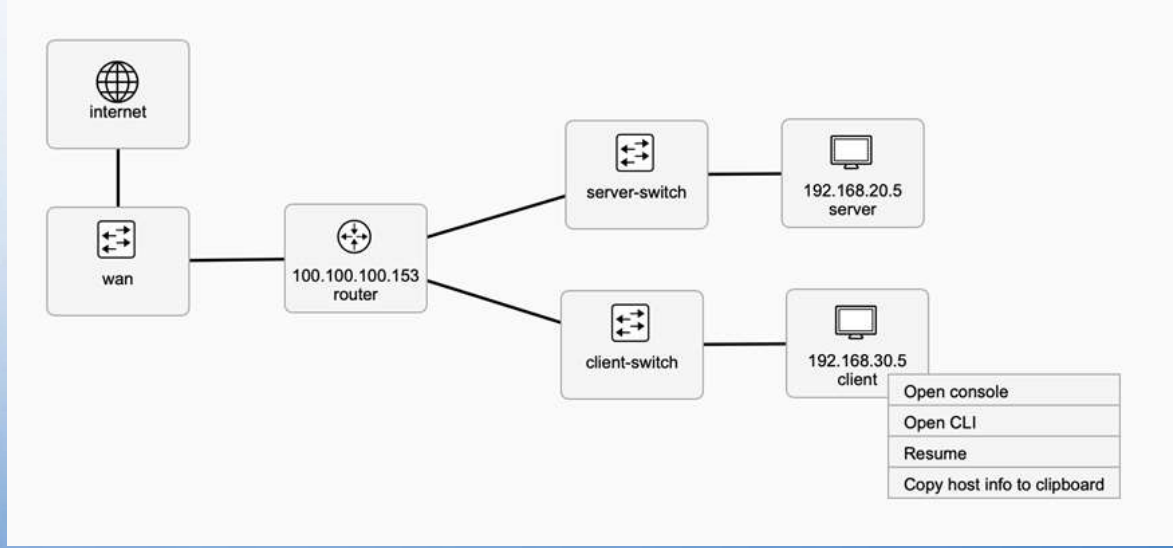
- Scenarios and exercises that are designed to **replicate a networked environment**, complete with various systems, applications, and infrastructure components.
- In a Cyber Range, cybersecurity professionals can **practice, test, and refine their skills in a risk-free setting**.

REWIRE Cyber Range is powered by

REWIRE TOOLBOX – REWIRE CYBER RANGE

How Cyber Ranges are used in the Rewire Courses?

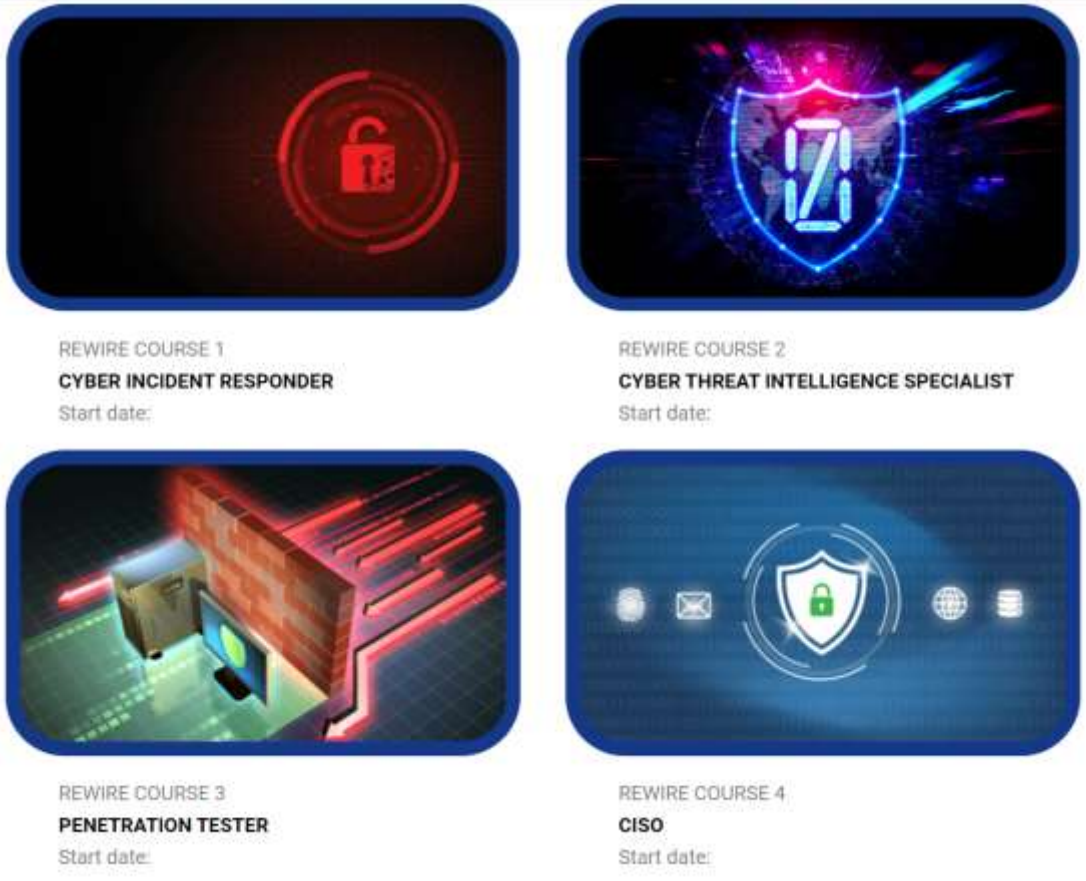
- ✓**Hands-on** activities specifically designed for each Occupational Profile
- ✓**Scenarios**
- ✓**Storylines**



REWIRE TOOLBOX - VIRTUAL LEARNING ENVIRONMENT (VLE)

https://vle.rewireproject.eu/

REWIRE TOOLBOX - VIRTUAL LEARNING ENVIRONMENT (VLE)



https://vle.rewireproject.eu/

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B

NEXT STEPS

We go live on Monday, 20/NOV 2023

September 2023

Finalisation of the Virtual Learning Platform

October 2023

Launch of the Virtual Learning Platform [Pilot]

November 2023 - January 2024

REWIRE Courses Public Launch

Invitation to students to enroll in REWIRE courses [1st delivery]

February 2024

REWIRE Courses Certification

Public provision of Certification [1st round]

2nd delivery

THANK YOU

Name of the presenter:

Name of the presenter organization:

E-mail: