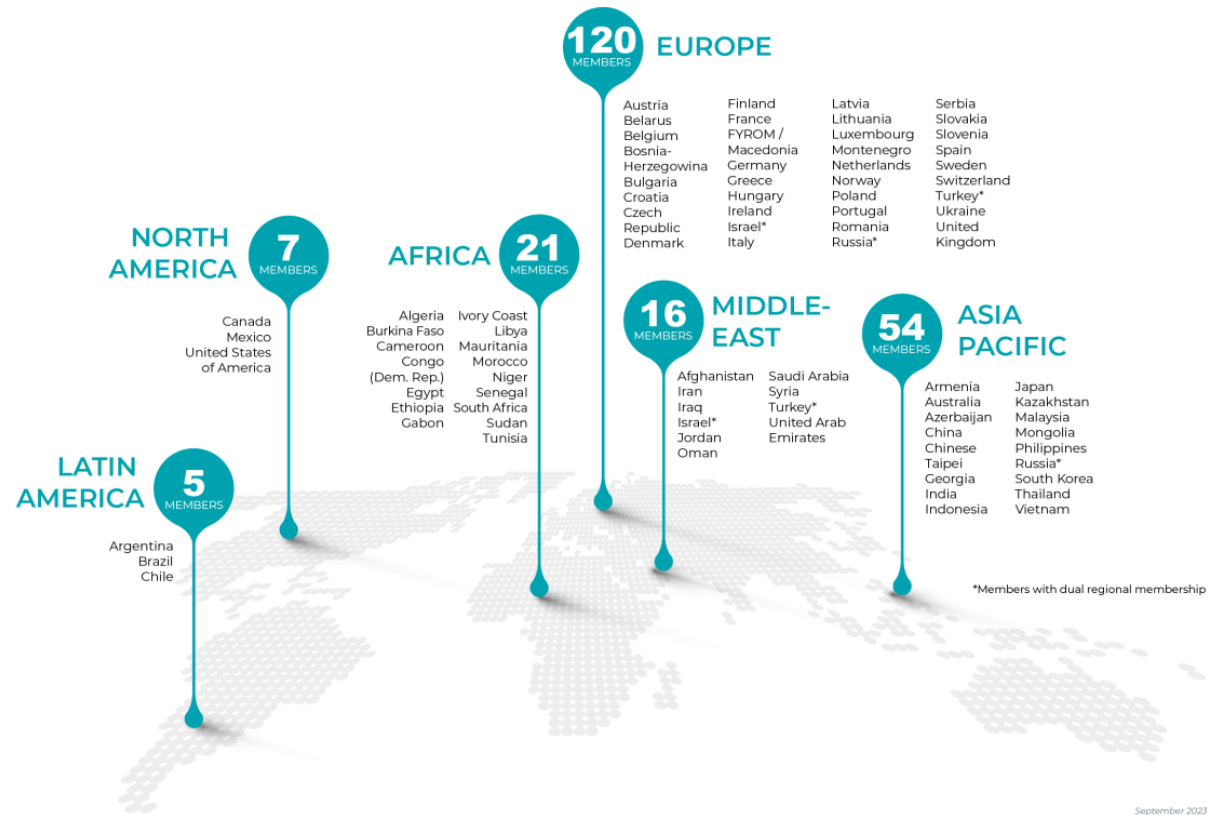


# UIC - The Worldwide Railway Organization

- ❖ Founded in **1922** in Paris
- ❖ Promotes the development of rail transport at world level
- ❖ Counts **200** members in **95** Countries
- ❖ Platform for:
  - Cooperation
  - Research projects
  - Dissemination
  - Training
  - Standards & Technical solutions



# CYRUS Project

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

**Bruno DE ROSA**

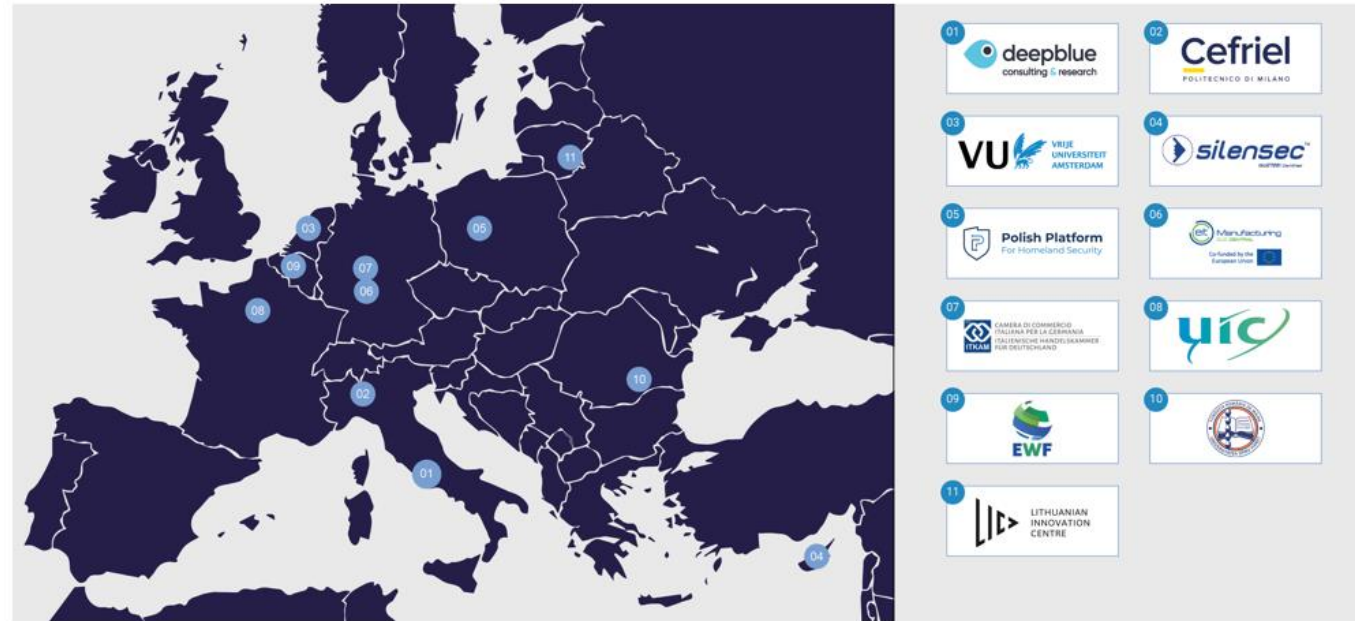
UIC Security Division

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



# 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.



# The challenges

- **Digital transformation increases risks and exposure to cyberattacks.**
- **74% of all breaches involve the human element** (source: [Verizon](#))
- **Organisational and economical limitations often restrain companies from effectively training their personnel.**



## Our vision

**A novel training system to sharpen employees' skills, making them more vigilant and capable to identify and to respond to cyber-threats**

- Innovative methods for training implementation
- Virtualisation-dedicated cyber-range simulations in operational settings
- Work-based learning allowing timely and efficient course delivery



# Objectives



## Assess SME cyber posture

Field studies help understand SMEs' needs to tailor trainings



## Develop novel training system

Training tools that are cost-effective, flexible and available on the job



## Set new standards

Build a robust innovation DNA on cybersecurity in European organisations



## Upskill staff

Boost cybersecurity competencies to better protect companies



## Raise awareness

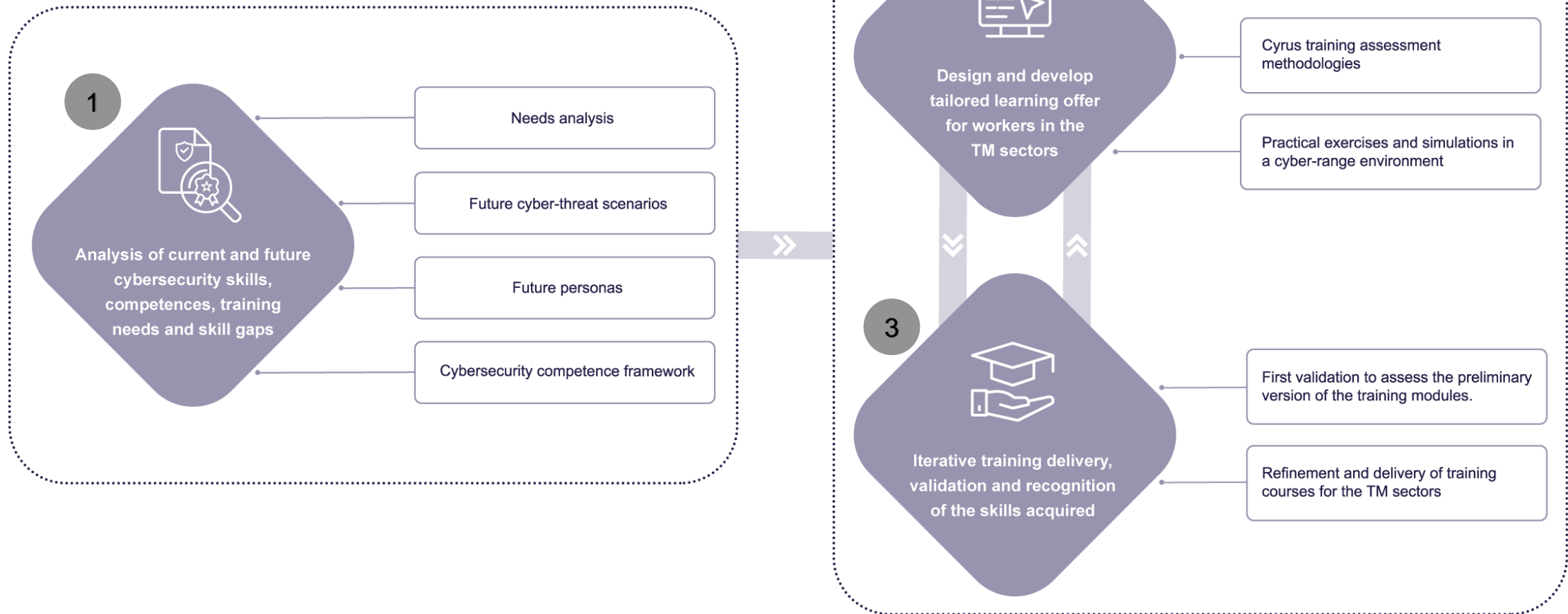
Foster a general increase in knowledge and cybersecurity awareness



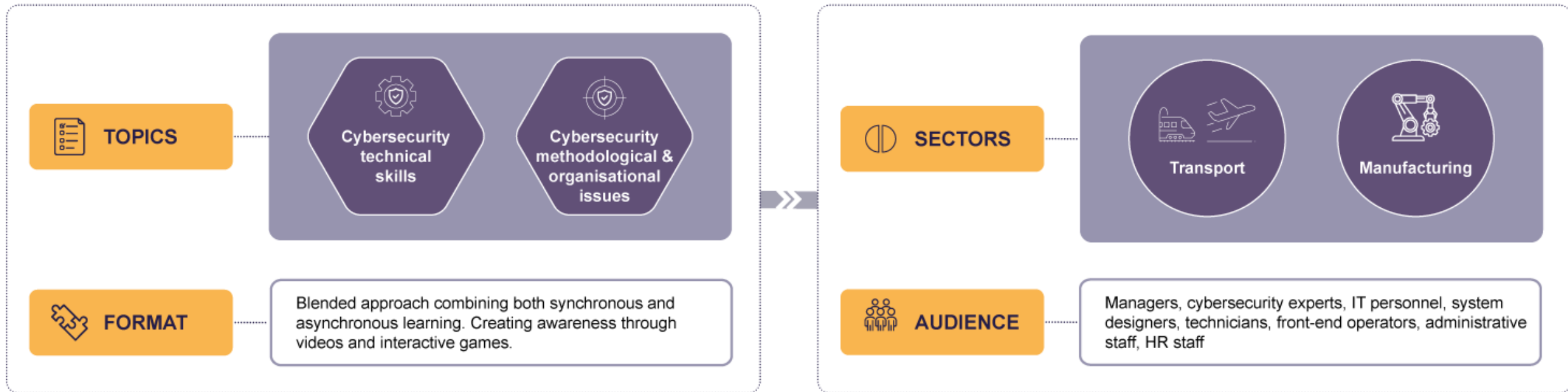
## Personalised training

Provide training solutions that are customised for different roles

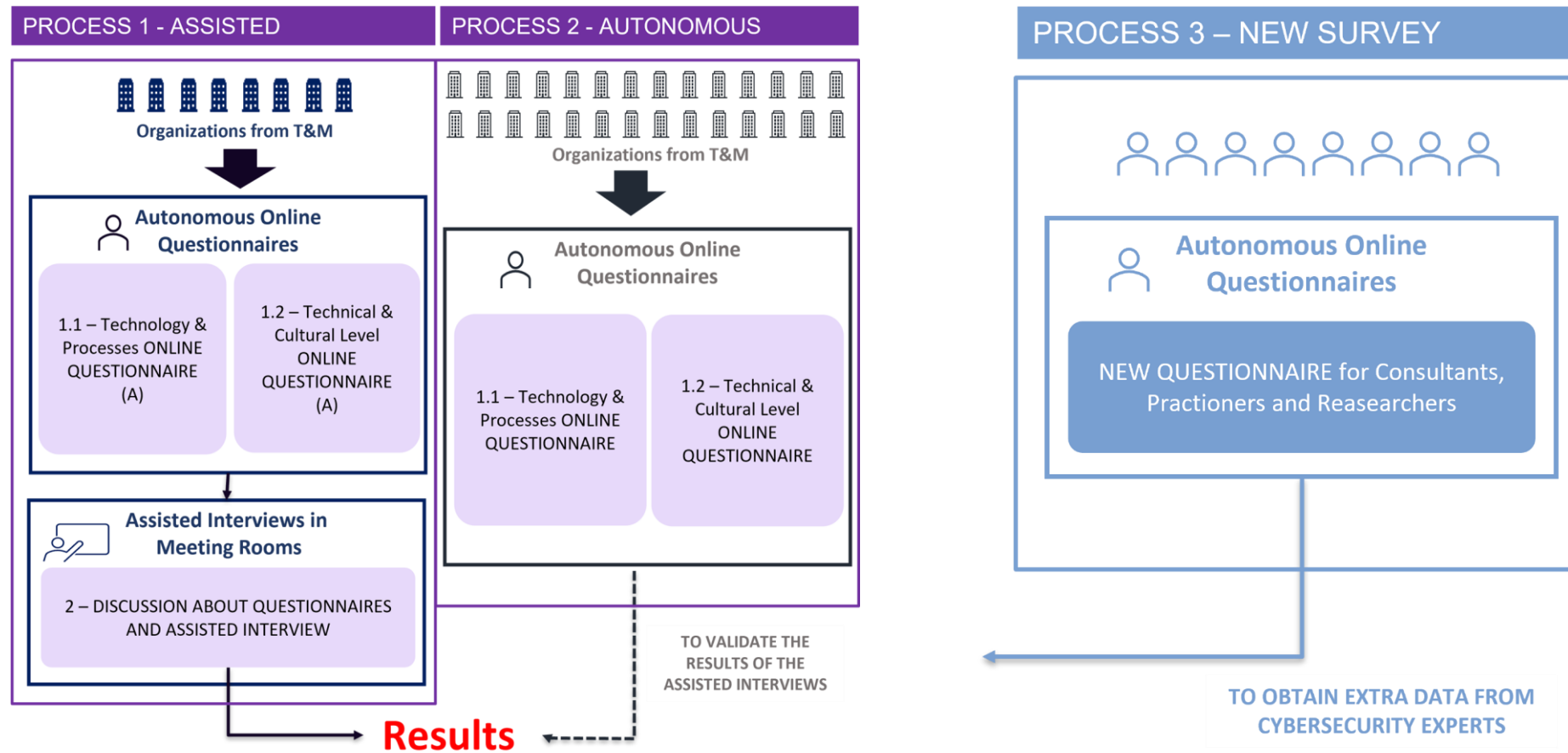
# Our approach



# Cybersecurity training structure






# First Phase: Collecting needs and requirements – Methodology





# Cybersecurity Maturity Model for Educational Paths (CMM-EP)

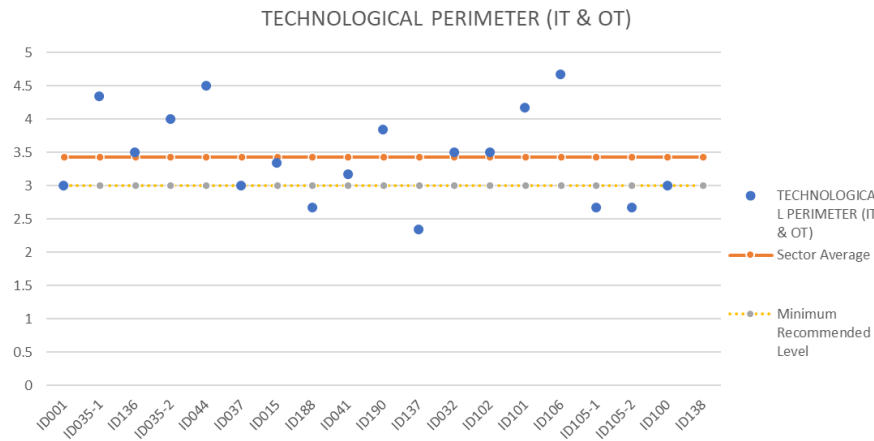
Three dimensions

	 <b>INFORMATION &amp; OPERATIONAL TECHNOLOGIES</b>	 <b>PROCESSES</b>	 <b>TECHNICAL AND CULTURAL LEVEL OF PEOPLE</b>
<b>5. SUSTAINABLE</b>	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
<b>4. STRUCTURED</b>	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
<b>3. STANDARD</b>	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
<b>2. BASIC</b>	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)
<b>1. NOT AWARE</b>	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

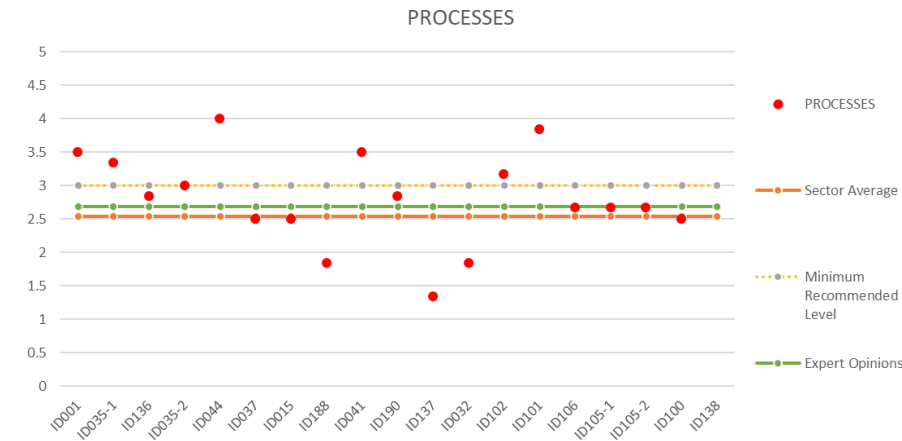
Based on the CMMI Framework. It is structured over three pillars and five distinct maturity levels.

# CMM-EP – Overall Results for Transport Sector

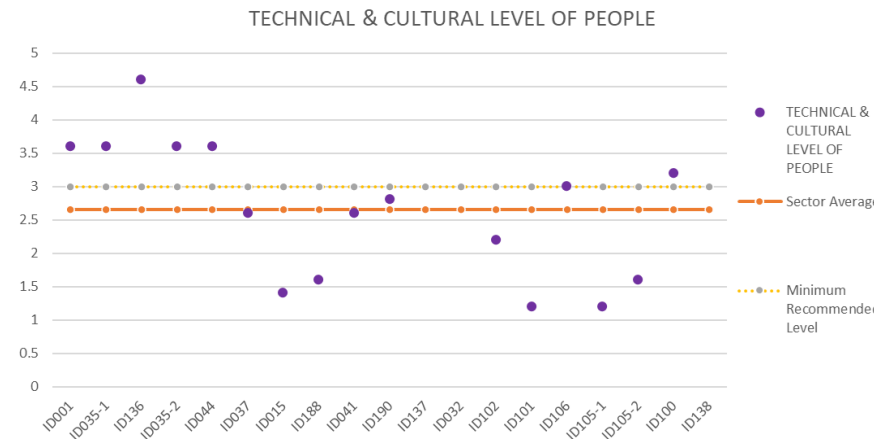
The average of **Technological Perimeter** is around 3.5: showing the compliance with basic guidelines.



The average of **Processes** is 2.5 demonstrating the need for postural improvement in this area. **Expert opinions agree with these values.**



The average **Technical & Cultural Level** is around 2.6: 47% of the organisations are at a maturity level below the minimum recommended.



# CYBERSECURITY NEEDS AND PAINS IN THE RAILWAY SUB- SECTOR

ANALYSIS OF SURVEYS AND INTERVIEWS AMONG RAILWAY  
COMPANIES

**Bruno DE ROSA**

UIC SECURITY DIVISION

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

# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

- **12 interviews** have been conducted by UIC Security Division among its Members in 1-to-1 mode.
- **27 online surveys** filled out by railway sector experts (companies + external).
- **2 Focus Groups** with railway cybersecurity experts

TO WHICH SUBSECTOR DO RESPONDENT COMPANIES BELONG? (C5, 27)



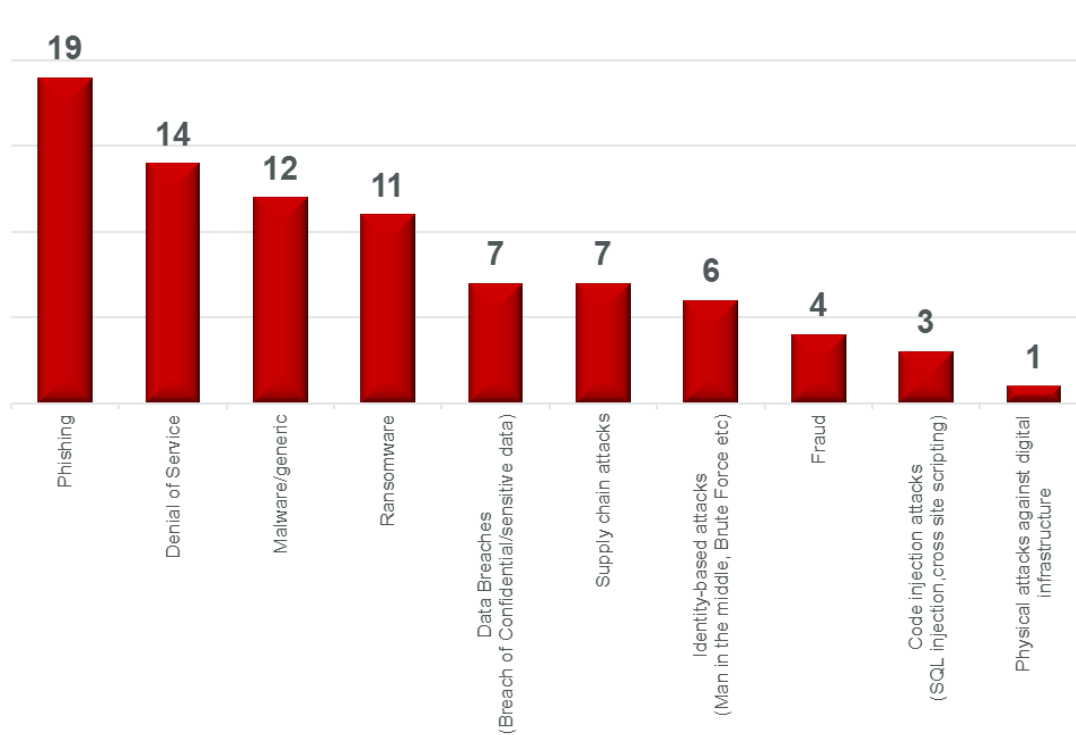
## 15 Countries represented:

AUSTRIA, BELGIUM, CZECH REPUBLIC, FINLAND, FRANCE, GERMANY, HUNGARY, IRELAND, ITALY, LUXEMBOURG, POLAND, SERBIA, SPAIN, SLOVAKIA, SLOVENIA.

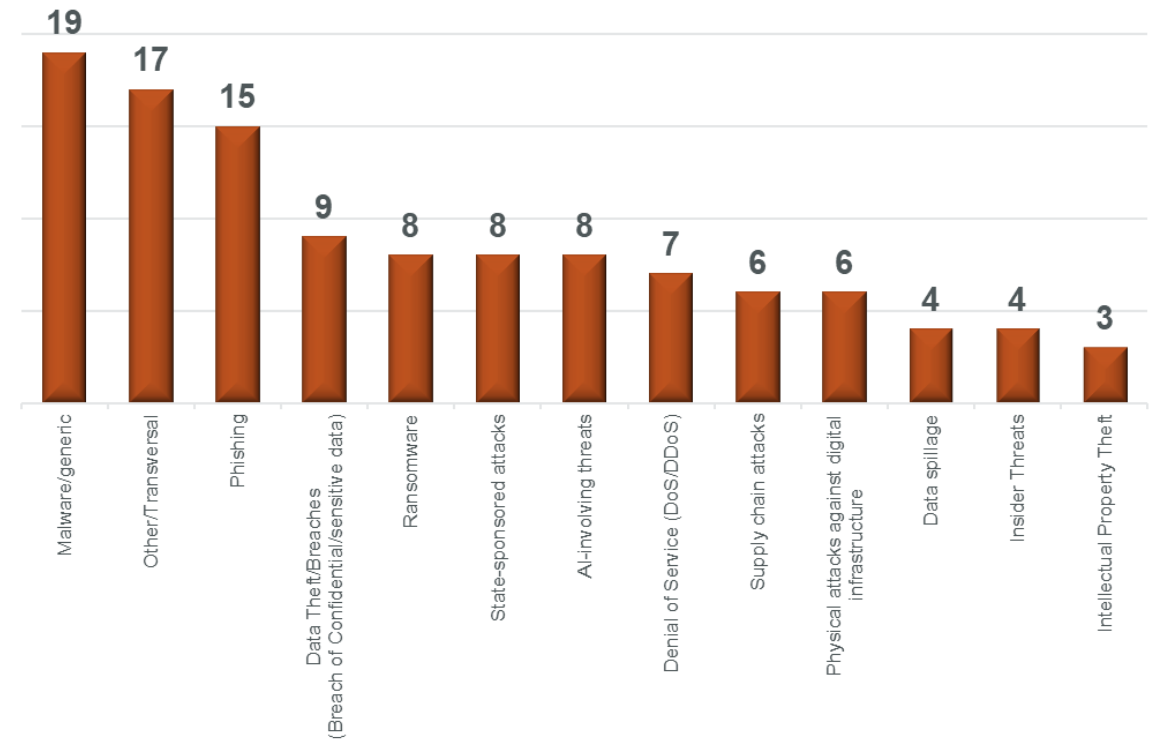
# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

## SECTION 2: MAIN THREATS AND CYBER ATTACKS ACCORDING TO RAILWAY COMPANIES

CONSIDERING EXPERIENCED AND KNOWN CYBER ATTACKS, WHICH ARE THE MAIN CURRENT CYBERTHREATS? (Z3, Q6, 26 responders)



WHICH WILL BE THE MAIN CYBER-ATTACK TYPES IN THE NEXT 5 YEARS? (Z4, Q7, 26)



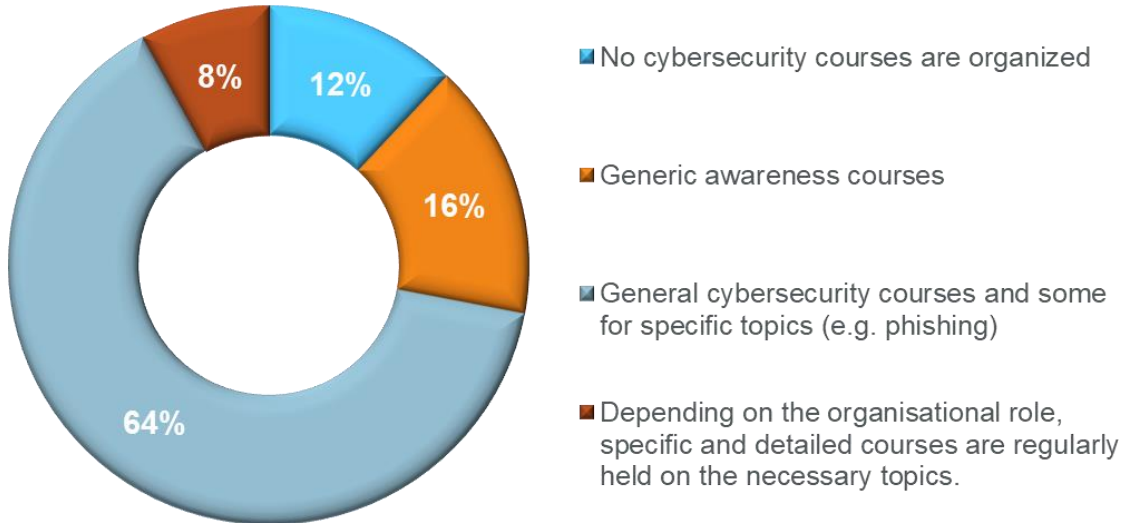
# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

## SECTION 3: CURRENT CYBERSECURITY TRAINING OFFER

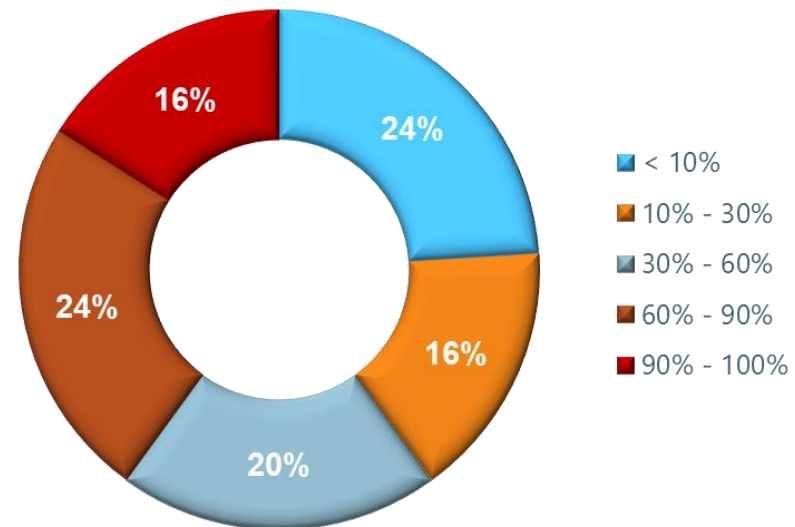
2.4/5

**AVERAGE SELF ESTIMATED COMPANIES' MATURITY LEVEL IN PROPOSING AND DELIVERING EDUCATIONAL PATHWAYS IN CYBERSECURITY** (Q21, 25 responders)

**WHAT TYPE OF CYBERSECURITY COURSES ARE DELIVERED BY YOUR ORGANIZATION?** (E16, 25 responders)



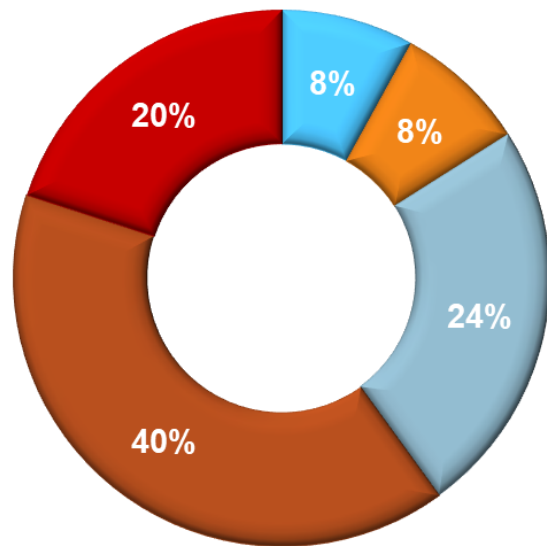
**HOW MANY PEOPLE IN YOUR ORGANISATION HAVE PARTICIPATED IN A CYBERSECURITY COURSE IN THE LAST 2 YEARS?** (E17, 25 responders)



# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

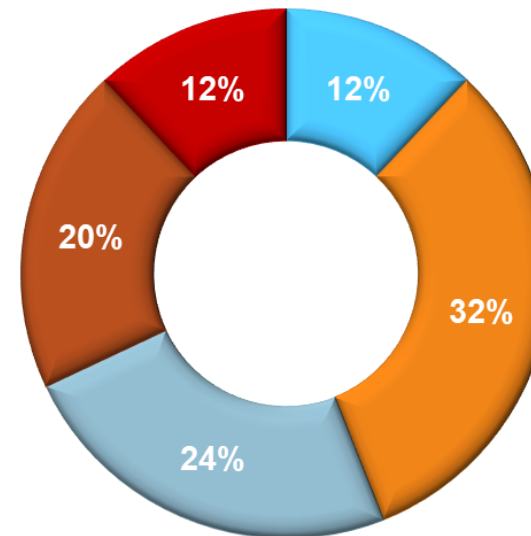
## SECTION 3: CURRENT CYBERSECURITY TRAINING OFFER

TO WHOM ARE THE CYBERSECURITY AWARENESS INITIATIVES DELIVERED BY YOUR ORGANIZATION ADDRESSED? (E18, 25 responders)



- No cybersecurity initiatives are organized.
- Only to those who have suffered an attack or security incident.
- Only to those who request it or only to people in a technical role.
- To the entire corporate population without distinction.
- To all, in an organizational role-dependent manner.

ARE CYBERSECURITY PATHS CUSTOMIZED ACCORDING TO YOUR ORGANISATION'S NEEDS? (E19, 25 responders)

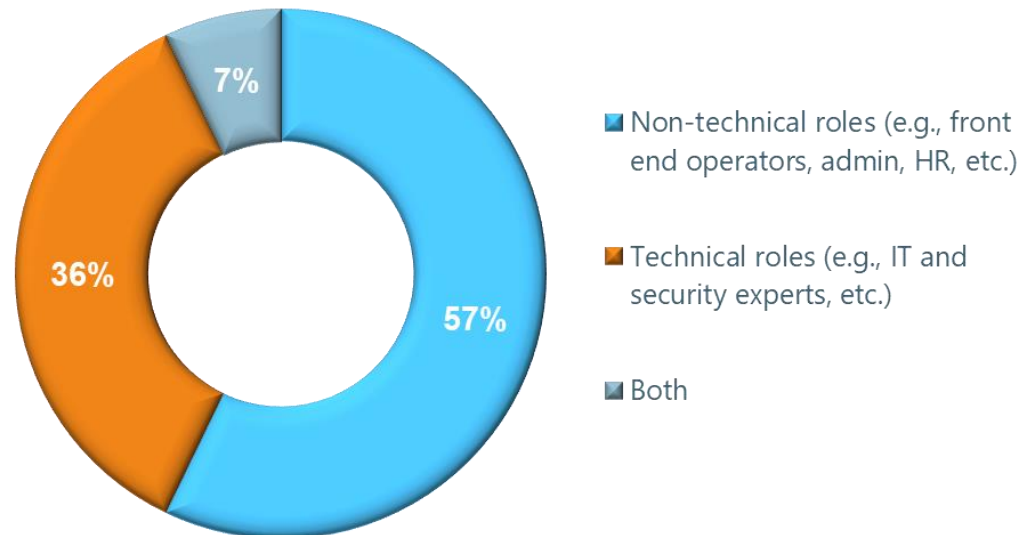


- No cybersecurity initiatives are organized.
- No, cybersecurity paths are taken out of the shelf.
- Yes, but only with small changes.
- Yes, but no distinction is made according to specific corporate roles.
- Yes, paths are fully customized and specific to different corporate roles.

# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

## SECTION 4: CURRENT GAPS AND CYBERSECURITY TRAINING NEEDS

WHAT ARE THE MOST VULNERABLE ROLES IN YOUR DOMAIN EXPOSED TO CYBER RISKS/ATTACKS? (Z5, 14 responders)



TO THE EXTENT OF YOUR KNOWLEDGE, WHAT **TECHNICAL ROLES** MOST NEED CYBERSECURITY TO UPSKILL OR RESKILL EDUCATIONAL PATHS? (Z9 + Q3, 26 responders)

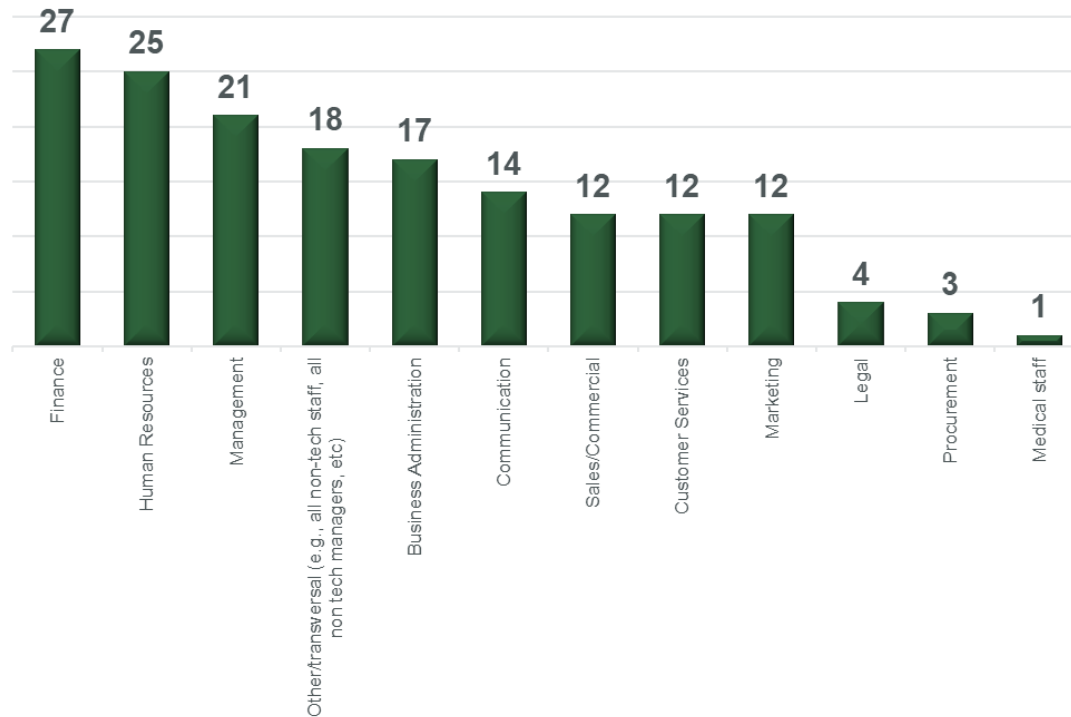




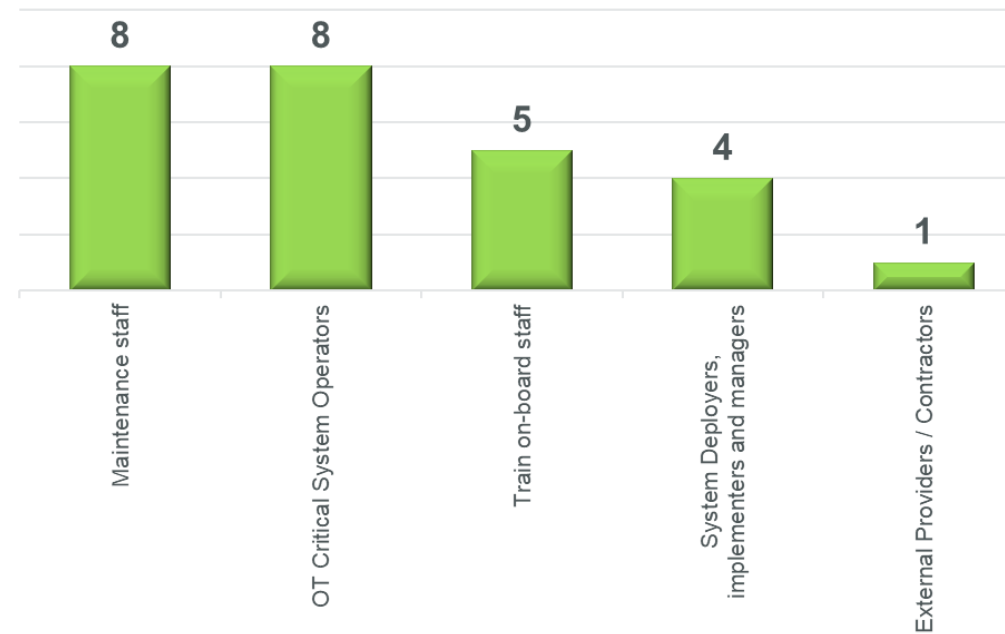
# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

## SECTION 4: CURRENT GAPS AND CYBERSECURITY TRAINING NEEDS

TO THE EXTENT OF YOUR KNOWLEDGE, WHAT **NON-TECHNICAL ROLES** MOST NEED CYBERSECURITY TO UPSKILL OR RESKILL EDUCATIONAL PATHS? (Q24 + Q4, 26 responders)



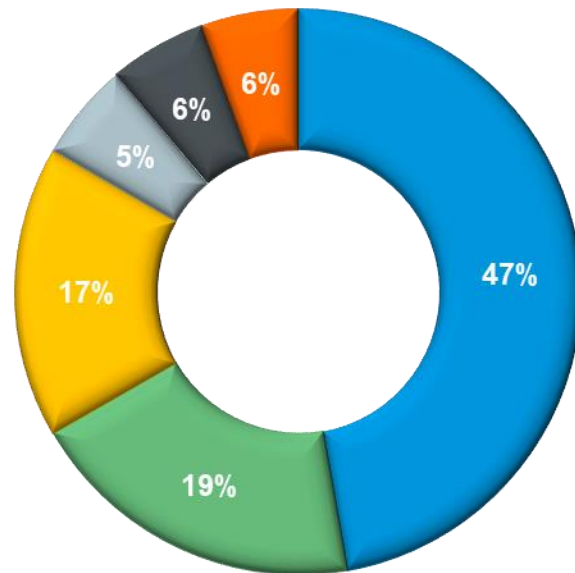
WHICH ARE THE **OPERATIONAL ROLES** IN YOUR ORGANIZATION THAT MOST NEED CYBERSECURITY AWARENESS EDUCATIONAL PATHS? (Q5, 12 responders)



# CYBERSECURITY TRAINING NEEDS AND PAINS - RAILWAY COMPANIES

## SECTION 4: CURRENT GAPS AND CYBERSECURITY TRAINING NEEDS

WHAT WOULD BE YOUR COMPANY'S DESIDERATA IN TERMS OF CYBERSECURITY TRAININGS? *(Interviews, 12 responders)*



LEGEND		
<span style="color: blue;">■</span>	Target-specific trainings	17
<span style="color: green;">■</span>	Exercises/Actions/Campaigns	7
<span style="color: yellow;">■</span>	Courses on Strategy, Standards & Regulations	6
<span style="color: grey;">■</span>	Industry/Company-specific trainings	2
<span style="color: black;">■</span>	Topic-specific trainings	2
<span style="color: orange;">■</span>	Trainings in national language	2

- (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 – awareness on 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.

# CYRUS PROJECT: NEXT STEPS

**2023**

**Consolidating the results and delivering the Competence Framework**

**2024**

**Designing role-specific training modules for each sector (Manufacturing and Transport)**

**2024**

**Delivering the first testing phase, collecting feedbacks and refining the courses.**

**2025**

**Delivering the final version of the tailored training modules.**

# PAST EU 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 –end 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](mailto:security@uic.org)



[www.uic.org/securit](http://www.uic.org/securit)



[@RailSecurityUIC](https://twitter.com/RailSecurityUIC)



[railsecurityhub.org](http://railsecurityhub.org)

## Head of Security Division



**Marie-Hélène Bonneau**

[BONNEAU@uic.org](mailto:BONNEAU@uic.org)

## Senior Security Research Advisors



**Grigore Havarneanu**

[HAVARNEANU@uic.org](mailto:HAVARNEANU@uic.org)



**Laura Petersen**

[PETERSEN@uic.org](mailto:PETERSEN@uic.org)

## Senior Security Advisors (seconded)



**Bruno De Rosa**

[DEROSA@uic.org](mailto:DEROSA@uic.org)



**Kacper Kubrak**

[KUBRAK@uic.org](mailto:KUBRAK@uic.org)

## Security Intern



**Grace Poley**

[POLEY@uic.org](mailto:POLEY@uic.org)