CYRUS Project

A personalised, customised, work-based training framework for enhanced CYbeR-security skills across indUstrial Sectors

Marie-Hélène BONNEAU

Head of UIC Security Division

CYRUS
enhanced cybersecurity skills

This project has received funding from the European Union‘s Horizon Europe research and innovation programme under grant agreement No 101100733

Co-funded by the European Union

CYRUS in a nutshell

Project title: CYRUS - A personalised, customised, work-based training framework for enhanced CYbeR-security skills across indUstrial Sectors

Type of action: Digital SME Support Actions

Topic: DIGITAL-2022-TRAINING-02-SHORT-COURSES

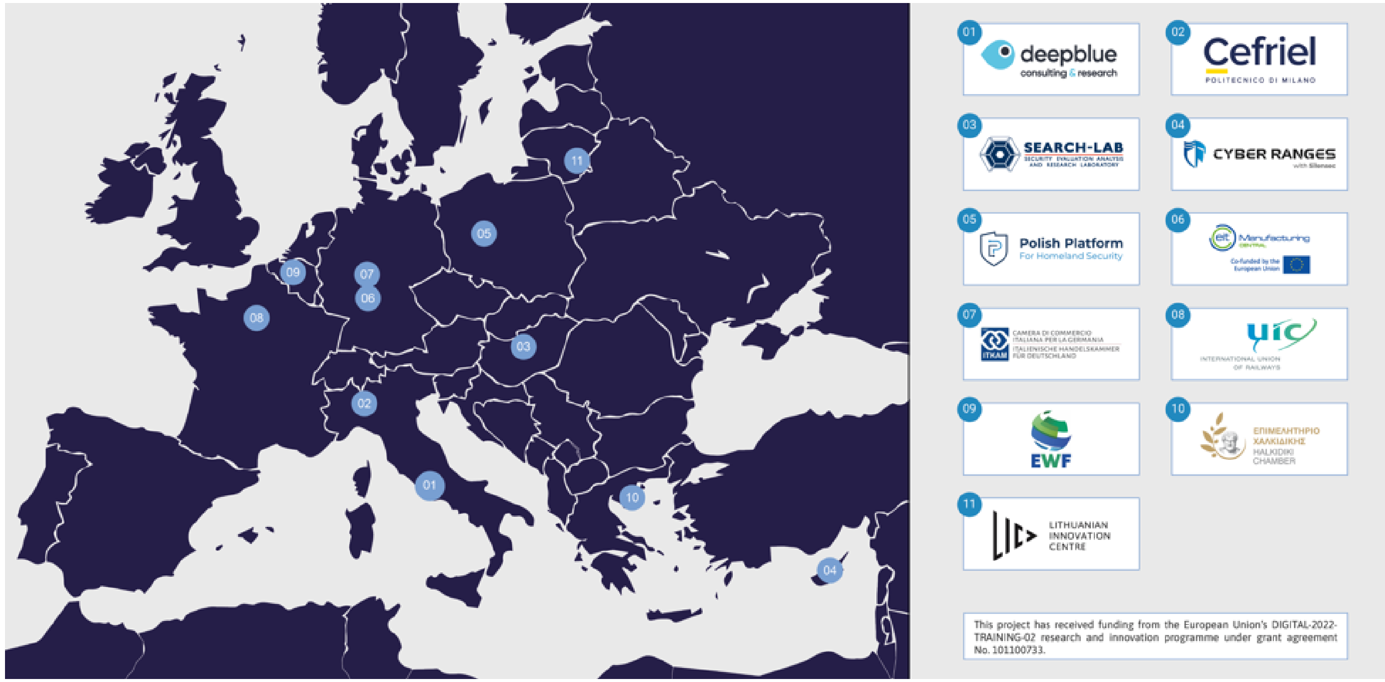
Granting Authority: European Health and Digital Executive Agency

Project duration: 36 Months (1 Jan 2023 – 31 Dec 2025)

Total funding: 2,066,121.85 €

Total budget: 3,247,642.60 €

11 partners from nine EU Countries.


01
02
03
04
05
06
07
08
09
10
11
01 deepblue consulting & research
02 Cefriel POLITECNICO DI MILANO
03 SEARCH-LAB SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY
04 CYBER RANGES with Silensec
05 Polish Platform For Homeland Security
06 eit Manufacturing CENTRAL Co-funded by the European Union
07 ITKAM CAMERA DI COMMERCIO ITALIANA PER LA GERMANIA ITALIENISCHE HANDELSKAMMER FÜR DEUTSCHLAND
08 uic INTERNATIONAL UNION OF RAILWAYS
09 EWF
10 ΕΠΙΜΕΛΗΤΗΡΙΟ ΧΑΛΚΙΔΙΚΗΣ HALKIDIKI CHAMBER
11 LIC LITHUANIAN INNOVATION CENTRE

This project has received funding from the European Union's DIGITAL-2022-TRAINING-02 research and innovation programme under grant agreement No. 101100733.

Our vision

CYRUS Introductory video

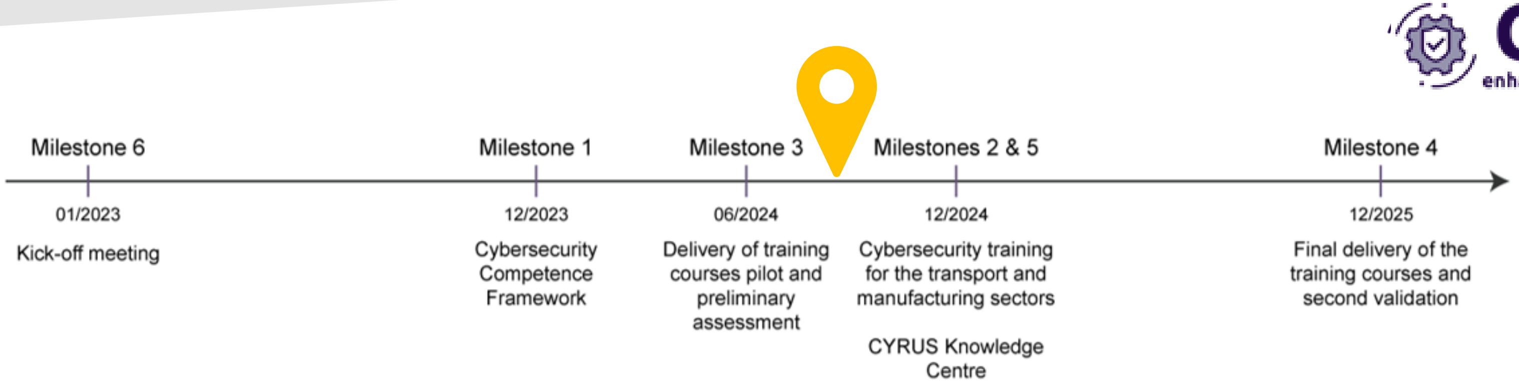
https://www.youtube.com/watch?v=e39P3zSHDVw

The **goal of the CYRUS project** is to propose a **novel training programme** to develop a **cybersecurity innovation DNA** and **support companies in transport and manufacturing sectors** to respond to and mitigate cyber threats and attacks.

Starting from the analysis of current needs and future cyber threat scenarios the project creates personalised cybersecurity training and assessment methodology for employees and professionals in the two sectors.

Co-funded by the European Union

Timeline & Milestones



Milestone 6
01/2023
Kick-off meeting

Milestone 1
12/2023
Cybersecurity Competence Framework

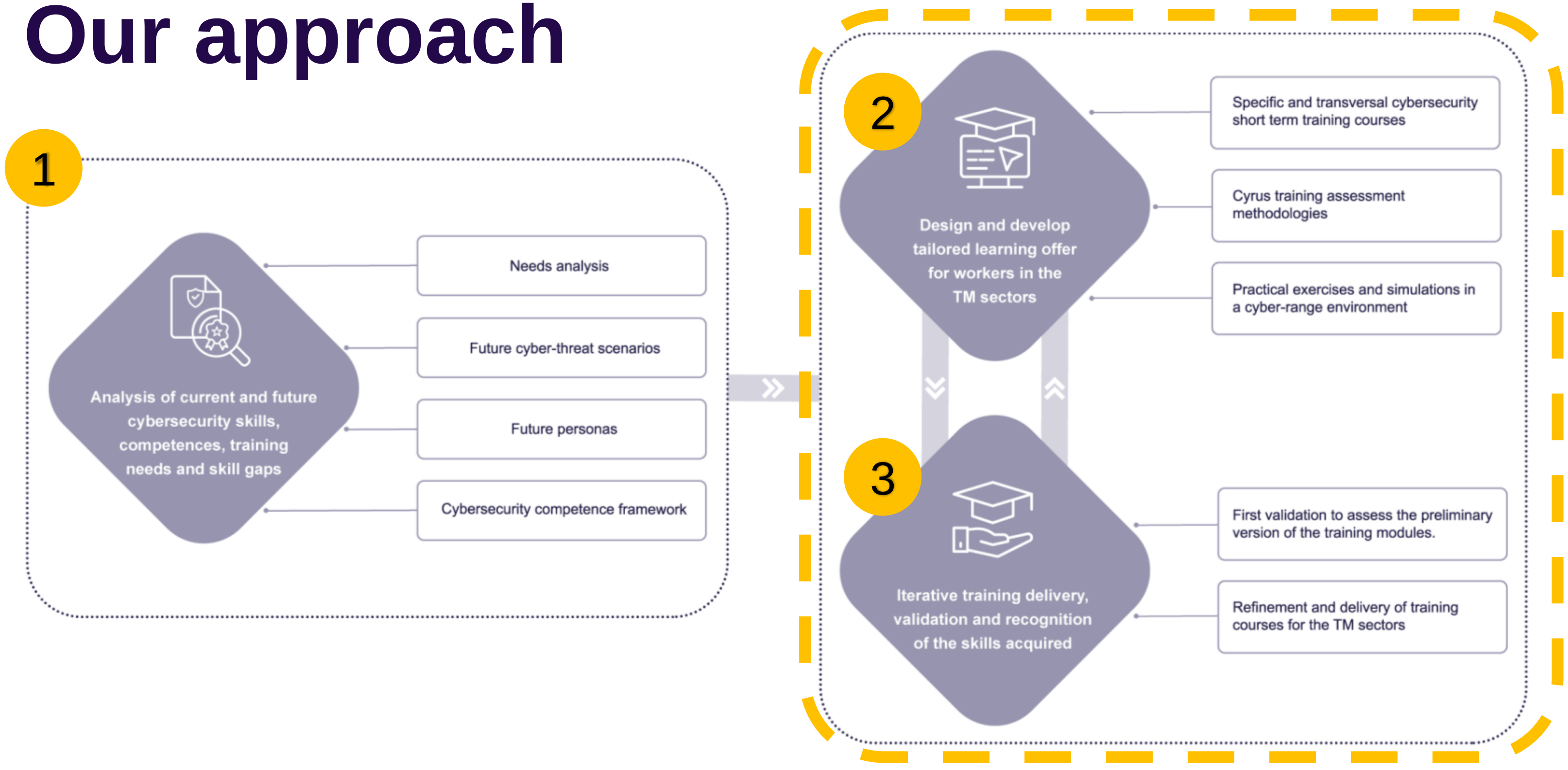
Milestone 3
06/2024
Delivery of training courses pilot and preliminary assessment

Milestones 2 & 5
12/2024
Cybersecurity training for the transport and manufacturing sectors

CYRUS Knowledge Centre

Milestone 4
12/2025
Final delivery of the training courses and second validation

Our approach



1
Analysis of current and future cybersecurity skills, competences, training needs and skill gaps
- Needs analysis
- Future cyber-threat scenarios
- Future personas
- Cybersecurity competence framework

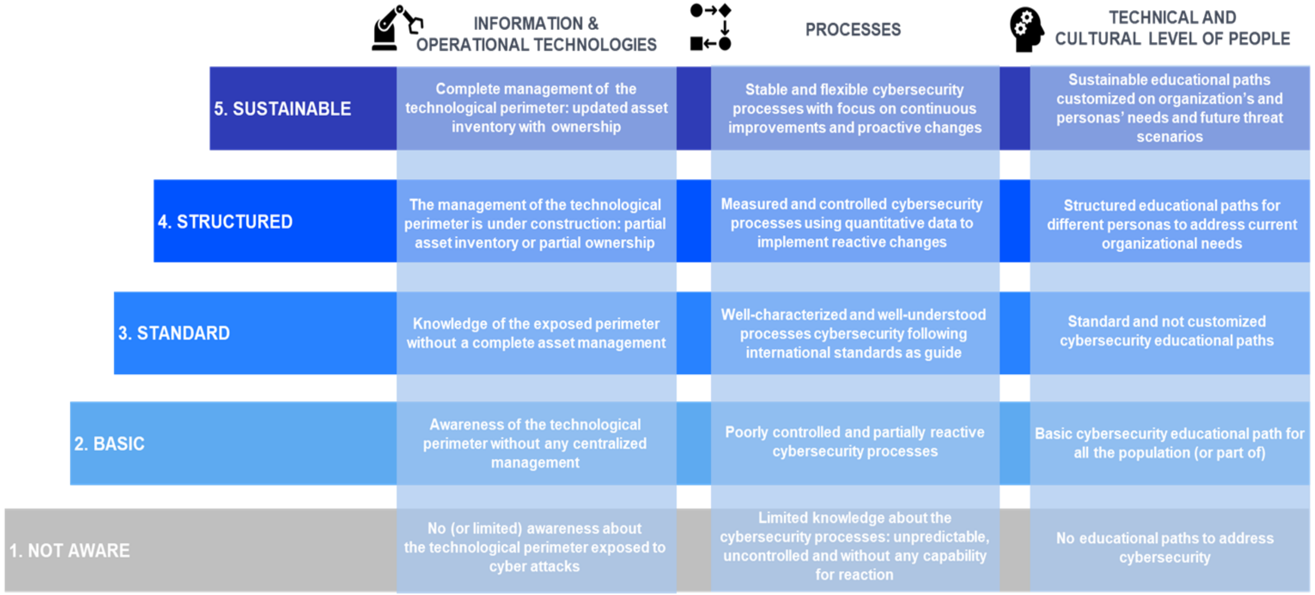
2
Design and develop tailored learning offer for workers in the TM sectors
- Specific and transversal cybersecurity short term training courses
- Cyrus training assessment methodologies
- Practical exercises and simulations in a cyber-range environment

3
Iterative training delivery, validation and recognition of the skills acquired
- First validation to assess the preliminary version of the training modules.
- Refinement and delivery of training courses for the TM sectors

Iterative process

CMM-EP – Overall Results for Transport Sector

CYBERSECURITY MATURITY MODEL FOR EDUCATIONAL PATHS (CMM-EP) - based on the CMMI Framework



	INFORMATION & OPERATIONAL TECHNOLOGIES	PROCESSES	TECHNICAL AND CULTURAL LEVEL OF PEOPLE
5. SUSTAINABLE	Complete management of the technological perimeter: updated asset inventory with ownership	Stable and flexible cybersecurity processes with focus on continuous improvements and proactive changes	Sustainable educational paths customized on organization's and personas' needs and future threat scenarios
4. STRUCTURED	The management of the technological perimeter is under construction: partial asset inventory or partial ownership	Measured and controlled cybersecurity processes using quantitative data to implement reactive changes	Structured educational paths for different personas to address current organizational needs
3. STANDARD	Knowledge of the exposed perimeter without a complete asset management	Well-characterized and well-understood processes cybersecurity following international standards as guide	Standard and not customized cybersecurity educational paths
2. BASIC	Awareness of the technological perimeter without any centralized management	Poorly controlled and partially reactive cybersecurity processes	Basic cybersecurity educational path for all the population (or part of)
1. NOT AWARE	No (or limited) awareness about the technological perimeter exposed to cyber attacks	Limited knowledge about the cybersecurity processes: unpredictable, uncontrolled and without any capability for reaction	No educational paths to address cybersecurity

OVERALL RESULTS FOR TRANSPORT SECTOR

INFORMATION AND OPERATIONAL TECHNOLOGIES scored **3.5 /5**, confirming the compliance with basic guidelines.

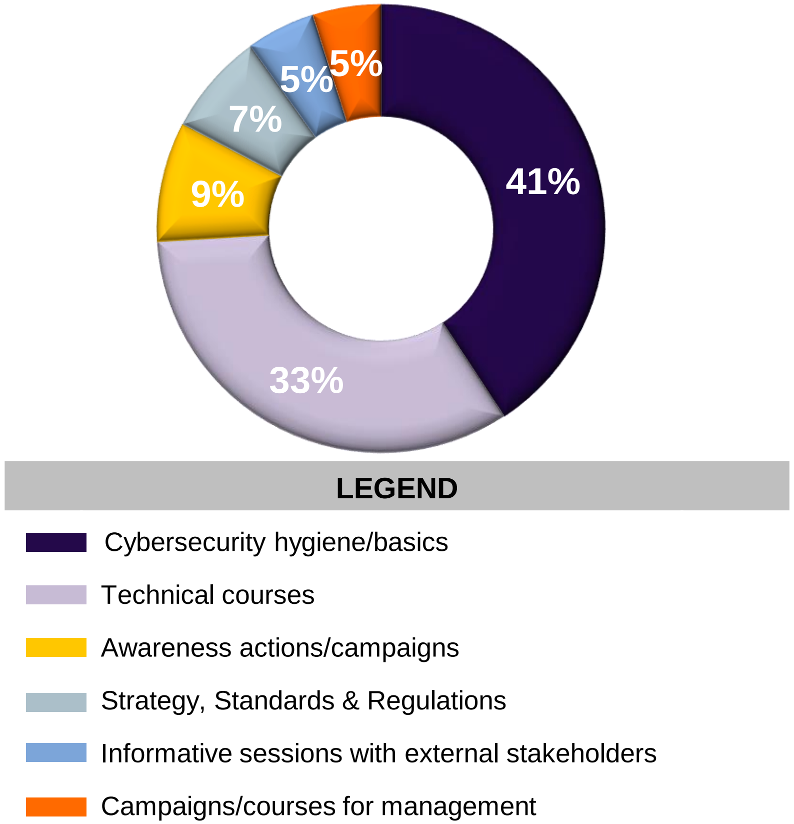
PROCESSES scored **2.5 /5**, demonstrating the need for postural improvement in this area.

TECHNICAL & CULTURAL LEVEL OF PEOPLE scored **2.6 /5**: 47% of the organisations display a maturity level below the minimum recommended.

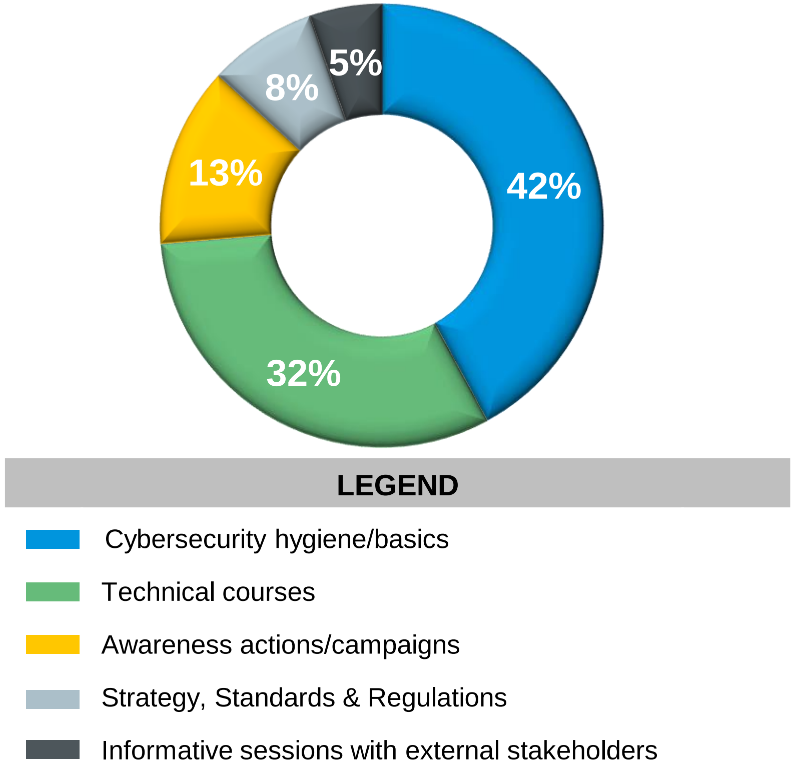
Main results and takeaways for the railway sub-sector

12 Interviews* conducted face-to-face with IT and security experts from *11 European railway companies

MAIN TOPICS ADDRESSED WITHIN INTERVIEWED COMPANIES’ TRAINING PROGRAMMES



TARGET AUDIENCE ADDRESSED WITHIN INTERVIEWED COMPANIES’ TRAINING PROGRAMMES



NEED FOR CYBERSECURITY EDUCATIONAL PATHS FOR NON-IT ROLES (OFFICE WORKERS)

Business areas which are **exposed to external contacts with customers** and/or **suppliers,** along with **Legal, HR, Finance departments** should be regarded as **critical from a cybersecurity perspective**.

⚠ ***Boards of Directors*** *and* ***high-level executives*** *are often overlooked by training managers because of their high degree of autonomy and scarce availability due to tight business schedules.*

NEED FOR CYBERSECURITY EDUCATIONAL PATHS FOR NON-IT ROLES (OPERATIONS)

Maintenance staff, system deployers/implementers (on lines/infrastructure, workshops and rolling stock), and **OT systems operators** should gain more cyber-security competences and be fully aware of the growing exposure of OT.

Train staff (train drivers and managers) are considered to be increasingly exposed to cyber threats, especially due to the growing number and complexity of on-board technical systems and the consequent exposure to cyber and cyber-physical threats

NEED FOR CYBERSECURITY EDUCATIONAL PATHS FOR IT ROLES (incl. CYBERSECURITY)

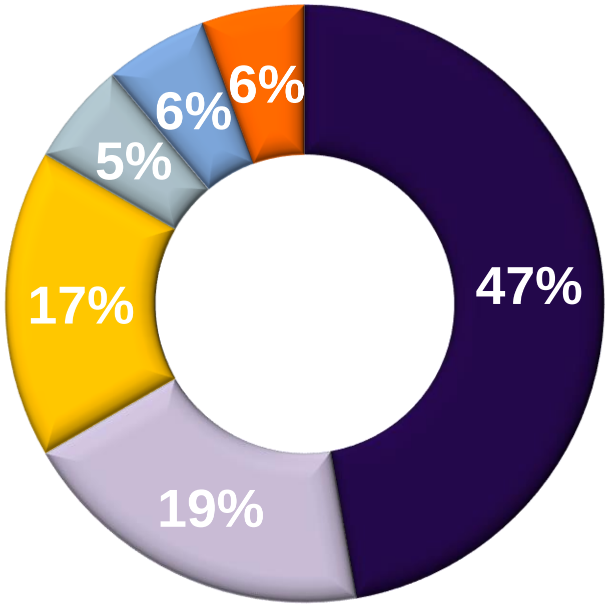
Software developers, **System architects and engineers** are the roles that most need cybersecurity up-skilling/re-skilling: integrating cybersecurity-by-design principles into in-house development is regarded as a priority.

IT infrastructure / system administrators and **technical managers** need a better technical understanding of cybersecurity in order to optimize and enforce information security principles and procedures

⚠ ***OT Technical staff and Managers*** *needs to achieve a better understanding of cybersecurity in order to effectively ensure a higher protection level for OT systems, especially due to the increasing IT-OT interactions.*

Co-funded by the
European Union

TRAINING NEEDS / DESIDERATA



LEGEND	
⬛	Role/category-specific trainings
🟪	Exercises/Actions/Campaigns
🟨	Courses on Strategy, Standards & Regulations
⬜	Industry/Company-specific trainings
🟦	Topic-specific trainings
🟧	Trainings in national language

- **(3) Awareness for Management/Executives/Board**
- **(2) Training for Business/Non-technical staff**
- **(2) Training for OT staff, not specified**
- **(1) Trainings tailored for different roles/sectors**
- **(1) Trainings tailored for railway Maintenance, Operations and Technical/Physical Security staff**
- **(1) Cybersecurity for OT security managers and staff**
- **(1) Cybersecurity for OT system leads and users**
- **(1) Training for Developers –DevSecOps**
- **(1) Training for Developers and Security Auditors on secure coding and code reviewing**
- **(1) Training for Maintenance staff/Workshop workers**
- **(1) Training for Operational/Non-technical staff**
- **(1) Training for Train Drivers**
- **(1) Training for Engineers in forensics**

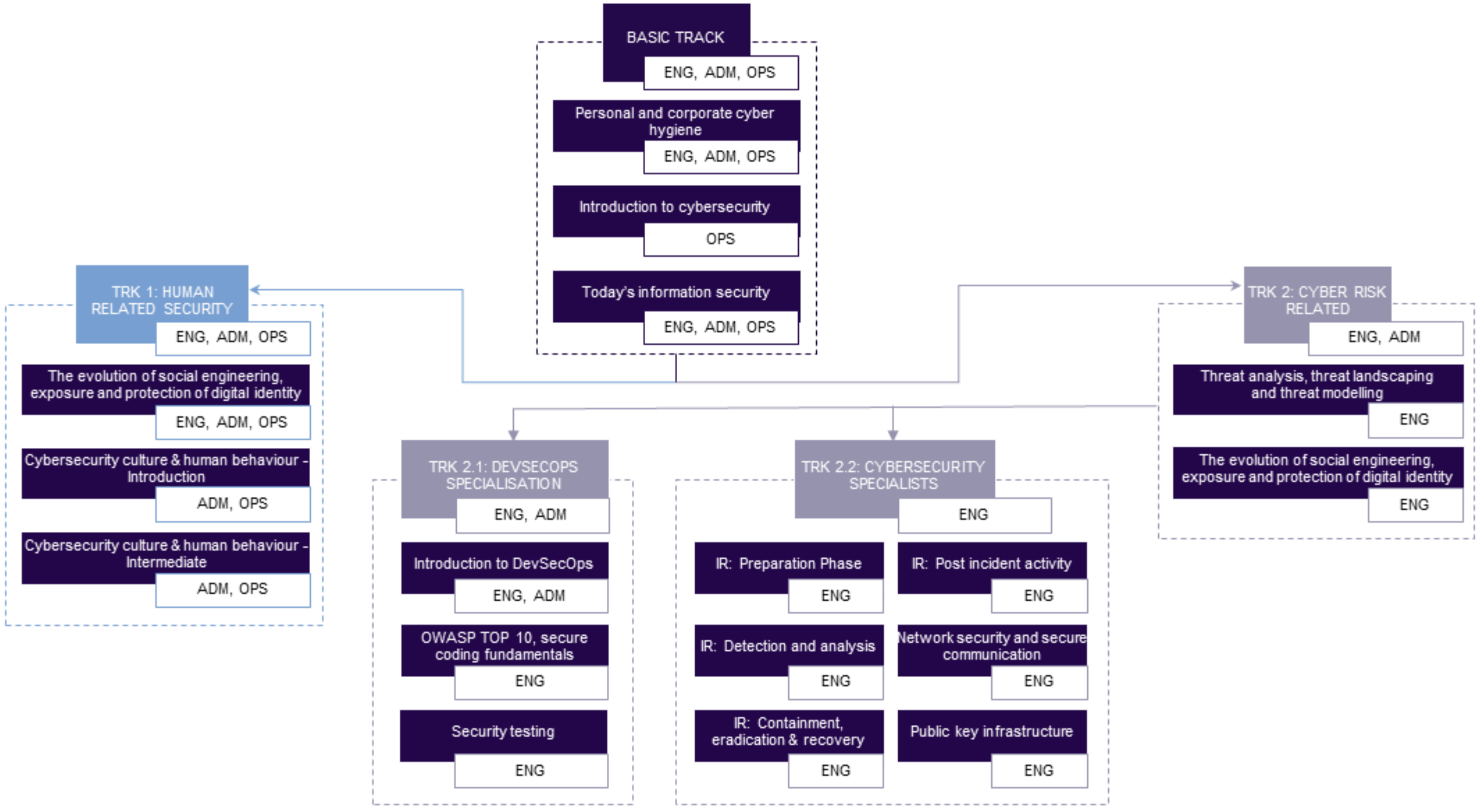
- **(1) Adapted role-play/use cases**
- **(2) Adapted/near-real training scenarios for railways**
- **(1) Phishing campaign organized between members of Er-ISAC**
- **(1) Red Team/Blue team exercises**
- **(1) Workshop-type training and exercise on OT security**
- **(1) Organization of exercises, not specified**

- **(3) Training on TS 50701 / IEC 63452**
- **(1) Training on Cyber Resilience Act**
- **(1) Training on ENISA instructions**
- **(1) Training on NIS 2 EU Directive**

- **(1) Handling suspicious emails and calls**
- **(1) Trainings on cross border security compliance, interoperability, governance, audit and incident response management relating to FRMCS.**

Co-funded by the
European Union

CYRUS Training tracks – Pilot phase



BASIC TRACK
ENG, ADM, OPS

Personal and corporate cyber hygiene
ENG, ADM, OPS

Introduction to cybersecurity
OPS

Today's information security
ENG, ADM, OPS

TRK 1: HUMAN RELATED SECURITY
ENG, ADM, OPS

The evolution of social engineering, exposure and protection of digital identity
ENG, ADM, OPS

Cybersecurity culture & human behaviour - Introduction
ADM, OPS

Cybersecurity culture & human behaviour - Intermediate
ADM, OPS

TRK 2.1: DEVSECOPS SPECIALISATION
ENG, ADM

Introduction to DevSecOps
ENG, ADM

OWASP TOP 10, secure coding fundamentals
ENG

Security testing
ENG

TRK 2.2: CYBERSECURITY SPECIALISTS
ENG

IR: Preparation Phase
ENG

IR: Post incident activity
ENG

IR: Detection and analysis
ENG

Network security and secure communication
ENG

IR: Containment, eradication & recovery
ENG

Public key infrastructure
ENG

TRK 2: CYBER RISK RELATED
ENG, ADM

Threat analysis, threat landscaping and threat modelling
ENG

The evolution of social engineering, exposure and protection of digital identity
ENG

- The **BASIC TRACK** provides basic information to align attendants for the specialized tracks.

- TRACK 1 focuses on human-related security with the goal to provide a clear understanding of human-centered security problems and solutions.

- TRACK 2 delves into cyber risk. It includes two specialization sub-tracks:
  - TRACK 2.1 centered on **DevSecOps** and **Security testers.**
  - TRACK 2.2 is for **Network specialists** and **Incident responders.**

CYRUS
enhanced cybersecurity skills

Cybersecurity pilot trainings

BASIC TRACK

PERSONAL AND CORPORATE CYBER HYGIENE – beginner – ADM

PERSONAL AND CORPORATE CYBER HYGIENE – beginner –OPS

PERSONAL AND CORPORATE CYBER HYGIENE – beginner – ENG

INTRODUCTION TO CYBERSECURITY – beginner – OPS and ADM (self-paced)

INTRODUCTION TO CYBERSECURITY – beginner – OPS and ADM (instructor led, Polish language)

TODAY'S INFORMATION SECURITY – beginner – ADM

TODAY'S INFORMATION SECURITY – beginner – OPS

TODAY'S INFORMATION SECURITY – beginner – ENG

TRACK 1: HUMAN RELATED SECURITY

EVOLUTION OF SOCIAL ENG., EXPOSURE AND PROTECTION OF DIGITAL ID. – beginner – ADM

EVOLUTION OF SOCIAL ENG., EXPOSURE AND PROTECTION OF DIGITAL ID. – beginner – OPS

EVOLUTION OF SOCIAL ENG., EXPOSURE AND PROTECTION OF DIGITAL ID. – beginner – ENG

CYBERSECURITY CULTURE & HUMAN BEHAVIOR – beginner – ADM

CYBERSECURITY CULTURE & HUMAN BEHAVIOUR – beginner – OPS

CYBERSECURITY CULTURE & HUMAN BEHAVIOUR – intermediate – ADM

CYBERSECURITY CULTURE & HUMAN BEHAVIOUR – intermediate – OPS

TRACK 2: CYBER RISK RELATED

THREAT ANALYSIS, LANDSCAPING & MODELLING – expert – ENG

TRACK 2.1: DEVSECOPS SPECIALISATION

INTRODUCTION TO DEVSECOPS – expert – ADM

INTRODUCTION TO DEVSECOPS – expert – ENG

OWASP TOP 10 PART 1 – beginner – ENG

OWASP TOP 10 PART 2 – beginner – ENG

OWASP TOP 10 PART 3 – beginner – ENG

OWASP TOP 10 PART 4 – beginner – ENG

SECURITY TESTING PART 1 – intermediate – ENG

SECURITY TESTING PART 2 – intermediate – ENG

TRACK 2.2: CYBERSECURITY SPECIALIZATION

INCIDENT RESPONSE - PREPARATION PHASE – beginner – ENG

INCIDENT RESPONSE - DETECTION AND ANALYSIS – beginner – ENG

INCIDENT RESPONSE - CONTAINMENT, ERADICATION & RECOVERY – beginner – ENG

INCIDENT RESPONSE - POST INCIDENT ACTIVITY – beginner – ENG

NETWORK SECURITY AND SECURE COMMUNICATION – intermediate – ENG

PUBLIC KEY INFRASTRUCTURE – intermediate – ENG

Co-funded by the
European Union

Information about Cyrus pilot trainings

- **Running (from July) until mid-October 2024**
- Enroll for a selected range of our courses **for free.**
- **Courses differentiated by audience/role**: IT/engineers/cybersecurity (ENG), administrative/office staff (ADM), operators (OPS).
- **Courses differentiated by proficiency level**: beginner, skilled, expert
- **Your feedback** will help us **refine and customise our offerings** to better suit sectoral needs **towards the final training delivery** session, which is **scheduled for 2025**.

cyrus-project.eu/pilot-trainings/

SCAN THE QR CODE **TO ACCESS THE PILOT TRAINING CATALOGUE** AND **ENROLL FOR FREE**

Follow CYRUS

cyrus-project.eu

https://www.facebook.com/cyruseuproject/

https://www.youtube.com/@CYRUS-anEUproject

https://www.linkedin.com/company/cyrus-eu-project/

Co-funded by the European Union

PAST EU-FUNDED RESEARCH PROJECT FOCUSING ON RAIL CYBERSECURITY

- **SECRET (FP7 – ended on 2011)**
  - Security of railways against electromagnetic attacks
  - Website : https://secret-project.eu/
- **CYRAIL (S2R – ended on 2017) formation on the EU framework**
  - CYbersecurity in the RAILway sector
  - Website : https://cyrail.eu/
- **4SECURAIL (S2R – ended on 2021)**
  - Implementation of CSIRT (Computer Security Incident Response Team) model - UIC rail system department involvement
  - Website :https://www.4securail.eu/
- **SAFETY4RAILS (H2020 – ended on 2022)**
  - Increasing railways resilience to combined cyber-physical threats
  - Website : https://safety4rails.eu/

Stay in touch with UIC Security Team!

security@uic.org

www.uic.org/security

@RailSecurityUIC

railsecurityhub.org

Head of Security Division

Marie-Hélène Bonneau

BONNEAU@uic.org

Senior
Security Research Advisors

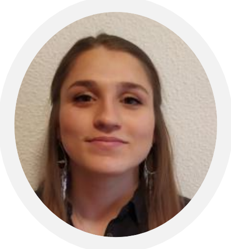
Grigore Havarneanu

HAVARNEANU@uic.org

Laura Petersen

PETERSEN@uic.org

Junior
Security Research Advisor



Paula Fernandez Díaz

FERNANDEZ@uic.org

Senior
Security Advisors (seconded)

Bruno De Rosa

DEROSA@uic.org

Kacper Kubrak

KUBRAK@uic.org