SURE5.0

Industry 5.0 webinar

Safe operation of heavy machinery through VR

Funded by the European Union

Please, turn off your camera and mute your microphone

VR / AR

Virtual Reality is a generic term for a set of immersive display and input technologies which create a feeling of being present inside a computer-generated environment.

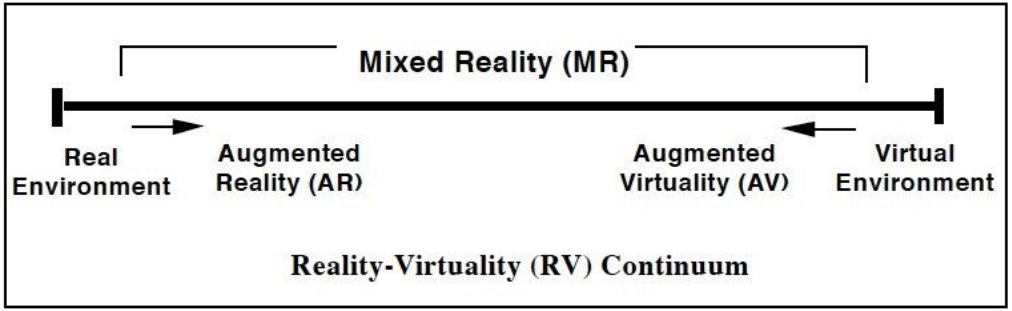
Augmented Reality is a set of technologies which allow to project virtual objects on top of the real world.

- A **high-end Human Computer Interface**
- It should **work in realtime**
- Interaction happens through **different sensorial channels** (multimodality)

Burdea and Coiet "Virtual Reality Technology"

Funded by the European Union

XR



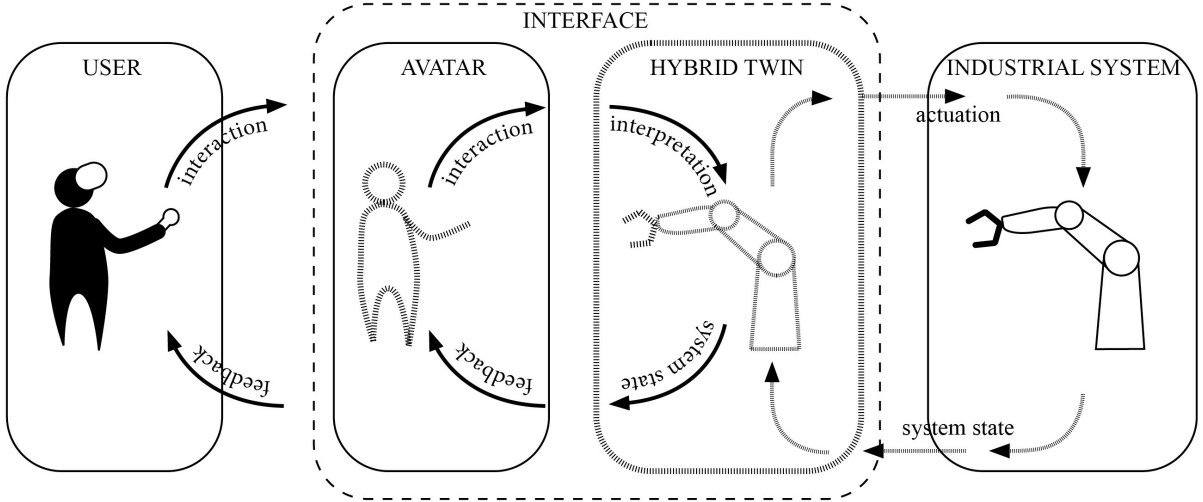
TECHNOLOGY DELIVERS THE **ILLUSION** YOU ARE IN STEP 1 WHEN, ACTUALLY, YOU AREN'T

USE OF **SENSORIAL** INPUTS

VR continuum Milgram et al. 1995

Funded by the European Union

DT based XR interfaces in HRI



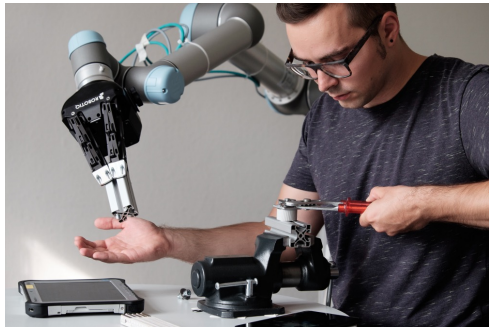
Funded by the
European Union

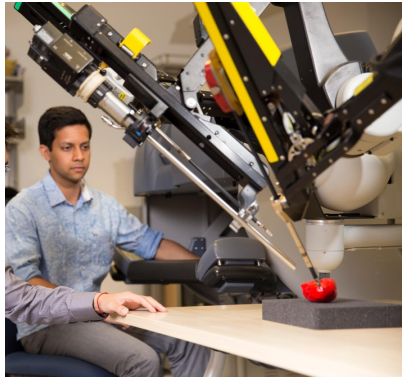
Opportunities

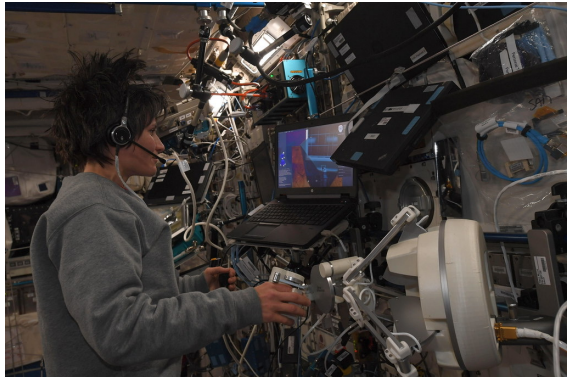
- Safe operation/collaboration in VR > no direct contact with heavy machinery
- Remote operation > accessing difficult environments in harsh conditions
- Training with DTs of real machines > fastening the learning process, optimizing repetitive procedures
- Testbenches for HRI and HRC > repeatability, easier data collection, safety
- Including the operator in the loop > user centered design approaches, assessment of human factors

Funded by the
European Union

Human Robot Interaction

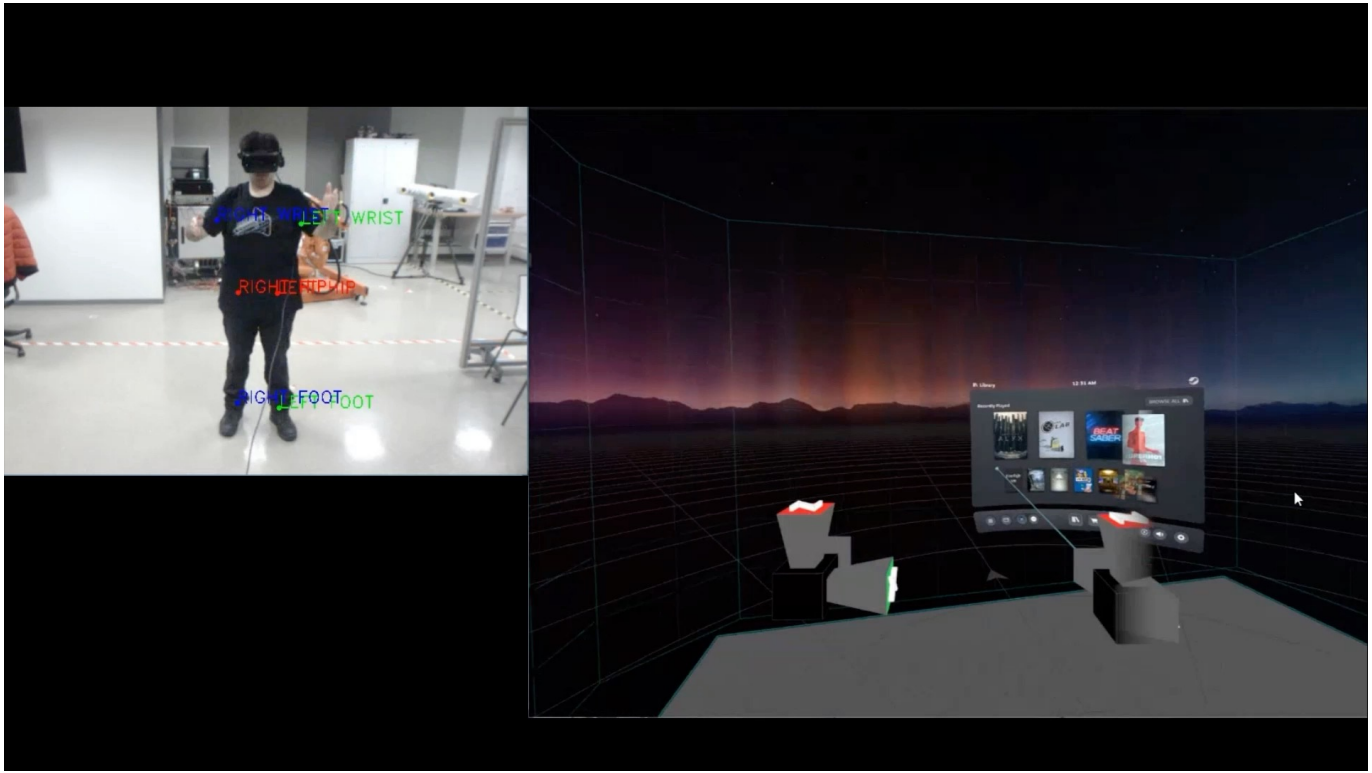






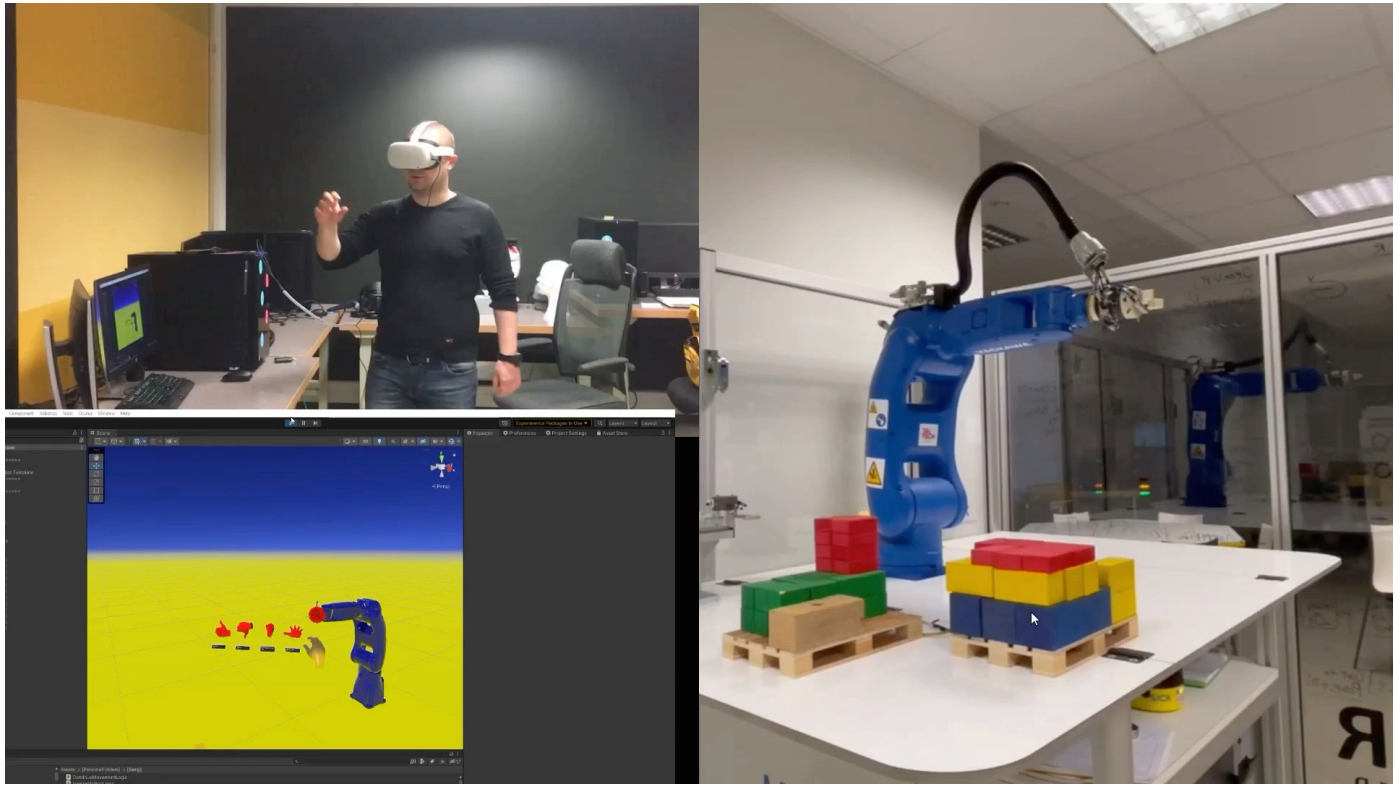
Funded by the
European Union

Camera based posture tracking



Funded by the
European Union

Gesture based VR UI for robot operation



Funded by the
European Union

AR UI for robot operation

Funded by the
European Union

VR UI for path planning and teleoperation

Funded by the
European Union

Criticalities

- Dependable on hardware technologies (including connectivity) and software architectures
- Lack of HRI standards using XR
- Use case dependable
- Privacy and cybersecurity concerns
- Assessment of human factors is difficult and there are no standardised metrics

Funded by the
European Union

SURE5.0

Thanks for your attention

www.sureproject.eu

Funded by the
European Union

SURE5.0

Cybersecurity in Production

Alexander Kreppein | Fraunhofer IPT | Germany
alexander.kreppein@ipt.fraunhofer.de

Funded by the European Union

SURE5.0

Inadequate cybersecurity measures are a major obstacle to digitalization in the manufacturing industry!

+126 Billion Euro Potential

estimated for manufacturing companies in Germany
through digitization by 2025

VS

Low Digitalization Rate

in large companies approx. 30%,
in SMEs approx. 20%

Cybersecurity as one of the main obstacles

Funded by the European Union

Source: McKinsey & Company (2019), iwconsult (2019), BITKOM (2020)

SURE5.0

Security in the operations technology (OT) is fundamentally different to security in the information technology (IT) sector

IT: Very common

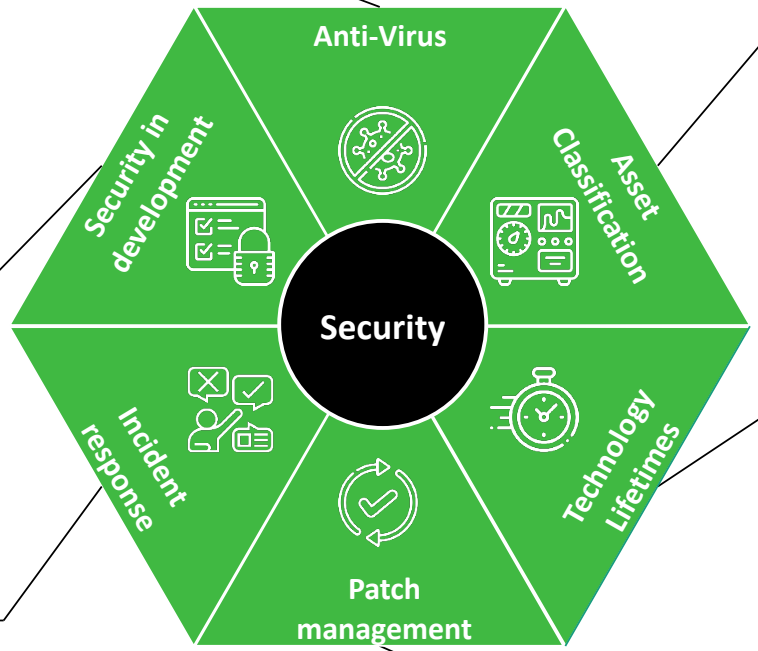
OT: Rare; Low hardware performance

IT: Integrated components

OT: Historically not considered

IT: Standard in most companies

OT: Focused on resumption of the system



IT: Regularly performed

OT: Only if committed

IT: 3 to 5 years

OT: 10 to 20 years

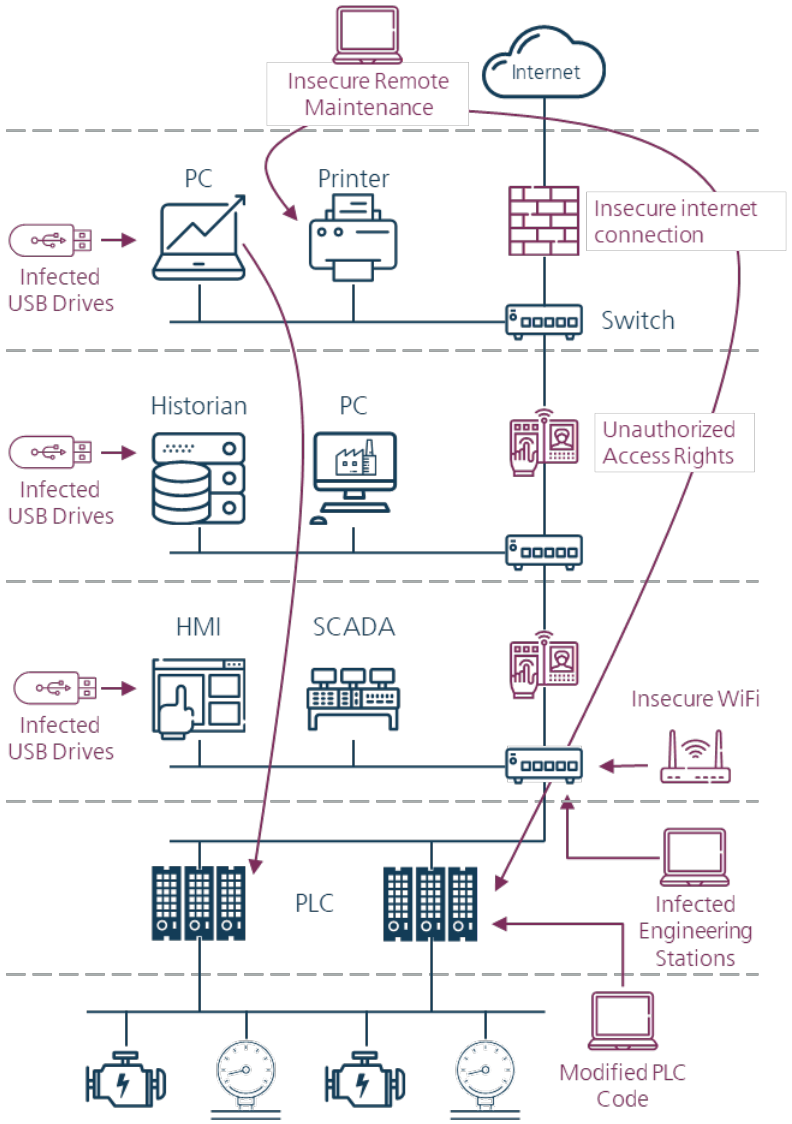
IT: Standard, regular and simple

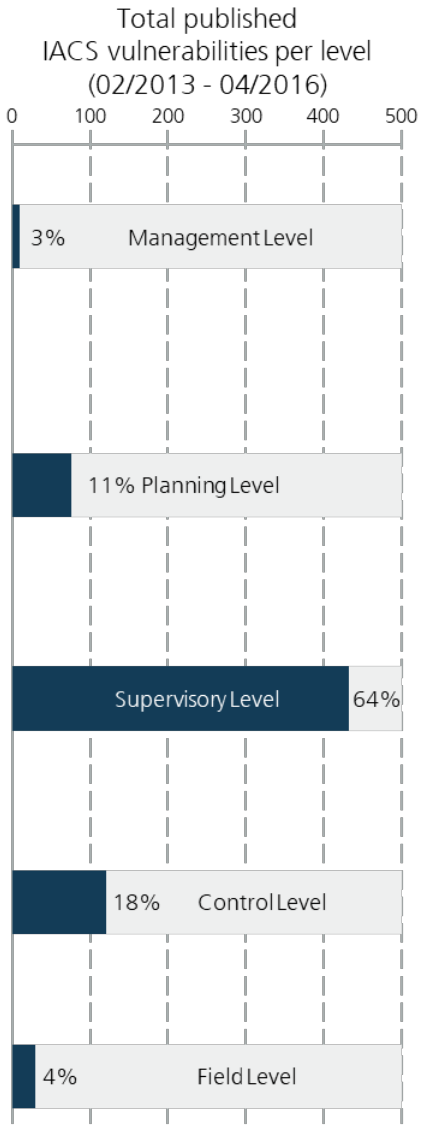
OT: Manufacturer-dependent and costly

Funded by the European Union

Source: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R; https://latesthackingnews.com/2020/12/26/flavor-and-fragrance-giant-symrise-ag-hit-by-clop-ransomware; https://www.abc12.com/2021/02/25/fbi-state-police-probing-cyber-hack-on-saginaw-township-schools/; https://securityaffairs.co/wordpress/112494/malware/clop-ransomware-symrise.html

Security weaknesses are often exploited within the supervisory control level





Funded by the European Union

A successful cyberattack causes severe damages to the affected company

Norsk Hydro Hacking Case

In 2019, Norsk Hydro, a multinational aluminum manufacturer with operations in 40 countries, closed many of its plants due to a cyberattack

The Company

Norwegian aluminum manufacturing

The Attack Results

$ 71 million in losses [1]

22.000 computers were hit

3 factories shut down

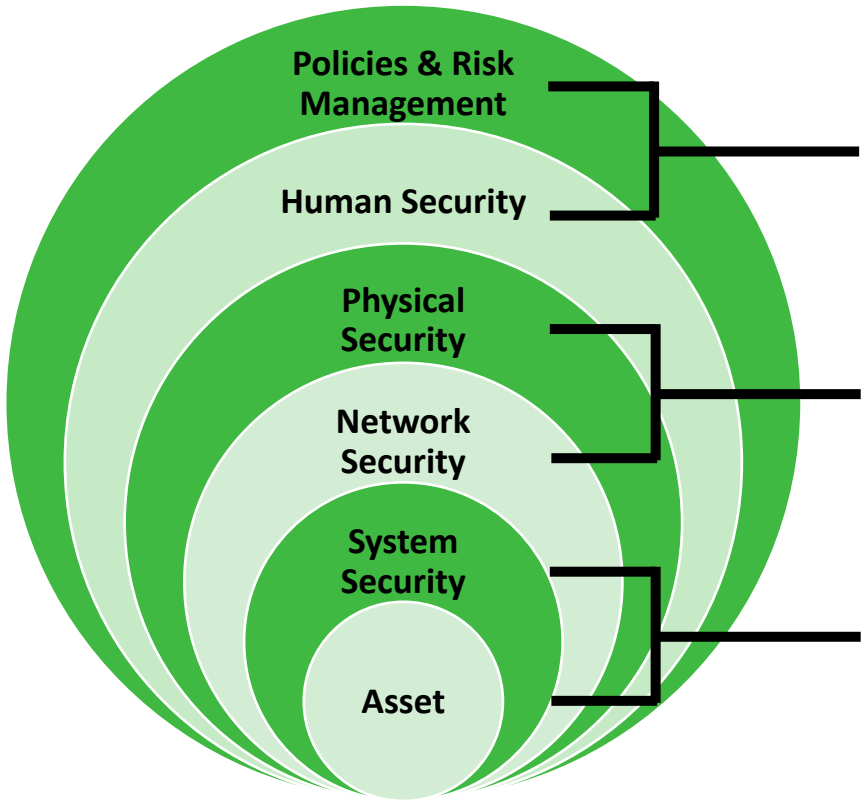
(Brazil, Qatar, and Norway)

Source: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Funded by the European Union

SURE5.0

Defense in Depth Strategy – Creating security layers around assets



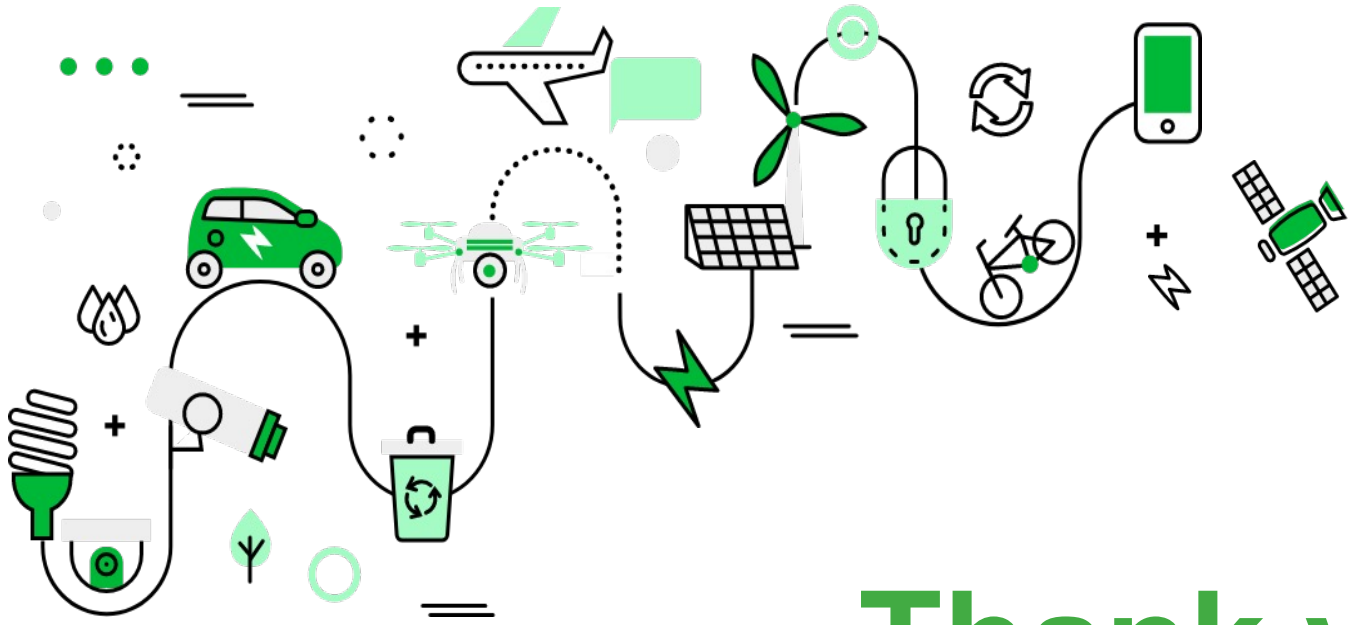
The three layers in Defense in Depth:

Administrative: The company's organization and processes regarding security

Physical: Includes any physical security measures that prevents access to

Technical: Soft- and Hardware based technologies to protect systems and assets

Funded by the European Union



SURE5.0

Thank you

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

CYRUS enhanced cybersecurity skills

SURE5.0

Industry 5.0 webinar

Rethink Cybersecurity from the human-element point of view

Funded by the European Union

Please, turn off your camera and mute your microphone

v2

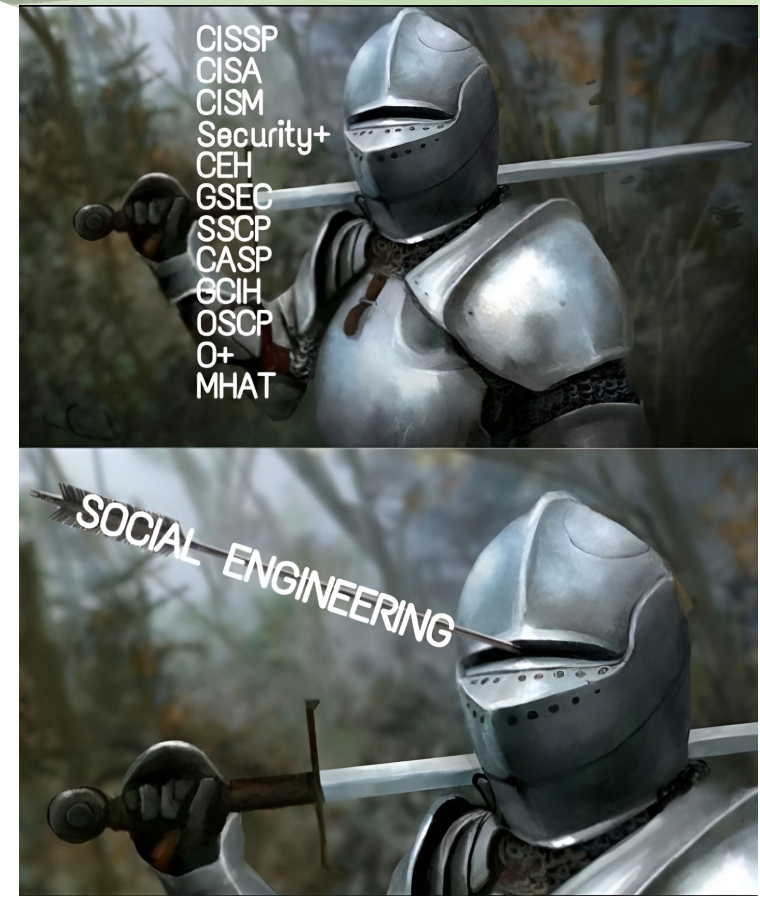
Social Engineering never disappears

Emotet is again active in Italy (01/11/2022)

A new campaign targeting Italian targets involves sending an email containing a password-protected ZIP attachment with an XLS file that contains malicious macros.

To get infected, a user needs to follow several steps. They must open an email with infected files, unzip and enter the password, enable Office macros by opening the Excel file, ignore any warnings on the screen, and switch off any suspect.

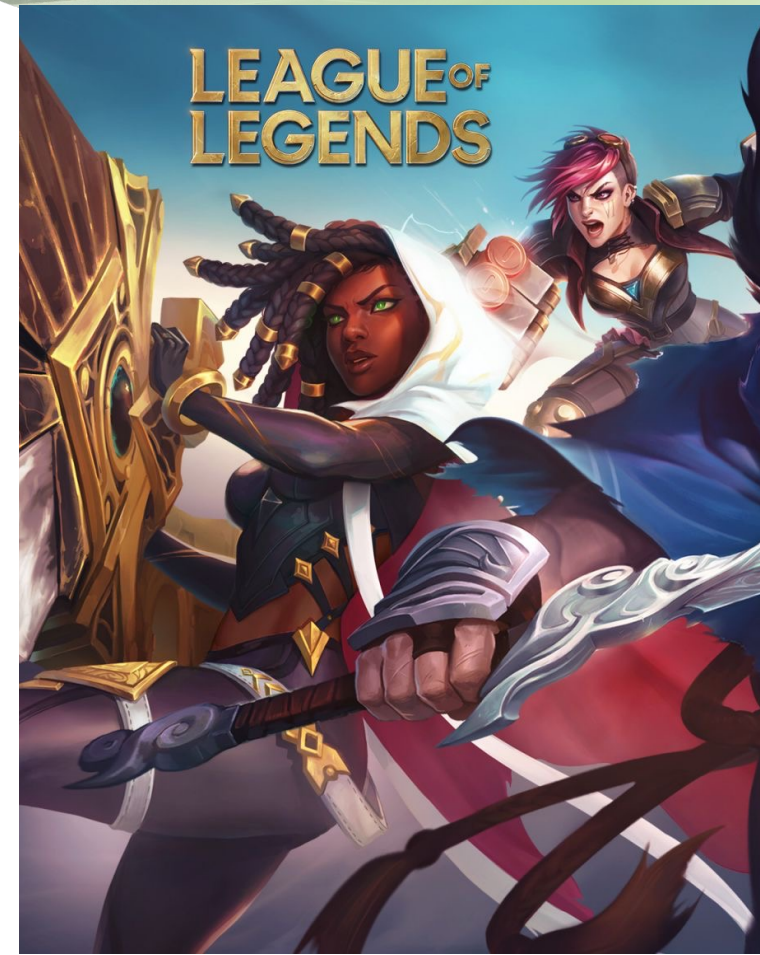
A user must manually do all these things!



Funded by the European Union

Social Engineering never disappears

- **Riot Games** nodded that it was a social engineering victim in December 2022.
- They claimed to have received a ransom of $10,000,000 and **refused to pay**.
- As a result, the source code for **League of Legends** is now for sale online.



Funded by the European Union

When did Social Engineering begin?

Funded by the European Union

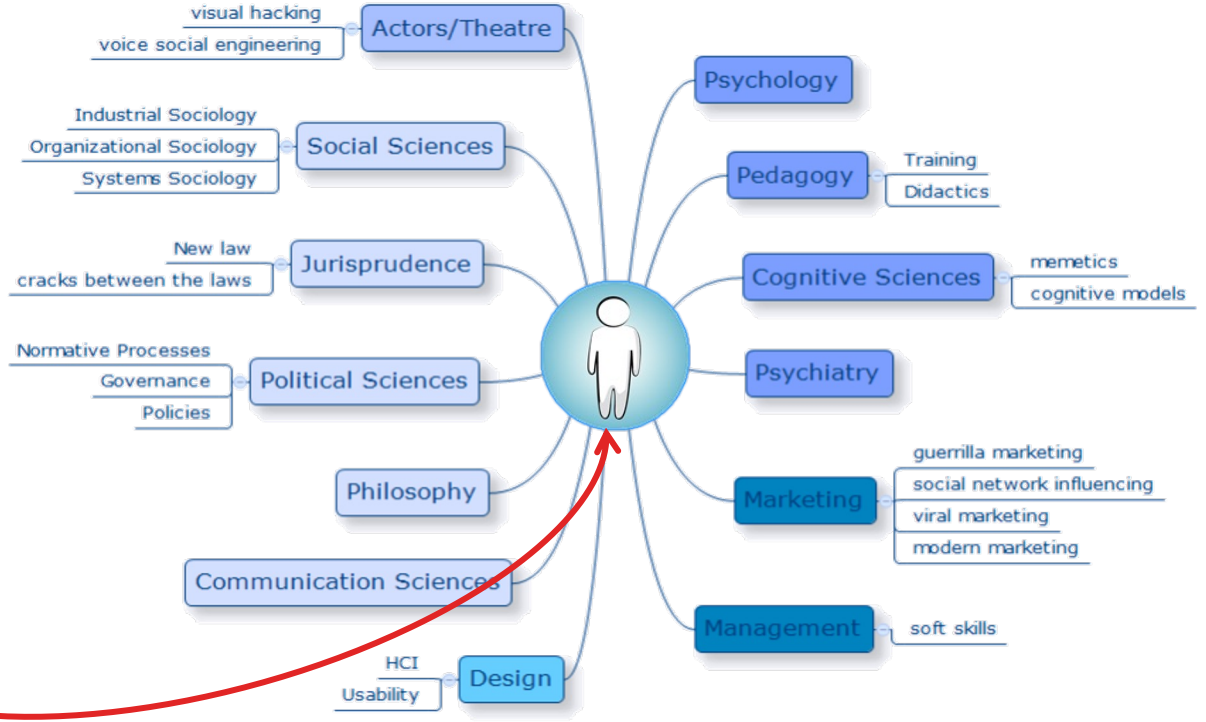

HUMAN

+

AN ELEMENT ABUSED BY ALMOST ALL THE ATTACKS, BY ALL THE CYBERCRIMINAL AND CYBERTERRORISM GROUPS

An element abused by all the CC/CT groups

- The human IS the “system” under attack
- Question: which sciences contribute to modelling the attacked systems?
- By definition, it is a multidisciplinary problem



Funded by the European Union

Rethink cybersecurity from the human element point of view

- WEF/IBM (2022), 95% of cybersecurity breaches result from human errors.
- 95% of risks (e.g., social engineering) are faced with less than 5% of the Organisations' IT security budget.
- Much of the cybersecurity market instead concentrates on the technical side of an attack (IT or OT).

Funded by the European Union

Things that require protection

HARDWARE

SOFTWARE

WETWARE

Funded by the
European Union

Uncharted cyber risks: what we still struggle to estimate correctly

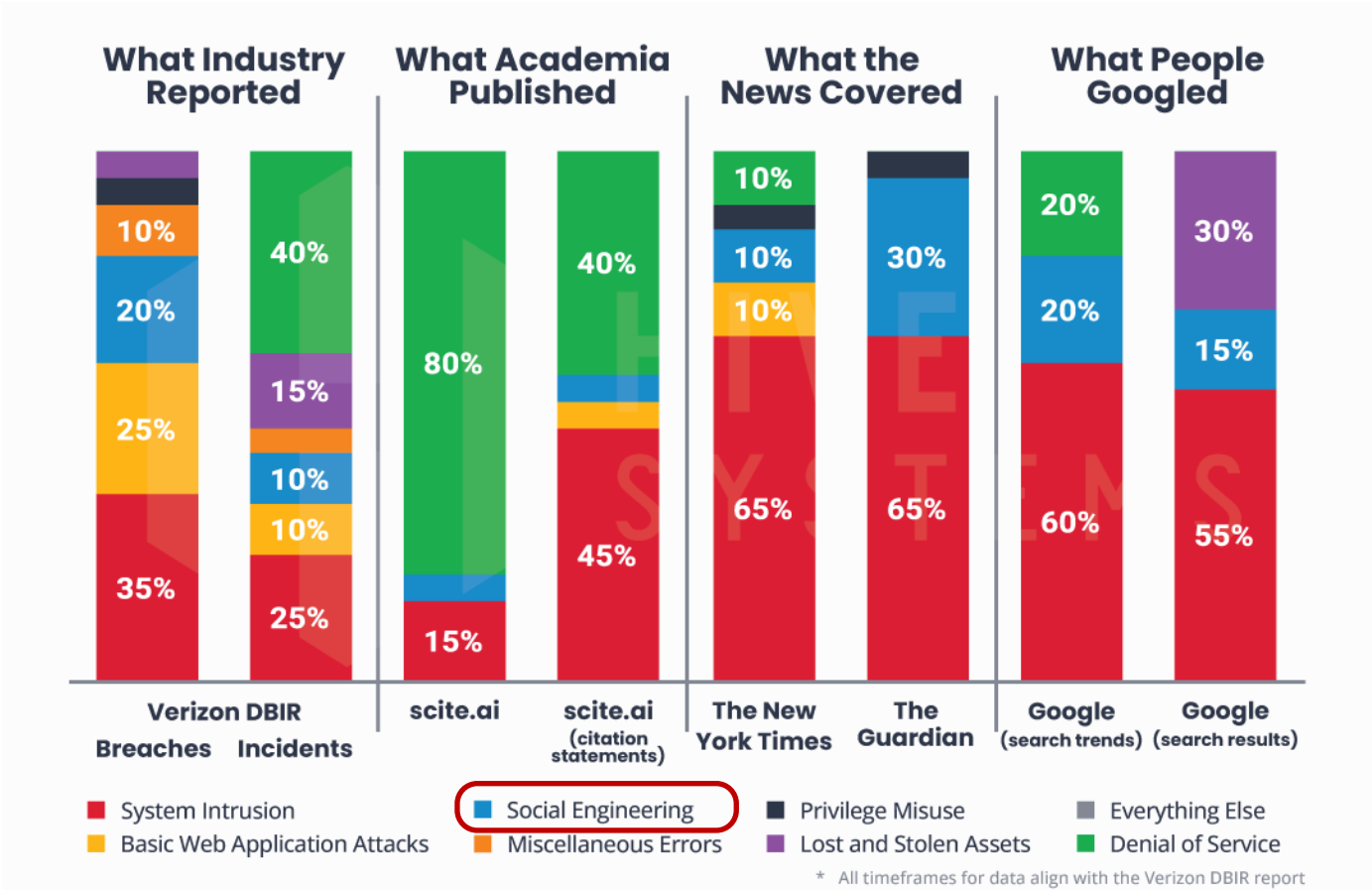
HARDWARE

SOFTWARE

WETWARE

Funded by the
European Union

The cybersecurity incident and breach perception problem in 2023



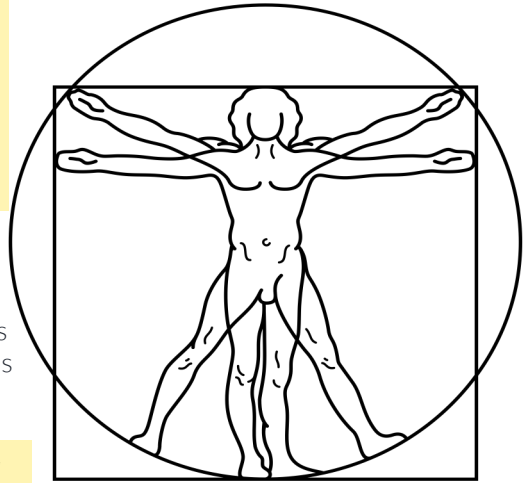
Rethink cybersecurity from the human element point of view

SURE5.0

1. **Special Education Tracks**
Special education tracks are built around the organisation's culture to communicate the emergencies and maximise the impact of training (e.g., People Analytics)

2. **Vulnerability Assessment/Penetration Testing of the human element**
Vulnerability Assessment of the human element, such as phishing campaigns or simulated attacks, to test people's resilience, employees of IT staff (e.g., SDVA, FSVA).

3. **Training as a defence instrument to reduce cyber risk**
Training pathways aligned with the European Competency Framework (e-CF) or minimum skill set but proportionate to the business sector, role and assets under management.



4. **Threat intelligence of the human layer**
Ethical and legal constraints are the core problem when dealing with humans; threat intelligence must consider them (e.g., ethical or automated OSINT).

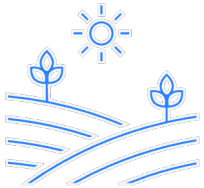
5. **Simulation of human-related threats and attack patterns**
It is necessary to simulate human attacks in cyber ranges, including both human and technological aspects of an attack, such as Gold Teams beside Red/Blue and improve tabletop exercises.

6. **AI for mitigation of human-related threats**
The use of anti-deception systems and systems to assist people in suggesting correct behaviours and avoiding risks, creation of a corporate mind firewalls and use of Human Sensor Networks.

7. **Integrated estimation of the cyber risk, including IT, OT and Human Risk**
Integration of human, operational, and information technology risk models, including human risk management and integrated risk models.

Funded by the European Union

Rethink cybersecurity from the human element point of view



- It is a **multicultural** problem that requires different competencies, not only technical.
- The human element of security is a genuinely multicultural and interconnected approach that brings new opportunities to IT security.

The key is the interdisciplinarity of competencies.

1. IT experts
2. Cognitive science
3. Cyber Risk modelling
4. Cyber sociology,
5. Psychologists
6. Philosophy
7. Political sciences
8. Pedagogy
9. Acting performance
10. Marketing experts
11. Designer
12. ...

Funded by the European Union

The importance of Education

CHALLENGE

- Training/learning of employees and contractors is a critical step in increasing the security of the human element.
- The challenge is to **create impactful, long-lasting learning paths.**

SCOPE

The target is:

- Gold Teams
- IT experts
- Employees
- …

> ***"Cybersecurity narrative is too tech-intensive; there are cybersecurity career paths that do not include breaking bits."***
>
> *Jean-Christophe Gaillard, founder of Corix Partners*

> ***"Third generation security awareness programs should be expected to become more effective, with maximal use of creative, multi-media training options."***
>
> *Outlook for 50 Cyber Controls, Tag Cyber, 2020Third-generation*

Funded by the European Union

SURE5.0

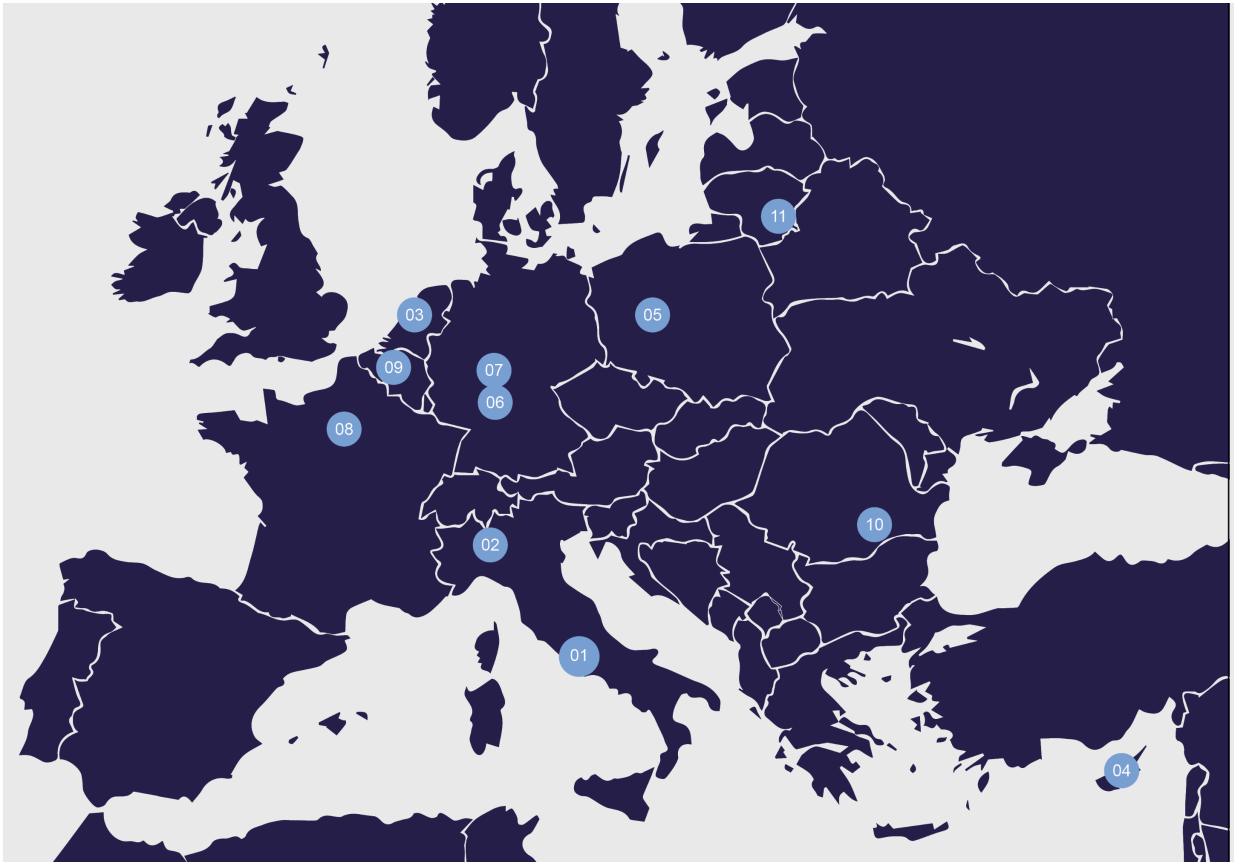
CYRUS

enhanced cybersecurity skills

Funded by the
European Union

CYRUS EU Funded Project

SURE5.0



01 deepblue consulting & research

02 Cefriel POLITECNICO DI MILANO

03 VU VRIJE UNIVERSITEIT AMSTERDAM

04 silensec

05 Polish Platform For Homeland Security

06 eit Manufacturing CLC CENTRAL Co-funded by the European Union

07 CAMERA DI COMMERCIO ITALIANA PER LA GERMANIA ITKAM ITALIENISCHE HANDELSKAMMER FÜR DEUTSCHLAND

08 uic

09 EWF

10

11 LITHUANIAN INNOVATION CENTRE

Traditional security awareness and training programs don’t work …

Funded by the
European Union

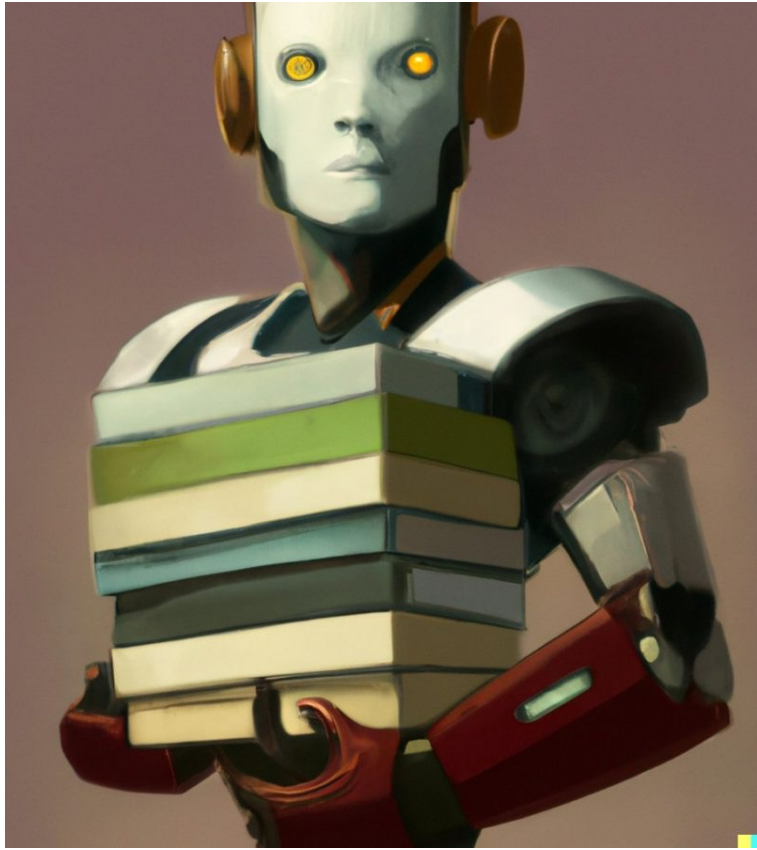
Skills shortage

Only **14% of organisations set a long-term workforce strategy** focused on the skills, competencies and roles needed in 5-10 years. [Gartner]

48% of organisations are currently struggling to find and hire cybersecurity professionals [Gartner]

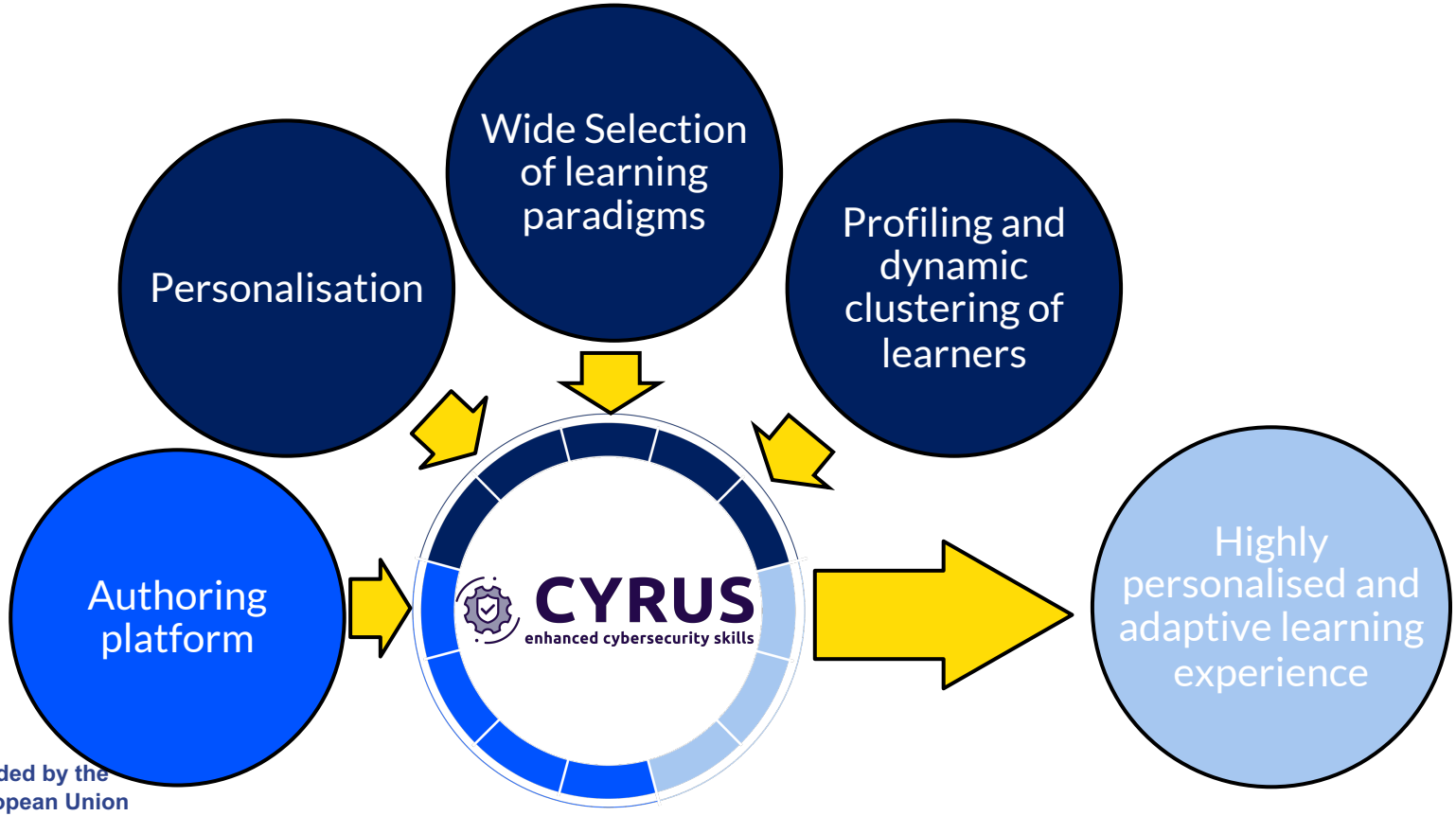
Huge cybersecurity skill gap, especially in sectors where technology is mission-critical. Worsening trend until 2030, whose effects are **dooming today's cybersecurity landscape**: the current offering is below the market demand while the threats are high. [CYRUS, ENISA].

People do not have time to follow training [CYRUS]



Funded by the European Union

A new learning paradigm?



Funded by the European Union

Contacts

Enrico Frumento

Cybersecurity Research Lead

Cefriel - Politecnico di Milano

www.cefriel.com

Viale Sarca 226 – 20126 Milano – IT

https://www.linkedin.com/in/enricofrumento/

http://www.cyrus-project.eu/

Funded by the European Union

SURE5.0

Thanks for your attention

www.sureproject.eu

Funded by the
European Union