



# AI supporting Cyber Risk Management and Resilience of Critical Infrastructures

30<sup>th</sup> September 2024

# AI Supporting Cyber Risks And Resilience Of Critical Infrastructures

Insights From CS-AWARE NEXT, DYNABIC, & AI4CYBER



Join us

**30 September 2024**

16:00 – 17:30 CEST



**Prof. Juha  
Röning**

*CS-AWARE NEXT Project  
Coordinator, University of Oulo*



**Erkuden  
Rios**

*AI4CYBER and DYNABIC  
Project Manager, TECNALIA*



**Victor  
Muntés-Mulero**

*Exploitation and Innovation  
Manager at DYNABIC, Beawre*

In collaboration with



## 16:00 – 17:00 – AI Solutions supporting Cyber Risk Management



### **Design-Science and AI harnessed for improving Cybersecurity on infrastructure ecosystems**

Prof. Juha Röning, Professor at the University of Oulu, CS-AWARE NEXT Coordinator  
- Q&A



### **Smart Risk Management for Business Continuity in Critical Infrastructure**

Victor Muntés-Mulero, Co-founder and CEO at Beawre, Exploitation and Innovation Manager at DYNABIC  
- Q&A



### **Trustworthy AI for cybersecurity solutions**

Erkuden Rios, AI4CYBER and DYNABIC Project Manager, TECNALIA  
- Q&A

## 17:00 – 17:30 - Roundtable with speakers

Chair – Nicholas Ferguson, Trust-IT & ECCO

- The webinar is being recorded. A link to the full recordings will be shared with participants afterwards
- You're welcome to ask questions! Please use Q&A panel to ask your questions: we will activate your microphone.
- You can also raise your hand during the dedicated Q&A time
- Roundtable at the end for further questions!

# Design–Science and AI Harnessed for Cybersecurity Infrastructure Ecosystem

Juha Röning

BISG

University of Oulu

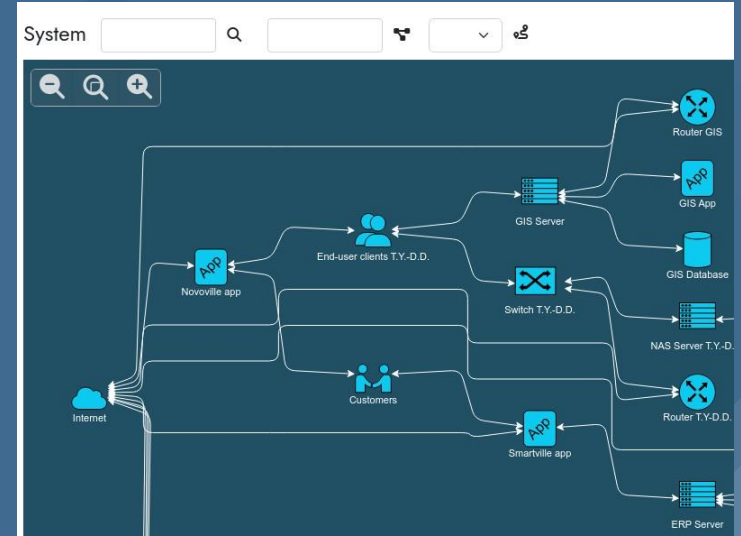
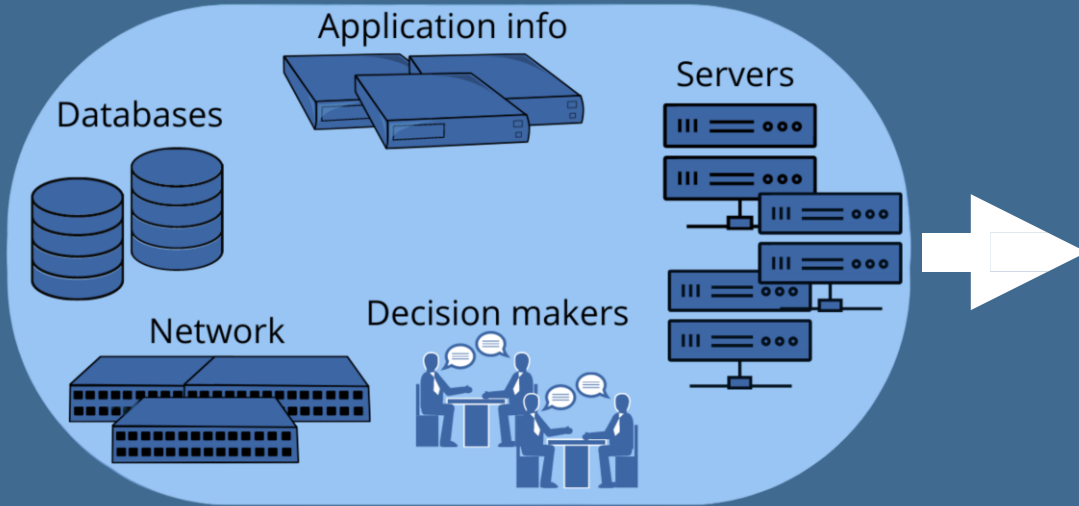
Finland

[Juha.Roning@oulu.fi](mailto:Juha.Roning@oulu.fi)

# The CS-AWARE H2020 project

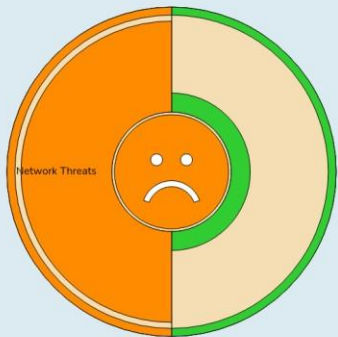
- A socio-technical systems based approach to cybersecurity management in organisations based on awareness
  - Humans are a central factor in any complex system
  - CS-AWARE enables humans to be part of the solution in solving cybersecurity issues
- 2 pillars
  - **Analysis:** Socio-technical workshops allow the people working in an organisation to specify their systems, and how they work in practice (co-design)
  - **Monitoring:** Provide the technical capability for data-driven real-time monitoring and managing the system as specified by the people of an organisation

# CS-AWARE process – Analysis



# CS-AWARE process – Monitoring

22/02/2024



Network Threats

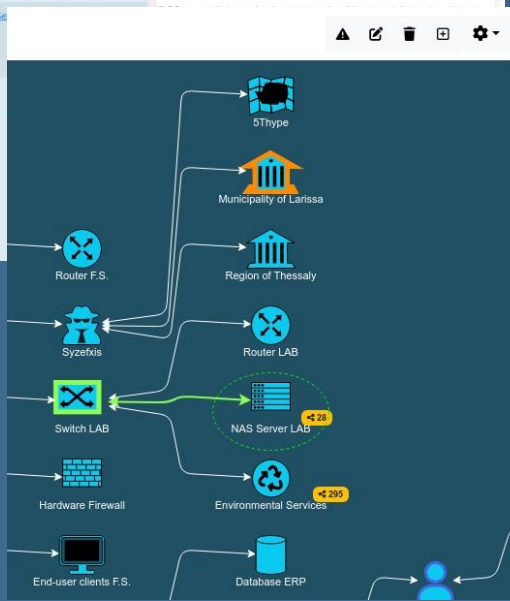
Top Threats

| Severity | First observed    | Assigned to         | Group           | Where                    | Name   |
|----------|-------------------|---------------------|-----------------|--------------------------|--|
| Severe   | 02/11/2023, 08:04 | patfred@rheasoft.dk | Network Threats | Municipality of Larissa  | RCE exploit for Wyze Cam v3 publicly released, ... |
| Moderate | 19/11/2023, 15:17 | kim@rheasoft.dk     | Network Threats | Novoville.app, Customers | Uanset om du er ny til Whats App eller en lang ... |
| Low      | 28/11/2023, 15:13 | kim@rheasoft.dk     | Network Threats | Telemetry.S...           |  |
| Low      | 27/02/2017, 22:37 |                     |                 |                          |  |

Cybersecurity Posts Summary

The role of cybersecurity is to protect computer systems, networks, and data from unauthorized access, theft, disruption, or damage. It encompasses technologies, processes, and practices designed to safeguard digital assets and ensure the confidentiality, integrity, and availability of information [\[source\]](#).

The US government shares tips for water utilities to defend against cyberattacks, outlining top actions like reducing exposure of assets to the internet and implementing multifactor authentication [\[source\]](#).



NAS Server LAB

| Created at        | Text   | Keywords            |
|-------------------|--|---------------------|
| 22/02/2024, 08:52 | Blackhat Asia Conference Hi there, Thinking about attending my first ever... | BlackHat, Black Hat |
| 20/02/2024, 20:24 | When it comes to ransomware attacks, median initial ransom demands for...    | BlackCat            |
| 20/02/2024, 12:30 | Police arrests LockBit ransomware members, release decryptor in global...    | BlackCat            |
| 19/02/2024, 22:38 | LockBit ransomware disrupted by global police operation [LockBit]...         | BlackCat            |
| 17/02/2024, 09:29 | How to be on the same network that provides internet? If I am going to be... | Black Hat           |

1 2 3 4 5 6 . > >>

Some new resource

Node Type

Category



# CS-AWARE commercialization

- A start-up was founded by core partners of the CS-AWARE project
  - Common exploitation of IP developed during project
  - Common exploitation allows establishing strong branding
  - Development to market readiness
  - Establishing sales channels
- Challenges
  - A TRL7 pilot demonstrator is not a market ready product, additional funding is required for commercialisation
  - Attracting funding at such an early commercial state is challenging
  - We are trying to fundamentally change how organisations manage cybersecurity. Not easy to convince customers, even if offering may be superior.
- We are now in a market ready state with the CS-AWARE lite platform, and are hopeful to have our first customers in 2024

# Why CS-AWARE-NEXT?

- Core insight from CS-AWARE project
  - Improving cybersecurity within an organisation is not enough, as organisations are part of ecosystems
- Inter-organisational collaboration
  - Using the CS-AWARE platform as the basis for organisational cybersecurity management, how can we support collaboration among organisations (e.g. supply chain), with a focus on improving regional collaboration
  - Collaboration does not simply happen because it is required, it needs support and focus to develop norms and practices

# CS-AWARE-NEXT Objectives

- The project has 8 objectives, clearly linked to the project work plan
  - Data-driven inter-organisational collaboration as the overarching theme
  - Enabling dynamic and pro-active cybersecurity management

# CS-AWARE-NEXT Objectives

## Objective 1

Dynamic  
policy support

WP1

Ecosystem  
Collaboration

AI based data  
correlation

BC/DR and  
self-healing

Information  
sharing

## Objective 6

Benchmarking  
and Profiling

WP7

## Objective 7

Implementation, Integration and deployment

WP6

## Objective 8

Design science based project implementation and validation

WP7

# Design–science based project implementation

“

In the design-science paradigm, knowledge and understanding of a problem domain and its solution are achieved in the building and application of the designed artifact

-- Hevner et. al., Design Science in Information Systems Research

”

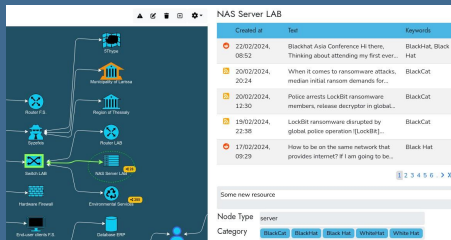
# Design–science based project implementation

- Design and implement information system artifacts
- **Co-design:** build around user needs, together with the users
- **Iterative design and validation:** Validate various states from conceptualisation to implementation with end users, and adopt according to insights gained

# Tools for supporting regional cybersecurity collaboration

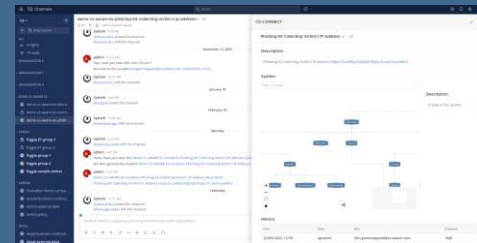
## CS-AWARE PLATFORM for information and awareness

- Organisational level
  - Policy support
  - New AI-based data and information engine
  - BC/DR support, self-healing
  - Information sharing with authorities

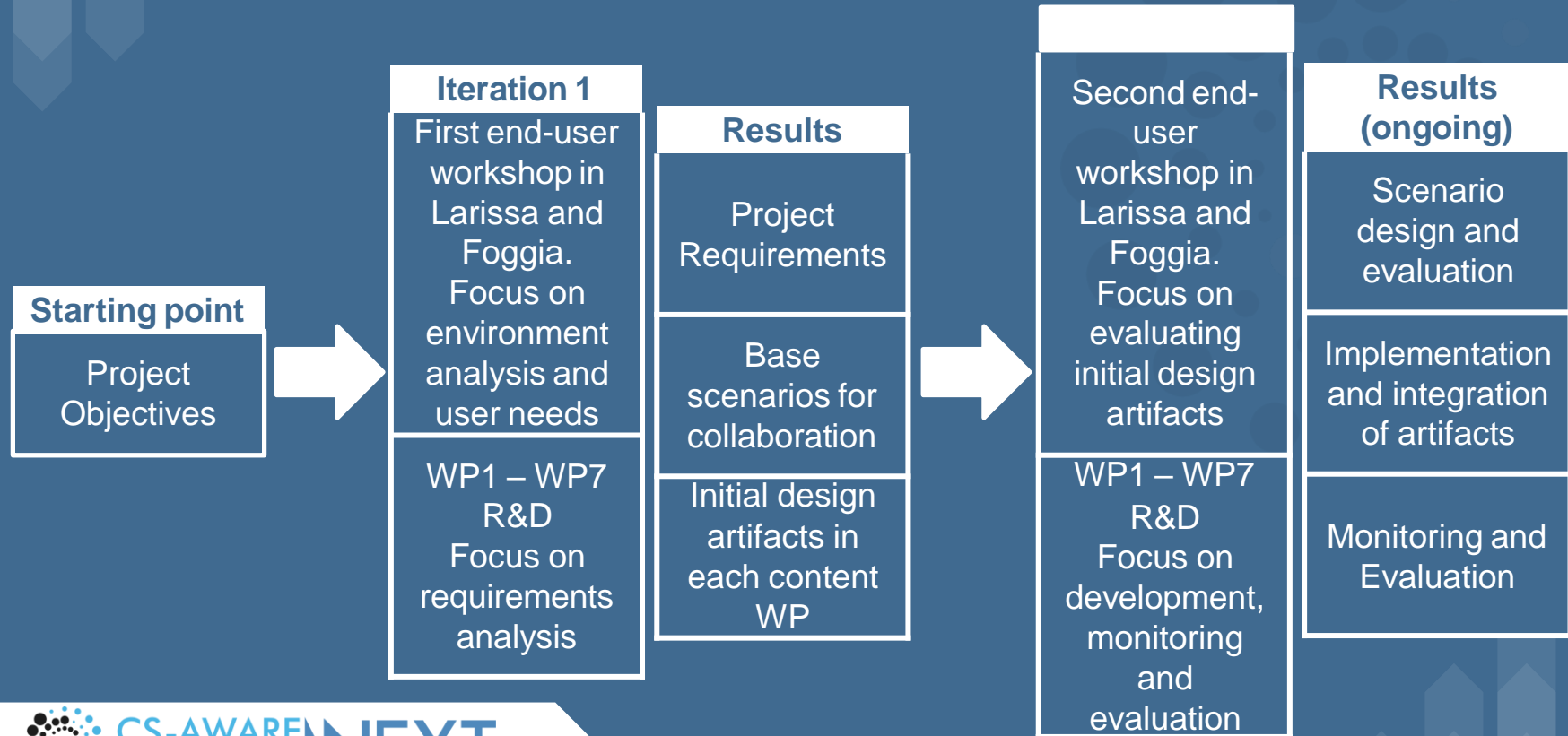


## CS-CONNECT as collaborative interface

- Ecosystem level collaboration
  - Mattermost-based
  - Co-designed collaboration scenarios
- Data-driven
  - Integration with data from
  - CS-AWARE platform
- Availability of AI-based contextualized data



# Project implementation overview





# Two representative pilot regions

## Pilot regions reflect current state in Europe well

- Larissa region
  - NIS sectors focus
  - Medium to high cybersecurity maturity
  - Pre-existing collaborations (e.g. health sector)
  - **Driver:** European legislation
  - High understanding of benefits of collaboration, and high motivation work together
- Foggia region
  - Industry focus
  - Low technology use and thus low cybersecurity maturity
  - **Driver:** customer demands
  - Reservations about inter-organisational collaboration (e.g. competitor rivalry)

# *Smart Risk Management for Business Continuity in Critical Infrastructure*



Funded by the  
European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070455.

**Disclaimer:** 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 European Commission. Neither the European Union nor the European Commission can be held responsible for them.

# The Challenge

Unforeseen **cascading impacts** within critical infrastructures, and inadequate management of business interruptions, leads to **financial losses in the millions and reputational damage**

**Ineffective risk management** due to lack of business awareness results in misguided risk mitigation efforts and diminishes decision-makers' control.

**Lack of standard-based technical security** testing makes training of Business disruption risk managers long and expensive.



An aerial photograph of an industrial facility, likely a refinery or fuel storage terminal. The facility is dominated by hundreds of large, white, cylindrical storage tanks arranged in neat rows. In the foreground, a large yellow tanker ship is docked at a pier, with other smaller vessels nearby. The background shows a body of water and a distant city skyline under a clear sky.

# Cyber-attack strikes German fuel supplies

*January 2022*

**Company paid \$11m in ransoms to the  
criminals who hacked them**

# Hackers hit Norsk Hydro with ransomware

*December 2019*

**The financial impact would eventually  
approach \$71 million.**





# Cyberattack Forces a Shutdown of a Top U.S. Pipeline

*May 2021*

**Shut down its 5,500 miles of pipeline, which it says carries 45 percent of the East Coast's fuel supplies**

**This caused a significant disruption in the supply of gasoline, diesel, and jet fuel across the East Coast, leading to fuel shortages and increased prices.**

**The company paid a ransom of nearly \$5 million to regain control of their operations.**

# RISKM4BC

RISKM4BC is a dynamic business risk management framework. Designed to offer both design and operational support, this tool is specifically tailored for cascading impact assessment and real-time risk quantification within the chain of Critical Infrastructures (CIs).



Control risks related to **cascading effects** among multiple interrelated CIs.



**Prediction of unwanted incidents and risk** to meet deadlines in your **workflows** to mitigate business disruptions.



**Bowtie Smart Center** to automate risk identification and predict threats.



Automated **link between business goals and lower-level system risks** leveraging LLMs.

# Technology

## Key technical features:

- Automated **risk likelihood and impact learning**.
- Risk propagation through **cascading effects** calculation.
- Workflow digital twins for **workflow execution prediction**.
- Live preventive and mitigative action **recommendation in natural Language**.
- Automated link of **business goals** with system risks.



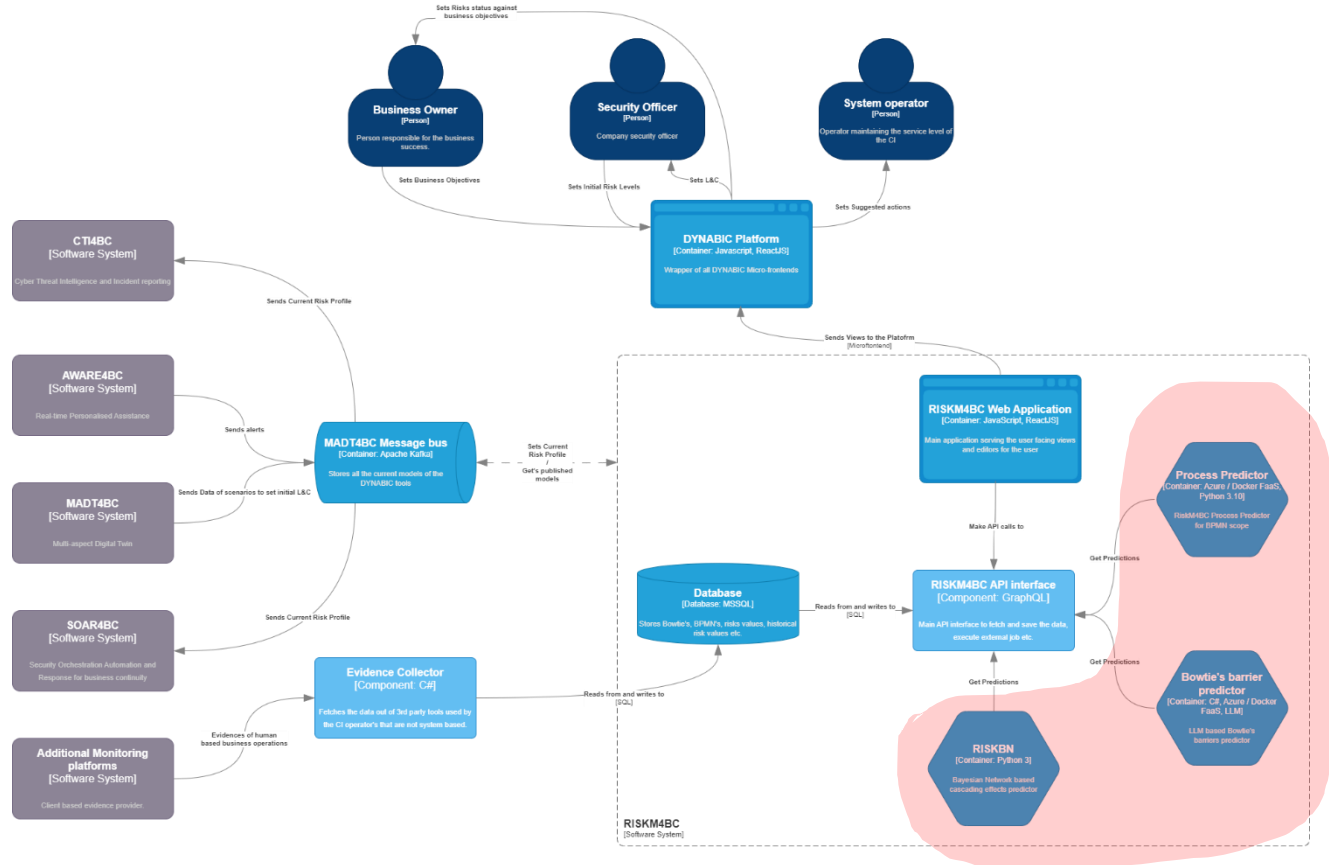
**Proprietary predictive AI algorithms**  
(transformers, LSTM, ...)



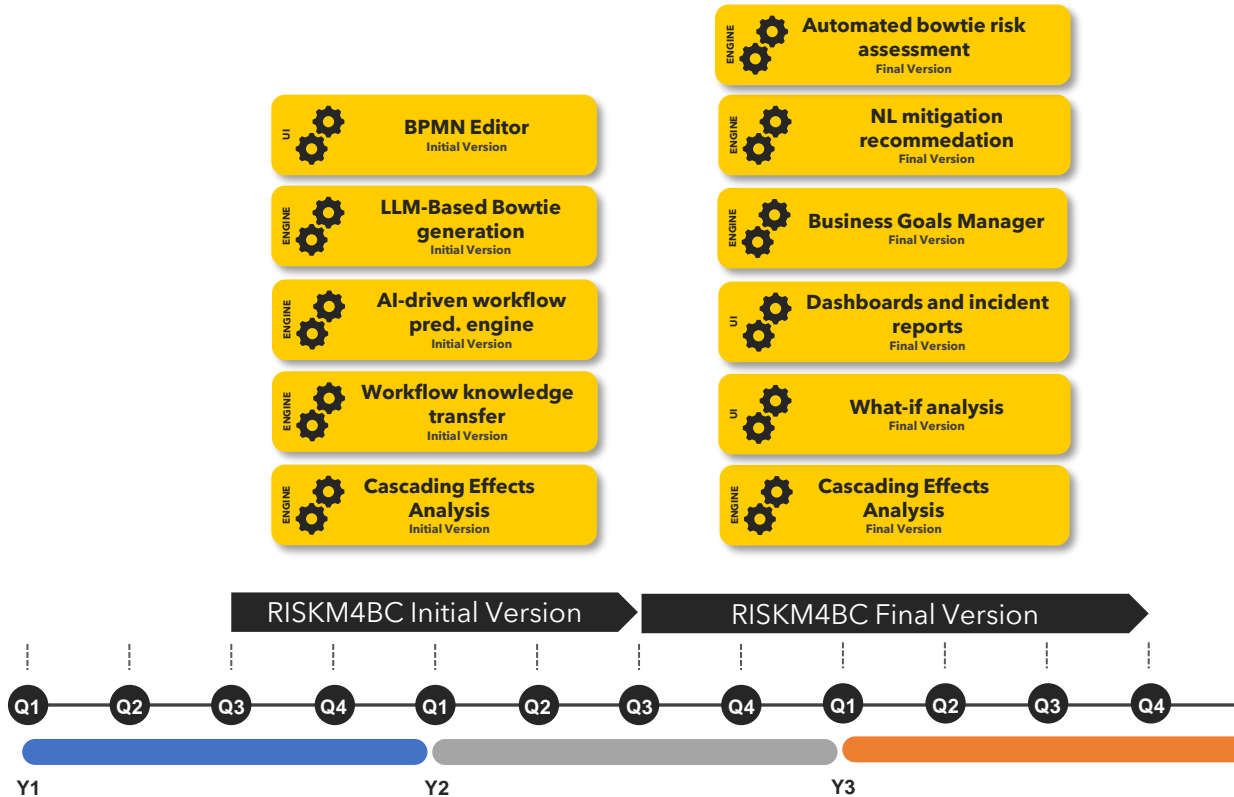
**Advanced use of the latest**  
**innovations in generative AI (LLM)**



# RISKM4BC Context within DYNABIC

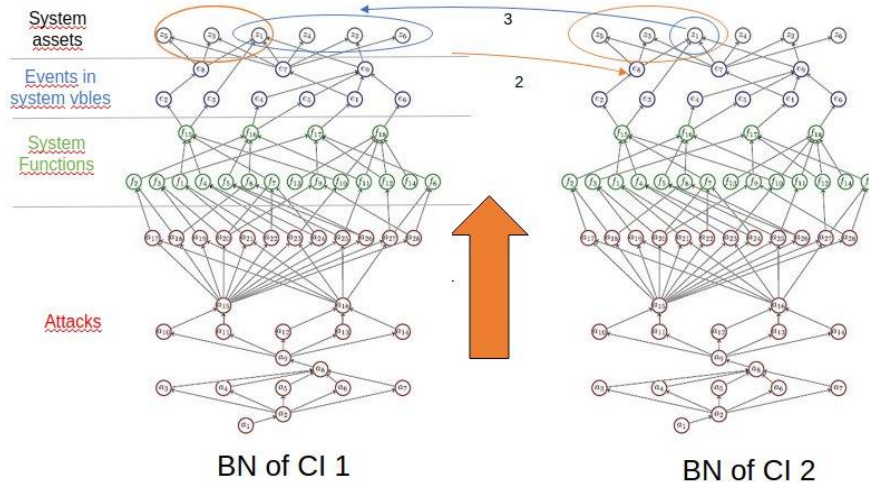


# Current status and technical roadmap



# RISKM4BC Research goals

**Research Objective 1: Create a system to control risks related to cascading effects among multiple interrelated CIs.**

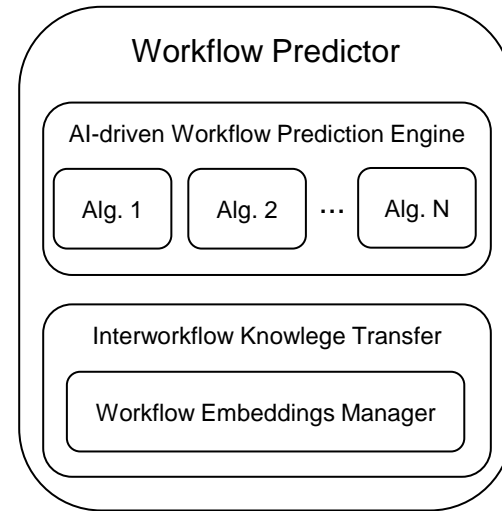
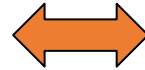
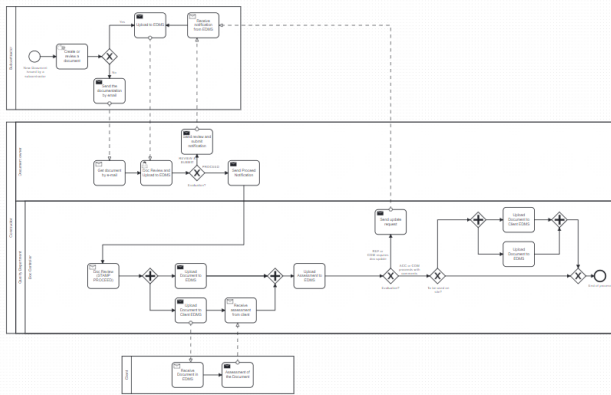


- Targeting CI interdependencies and Cascading Effects with other CIs.
- High degree of granularity on each CI, effects on different parts on connected CIs.
- CIs do not share their risk models (and live with it)

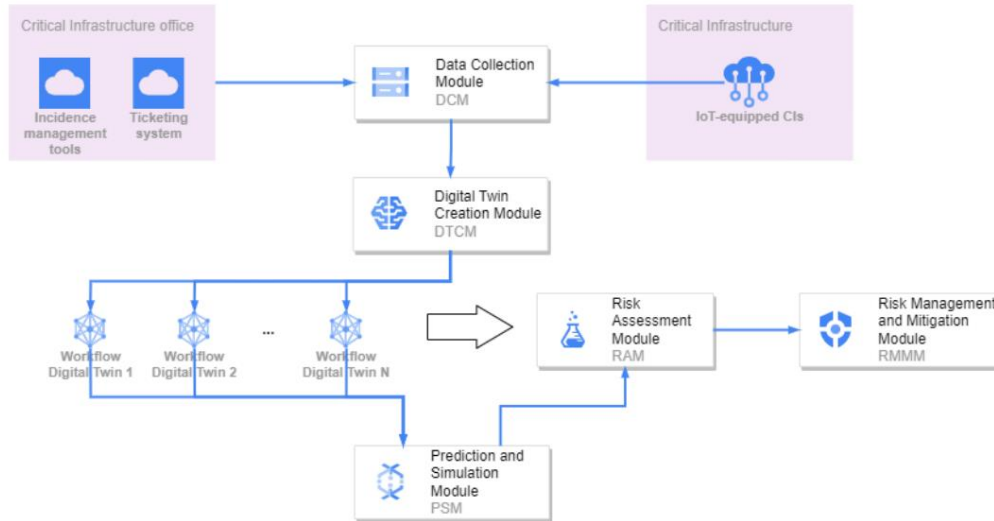
# RISKM4BC Research goals

## Research Objective 2: Create a live risk matrix leveraging AI-driven workflow digital twins to predict workflow evolution probability distributions

- Create and compare different AI-driven predictive algorithms to forecast current workflows evolution
- Create an ensemble approach with weighted algorithms
- Enable prediction capacity in non-observed workflows through knowledge transfer from different past observed workflows



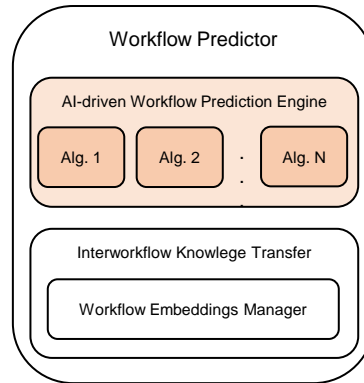
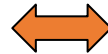
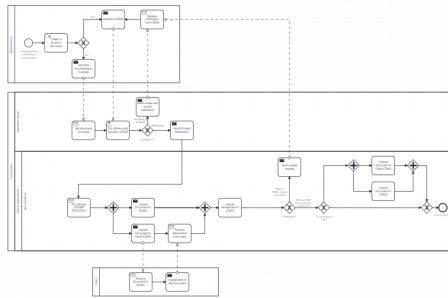
# Continuous Risk Management Concept



# WP3 Research goals

## Research Objective 2: Create a live risk matrix leveraging AI-driven workflow digital twins to predict workflow evolution probability distributions

- Create and compare different AI-driven predictive algorithms to forecast current workflows evolution
- Create an ensemble approach with weighted algorithms
- Enable prediction capacity in non-observed workflows through knowledge transfer from different past observed workflows



| name   | type                                       | last modified | created           | risk status / context |
|--|--|---------------|-------------------|-----------------------|
| Bridge 002 / Design - BIM/BIMB Use organization chart part 0   | Quality Plan (QP)                          | 01.1          | 5 January 2024    | 🟢                     |
| Bridge 002 / Design - Calculation rules for 1 half Standing Stone Group APC_2_Pn_200 mm max part 0   | Construction Design - Calculation Rules    | 01.0          | 28 August 2024    | 🟢                     |
| Bridge 002 / Design - Control Plan for Stone Steps Installation part 0   | Control Plan                               | 01.1          | 1 January 2021    | 🟢                     |
| Bridge 002 / Design - Calculation rules for 2 rows Standing Stone Group APC_3_Pn_100 mm max part 0   | Construction Design - Calculation Rules    | 01.0          | 28 August 2024    | 🟡                     |
| Bridge 002 / Design - Minimum shading Stone part 0   | Request For Information (RFI)              | 01.1          | 21 April 2024     | 🟡                     |
| Bridge 002 / Design - Request For Information (RFI)  | Request For Information (RFI)              | 01.0          | 27 June 2024      | 🟡                     |
| Bridge 002 / Design - Construction Drawing for 1 half Standing Stone Group A_3Pn_100 mm max (short 1/2) part 0   | Construction Design - Construction Drawing | 01.0          | 7 January 2025    | 🟢                     |
| Bridge 002 / Design - Principle Drawing of 0.5m half 1 half part 0   | Construction Design - Principle Drawing    | 01.0          | 28 September 2024 | 🟢                     |
| Bridge 002 / Design - SRF of manufacturing part 0  | Request For Information (RFI)              | 01.0          | 27 June 2024      | 🟡                     |
| Bridge 002 / Design - Control Plan for Interwall Stone manufacturing   | Control Plan                               | 02.0          | 28 January 2024   | 🟢                     |
| Bridge 002 / Design - 0.5m part 0  | Construction Design - Documentation        | 01.1          | 16 July 2024      | 🟢                     |
| Bridge 002 / Design - Principle Drawing for Abacus 0.7x1.1 0.0 0.014 - Chen wall 200 x 200 0.02 part 0   | Construction Design - Principle Drawing    | 01.0          | 7 November 2024   | 🟢                     |
| Bridge 002 / Design - Security requirements for Security terms evaluation part 0   | Request For Information (RFI)              | 01.1          | 30 May 2024       | 🟢                     |
| Bridge 002 / Design - SRF of 0.5m part 0   | Subcontractor Acceptance Form (SAF)        | 01.1          | 9 April 2024      | 🟢                     |
| Bridge 002 / Design - Calculation rules for 2 rows Standing Stone Group APC_3_Pn_100 mm max part 0   | Construction Design - Calculation Rules    | 01.0          | 28 August 2024    | 🟢                     |
| Bridge 002 / Design - Request For Information (RFI)  | Request For Information (RFI)              | 01.1          | 21 April 2024     | 🟡                     |
| Bridge 002 / Design - Electrical loads specification   | Construction Design - Specific Studies     | 01.0          | 5 September 2024  | 🟢                     |
| Bridge 002 / Design - SRF of 0.5m part 0   | Subcontractor Acceptance Form (SAF)        | 02.1          | 9 April 2024      | 🟢                     |
| Bridge 002 / Design - 0.5m Stone with transoms part 0  | Request For Information (RFI)              | 01.0          | 30 May 2024       | 🟡                     |
| Bridge 002 / Design - Materials requirement for standing stone installation part 0   | Supplier Creation Request (SCR)            | 01.1          | 6 June 2024       | 🟢                     |
| Bridge 002 / Design - Quality Compliance Request for Manufacturing part 0  | Quality Compliance Matrix (QCM)            | 01.1          | 3 January 2024    | 🟢                     |
| Bridge 002 / Construction Drawing for 1 half Standing Stone Group A_3Pn_100 mm max (short 1/2)   | Construction Design - Construction Drawing | 01.0          | 7 January 2025    | 🟢                     |
| Bridge 002 / Design - Principle Drawing of stone walls (standing stones) x100 and thickness of masonry (standing stones) for and settlement stone part 0 | Construction Design - Principle Drawing    | 01.0          | 6 November 2024   | 🟢                     |

# WP3 Research goals

## Research Objective 2: Create a live risk matrix leveraging AI-driven workflow digital twins to predict workflow evolution probability distributions

- Create and compare different AI-driven predictive algorithms to forecast current workflows evolution
- Create an ensemble approach with weighted algorithms
- Enable prediction capacity in non-observed workflows through knowledge transfer from different past observed workflows

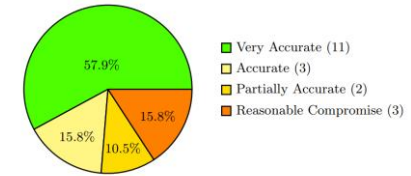
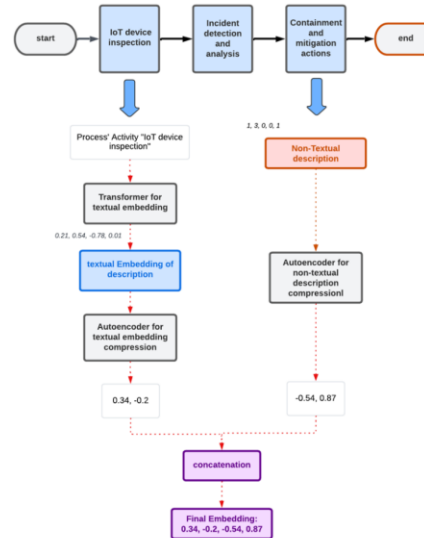
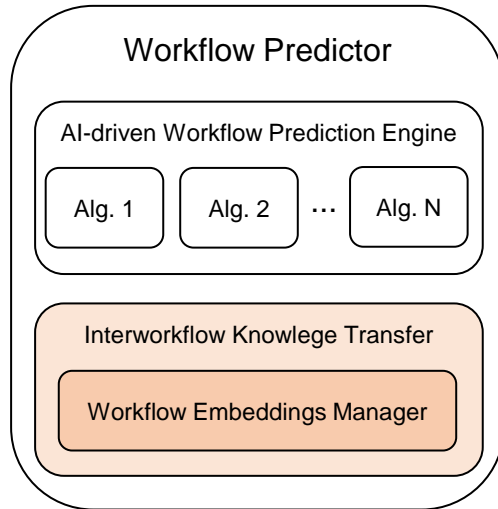
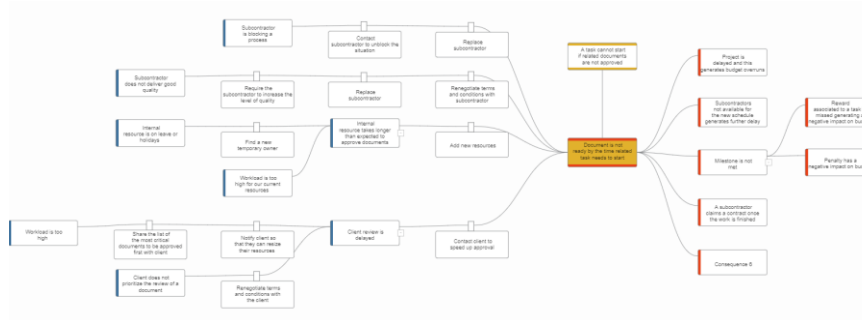


Fig. 9. Summary of Process Embedding Evaluations

# WP3 Research goals

## Research Objective 3: Create a bowtie smart center able to automate risk identification, predict threats and risk evolution, and chained risk effects

- Create mechanisms to automatically create bowties out of existing workflows, initial textual descriptions or partially defined bowties
- Create a continuous self-learning model to predict bowtie activations
- Enable prediction capacity in non-observed bowties through knowledge transfer from different past observed bowties
- Automated link of business objectives with lower-level bowtie components through LLMs

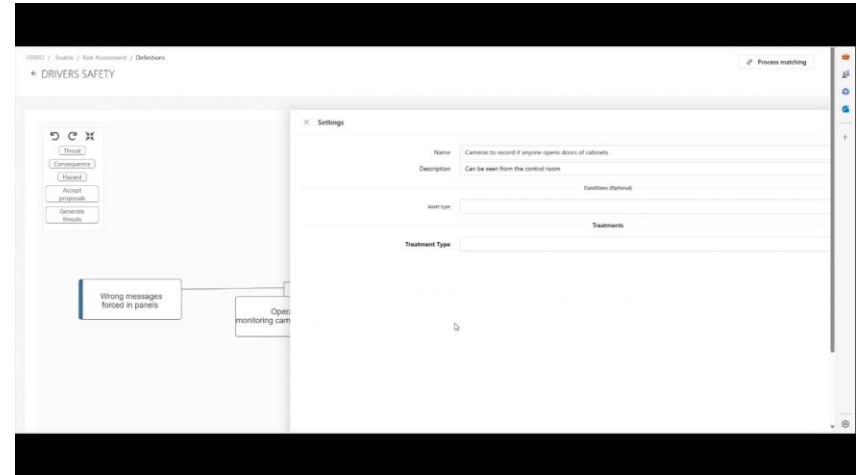




# WP3 Research goals

## Research Objective 3: Create a bowtie smart center able to automate risk identification, predict threats and risk evolution, and chained risk effects

- Create mechanisms to automatically create bowties out of existing workflows, initial textual descriptions or partially defined bowties
- Create a continuous self-learning model to predict bowtie activations
- Enable prediction capacity in non-observed bowties through knowledge transfer from different past observed bowties
- Automated link of business objectives with lower-level bowtie components through LLMs

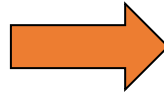
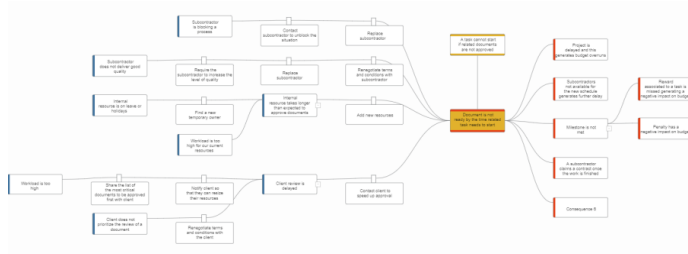




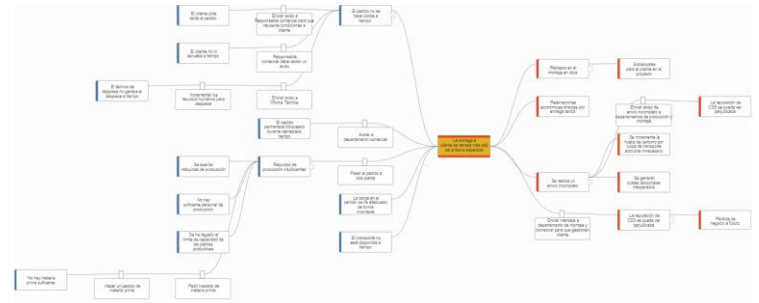
# WP3 Research goals

## Research Objective 3: Create a bowtie smart center able to automate risk identification, predict threats and risk evolution, and chained risk effects

- Create mechanisms to automatically create bowties out of existing workflows, initial textual descriptions or partially defined bowties
- Create a continuous self-learning model to predict bowtie activations
- Enable prediction capacity in non-observed bowties through knowledge transfer from different past observed bowties
- Automated link of business objectives with lower-level bowtie components through LLMs



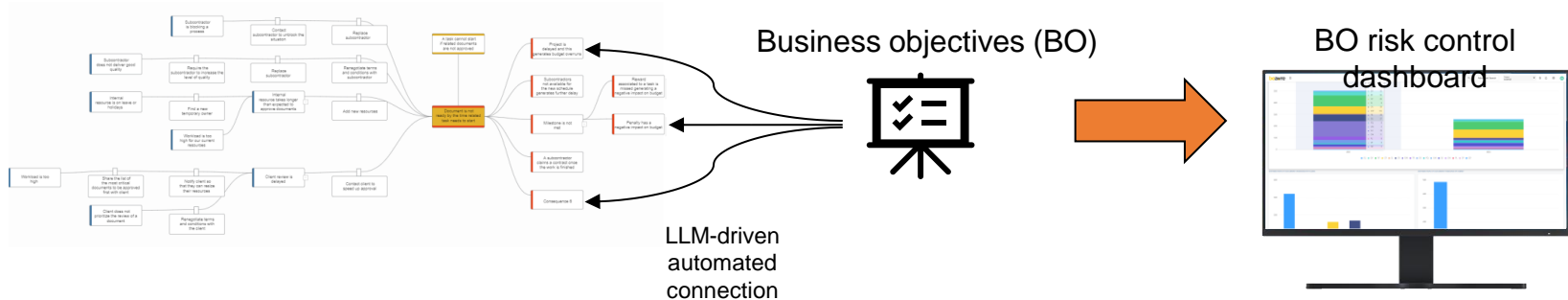
Bowtie embeddings for knowledge transfer



# WP3 Research goals

## Research Objective 3: Create a bowtie smart center able to automate risk identification, predict threats and risk evolution, and chained risk effects

- Create mechanisms to automatically create bowties out of existing workflows, initial textual descriptions or partially defined bowties
- Create a continuous self-learning model to predict bowtie activations
- Enable prediction capacity in non-observed bowties through knowledge transfer from different past observed bowties
- Automated link of business objectives with lower-level bowtie components through LLMs





**Q&A**

**ANSWERS TO YOUR QUESTIONS**



AI4CYBER



# AI Supporting Cyber Risks And Resilience Of Critical Infrastructures.

**Insights From  
CS-AWARE-NEXT,  
DYNABIC,  
& AI4CYBER**

**Online Webinar**

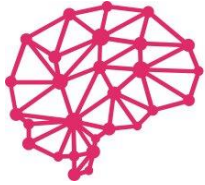
**30 September 2024**

**16:00 – 17:30**



Funded by  
the European Union





# AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR  
CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

## Trustworthy AI for cybersecurity solutions

Webinar “AI supporting Cyber Risks and Resilience of Critical Infrastructures”

30/09/2024

Erkuden Rios, AI4CYBER Project Manager  
[erkuden.rios@tecnalia.com](mailto:erkuden.rios@tecnalia.com)

**tecnalia**

MEMBER OF BASQUE RESEARCH  
& TECHNOLOGY ALLIANCE



Funded by the  
European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.

*Disclaimer: 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 European Commission. Neither the European Union nor the European Commission can be held responsible for them.*



# AI4CYBER

Trustworthy Artificial Intelligence for Cybersecurity  
Reinforcement and System Resilience

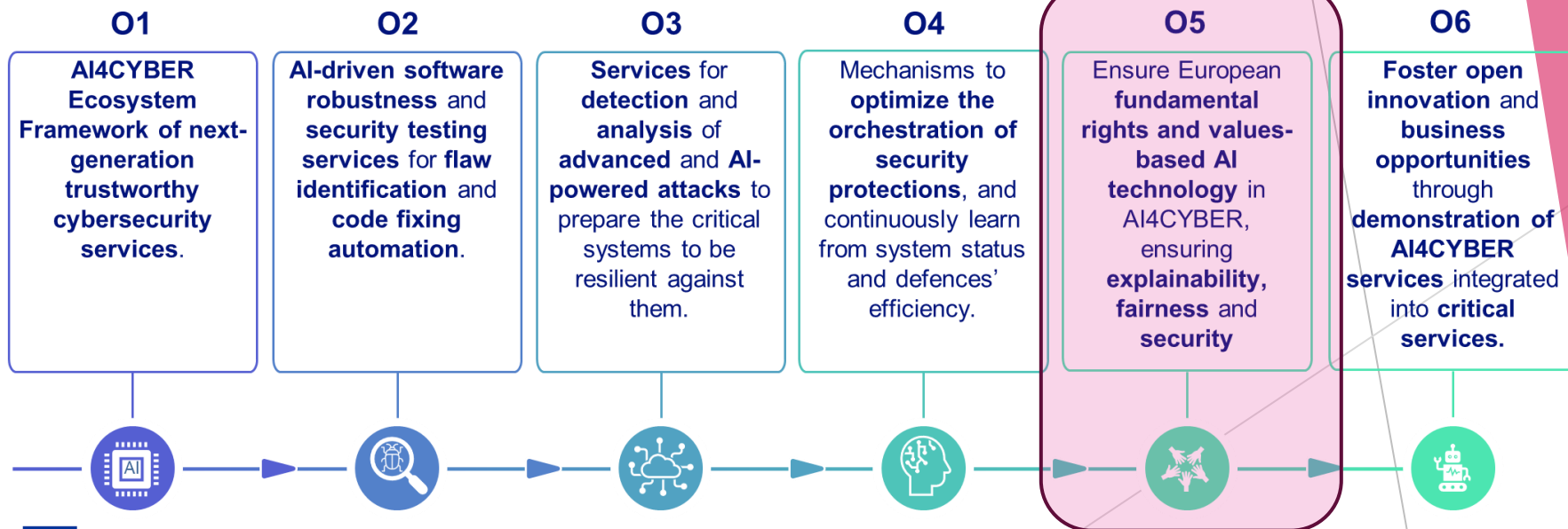
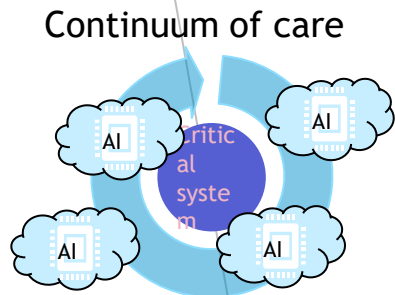
- ▶ Grant Agreement ID: 101070450
- ▶ Project Type: RIA
- ▶ Project Coordinator: Tecnalía
- ▶ Consortium: 13 partners
- ▶ Budget: € 3.998.413,00 €
- ▶ Start Date: 01/09/2022
- ▶ Duration: 3 years





# Key objectives

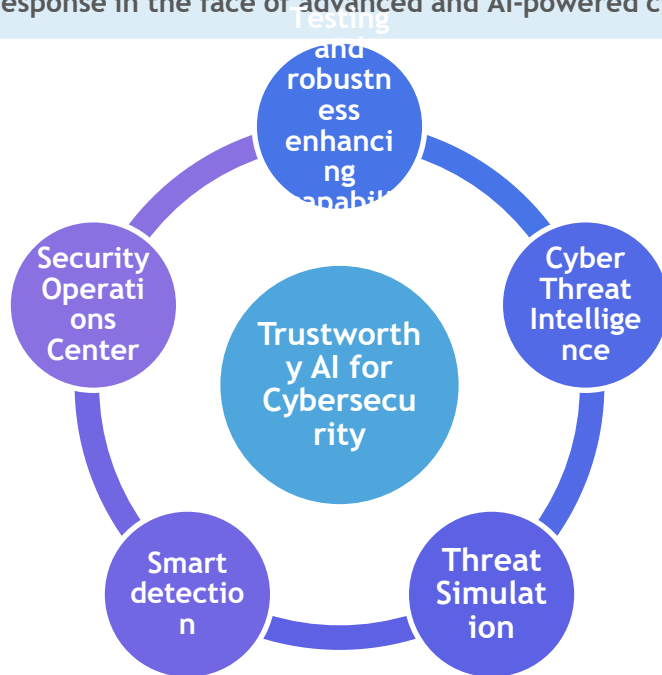
To establish an **Ecosystem Framework of next generation AI-based services** for supporting critical system developers and operators to **efficiently manage** system **robustness, resilience**, and appropriate **response** in the face of **advanced and AI-powered cyberattacks**.



# AI4CYBER in a nutshell

Establishing an Ecosystem Framework of next generation AI-based services for critical system robustness, resilience, and appropriate response in the face of advanced and AI-powered cyberattacks.

**11 Key Results**  
that cover  
**6 cybersecurity**  
areas



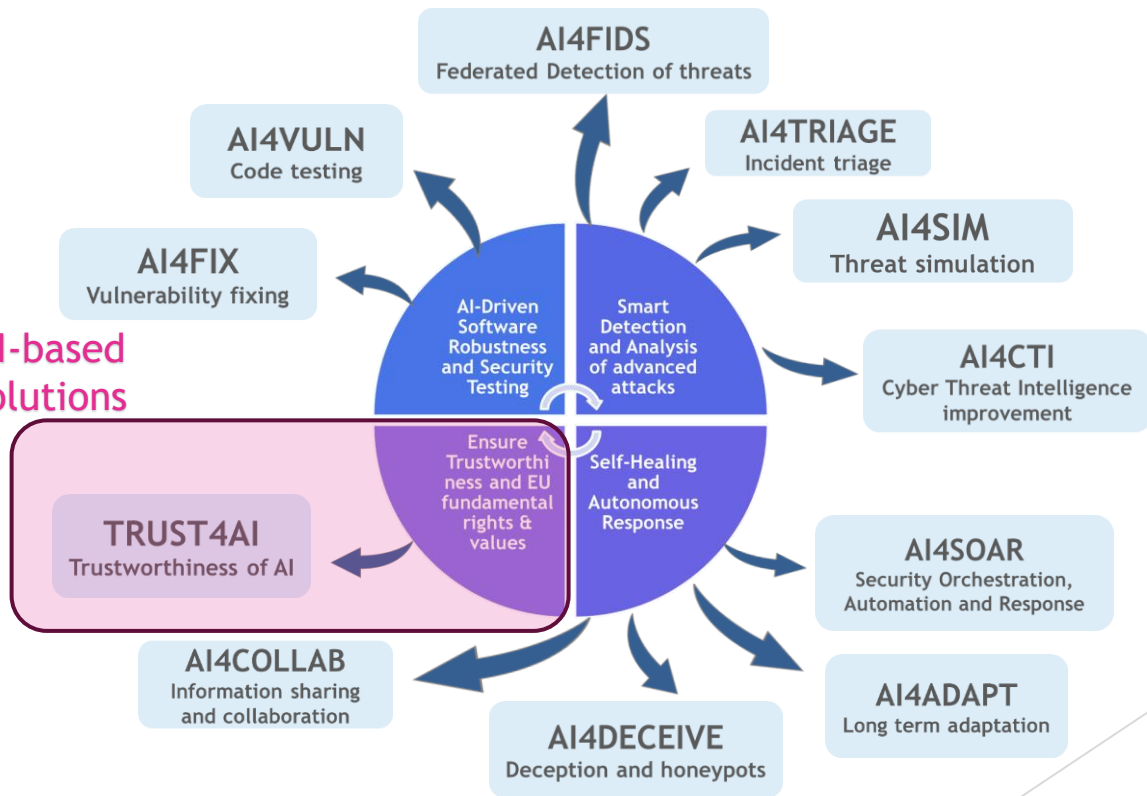
**3 Demonstrators**  
that foster  
**innovation**

Energy

Banking

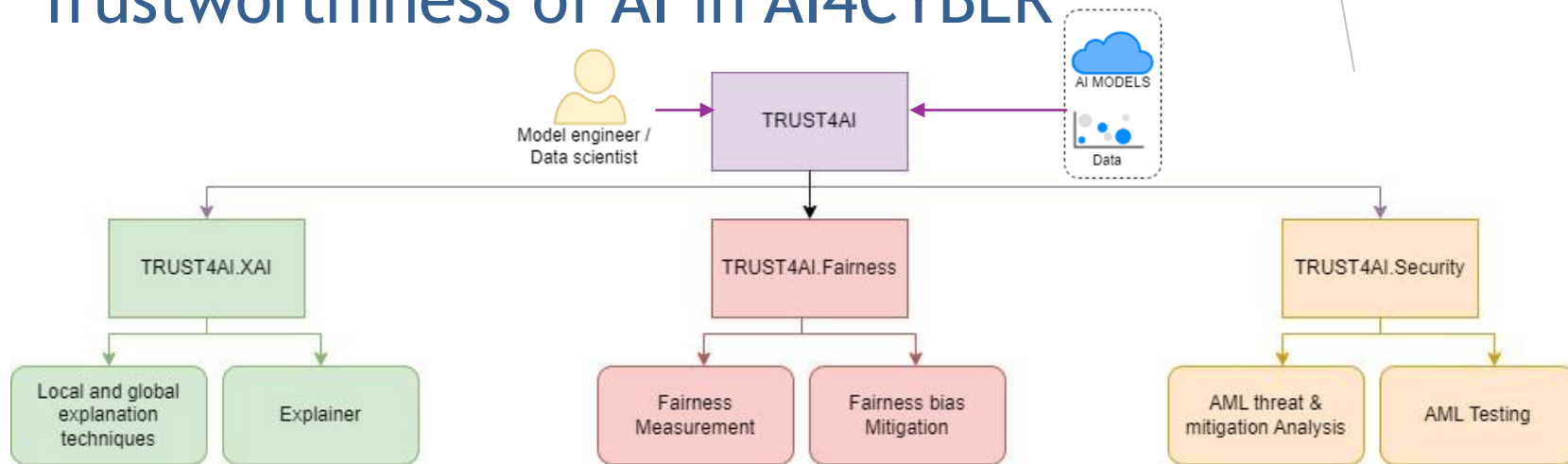
Health

# AI4CYBER Framework



TRUSTWORTHY AI-based cybersecurity solutions

# Trustworthiness of AI in AI4CYBER



**Explainability - XAI**  
 (i.e. Interpretability) of ML/AI models, to allow better understanding of the model to the data scientist who develops the ML model or to a potential end-user.

**Fairness** of the ML/AI models, to allow to correct potential bias against some sensitive attributes or against sub-populations.

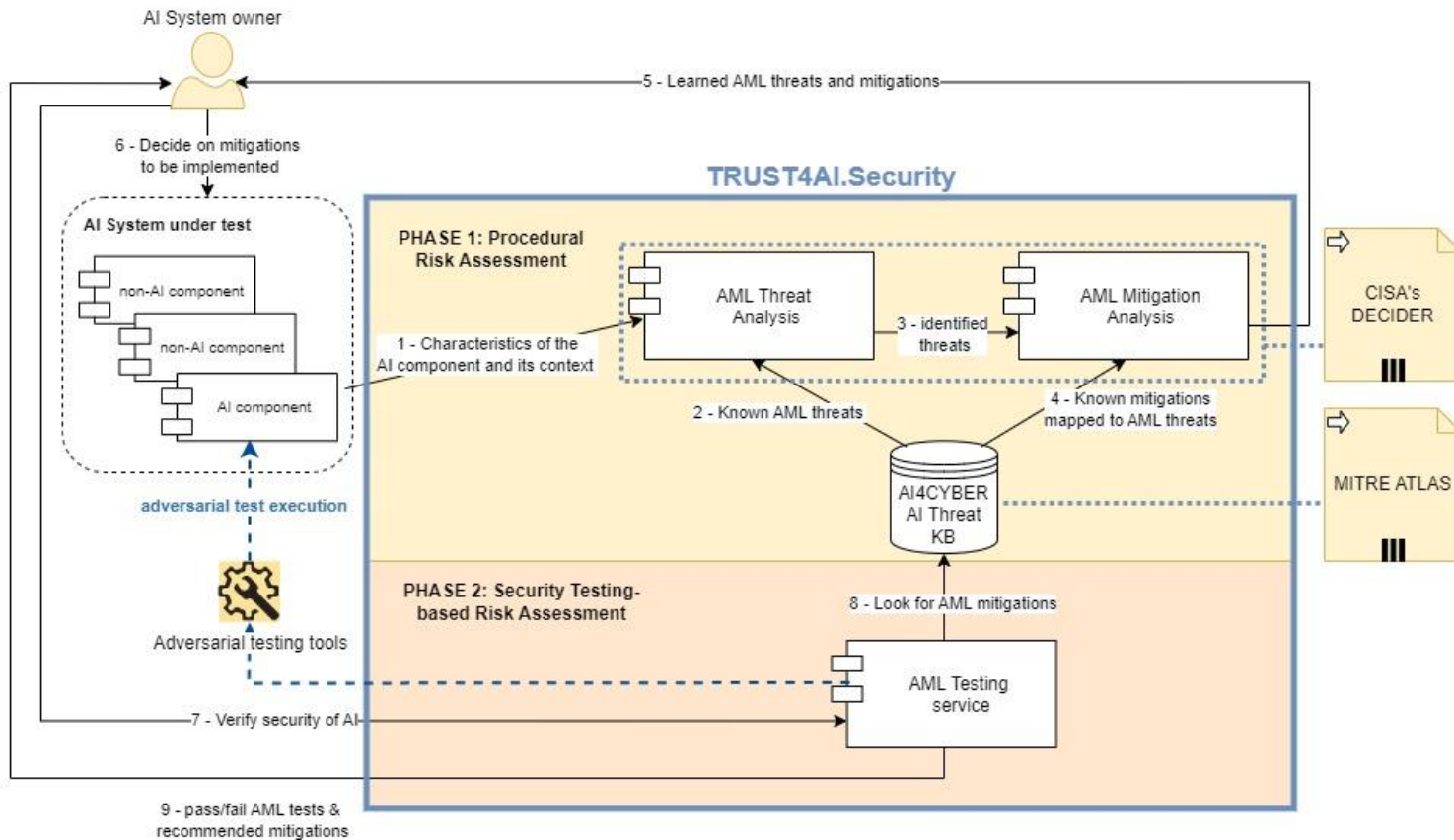
**Security** of the ML/AI models, to allow to learn potential Adversarial Machine Learning attacks and to protect against them.



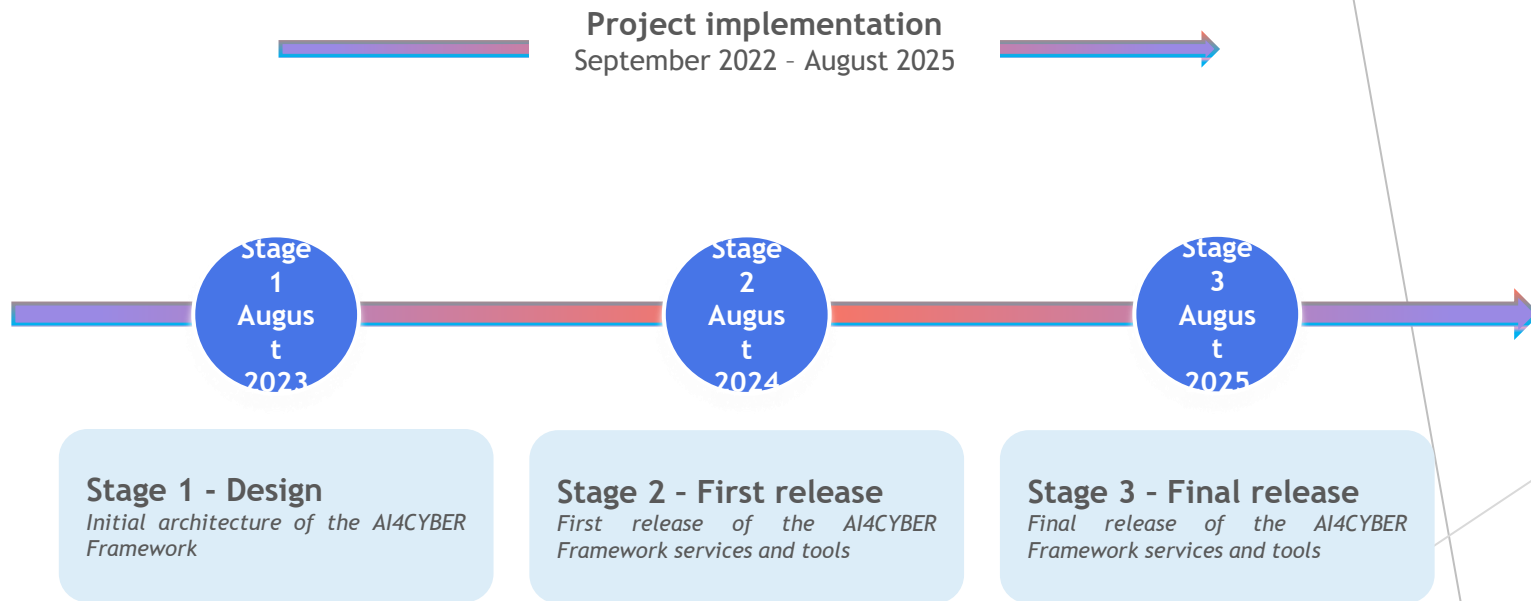
# TRUST4AI.Security Objectives

- ▶ Security of AI as part of Robustness of AI.
- ▶ Protect models from Adversarial Machine Learning (AML) attacks, including: *data protection*, poisoning, evasion, and oracle (privacy) attacks.
- ▶ Offer mechanisms for **countering** attacks to the AI-based cybersecurity tools, e.g., intrusion and anomaly detection tools based on AI models.
- ▶ Builds on top of the *AI Threat and Countermeasure Knowledge Base* from H2020 SPARTA project and MITRE ATLAS.
- ▶ Leverages CISA's Decider tool.

# AI system risk assessment with TRUST4AI.Security



# AI4CYBER Timeline



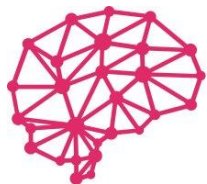


# TRUST4AI publications

- Kurek, W., Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2023, July). **Explainable Artificial Intelligence 101: Techniques, Applications and Challenges**. In International Conference on Intelligent Computing (pp. 310-318). Singapore: Springer Nature Singapore (SPRINGER LNCS).
- Pawlicki, M.: **Towards Quality Measures for xAI algorithms: Explanation Stability**, DSAA2023 (CORE A)
- Pawlicki, M., Pawlicka, A., Śrutek, M., Kozik, R., Choraś, M. **Interpreting Intrusions - The Role of Explainability in AI-based Intrusion Detection Systems** (IP&C 2023)
- Thouvenot V., Huynh C.B. **TSCFKit and CFKit, two Python modules dedicated to counterfactual generation**, JDS 2023.
- Dr. Marek Pawlicki panelist in CLAIRE AQuA: Cybersecurity of AI and AI for Cybersecurity. (<https://www.youtube.com/watch?v=u44CiZhkbnY>)
- Prof. Michał Choraś keynote on "Trustworthy and Explainable AI (xAI) in Emerging Network Security Applications" in ARES2023 (<https://www.ares-conference.eu/workshops-eu-symposium/ens-2023/>)
- Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., & Choraś, M. (2024, April). **A Novel Approach to the Use of Explainability to Mine Network Intrusion Detection Rules**. In Asian Conference on Intelligent Information and Database Systems (pp. 70-81). Singapore: Springer Nature Singapore.
- Pawlicki, M., Puchalski, D., Szelest, S., Pawlicka, A., Kozik, R., & Choraś, M. (2024, July). **Introducing a Multi-Perspective xAI Tool for Better Model Explainability**. In Proc. of the 19th International Conference on Availability, Reliability and Security (pp. 1-8).
- Kozik, R., Kątek, G., Gackowska, M., Kula, S., Komorniczak, J., Ksieniewicz, P., ... & Choraś, M. (2024). **Towards explainable fake news detection and automated content credibility assessment: Polish internet and digital media use-case**. *Neurocomputing*, 608, 128450.

# TRUST4AI publications

- Pawlicki, M. (2024). **ARIA, HaRIA and GeRIA: Novel Metrics for Pre-Model Interpretability**. IEEE Access.
- Nguyen, M. D., Bouaziz, A., Valdes, V., Rosa Cavalli, A., Mallouli, W., & Montes De Oca, E. (2023, August). **A deep learning anomaly detection framework with explainability and robustness**. In Proc. of the 18th International Conference on Availability, Reliability and Security (pp. 1-7).
- Asimopoulos, D. C., Radoglou-Grammatikis, P., Makris, I., Mladenov, V., Psannis, K. E., Goudos, S., & Sarigiannidis, P. (2023, August). **Breaching the defense: Investigating fgsm and ctgan adversarial attacks on IEC 60870-5-104 AI-enabled intrusion detection systems**. In Proc. of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).
- Villarini, B., Radoglou-Grammatikis, P., Lagkas, T., Sarigiannidis, P., & Argyriou, V. (2023, July). **Detection of Physical Adversarial Attacks on Traffic Signs for Autonomous Vehicles**. In 2023 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT) (pp. 31-37).
- Bouaziz, A., Nguyen, M. D., Valdés, V., Cavalli, A. R., & Mallouli, W. (2023, July). **Study on Adversarial Attacks Techniques, Learning Methods and Countermeasures: Application to Anomaly Detection**. In ICISOFT (pp. 510-517).
- Iturbe, E., Rios, E., & Toledo, N. (2023, December). **Towards trustworthy Artificial Intelligence: Security risk assessment methodology for Artificial Intelligence systems**. In 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 291-297).
- Blog post “Trustworthy AI” - General overview of TRUST4AI <https://ai4cyber.eu/?p=1136>



# AI4CYBER

TRUSTWORTHY ARTIFICIAL INTELLIGENCE FOR  
CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE



<https://ai4cyber.eu/>



<https://x.com/Ai4Cyber>



<https://www.linkedin.com/company/ai4cyber/>



Erkuden Rios



AI4CYBER Project Coordinator



[erkuden.rios@tecnalia.com](mailto:erkuden.rios@tecnalia.com)

## Thank you for your attention!





AI4CYBER



# AI Supporting Cyber Risk Management And Resilience Of Critical Infrastructures;

## Insights From CS-AWARE-NEXT, DYNABIC, & AI4CYBER

Online Webinar

30 September 2024

16:00 – 17:30

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450.



Funded by  
the European Union

