TLP : GREEN

INTERNATIONAL UNION
OF RAILWAYS

CYBER SECURITY SOLUTION PLATFORM

CYBER SECURITY
Working Group

Houbion Catherine

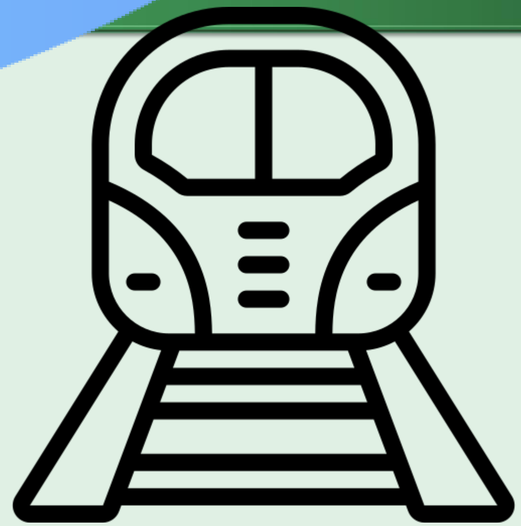
Cyber Security in railways – Different Situations

- We check and assess our equipments and systems for vulnerabilities
- We list our compliancy gaps
- We go back to our suppliers for solutions

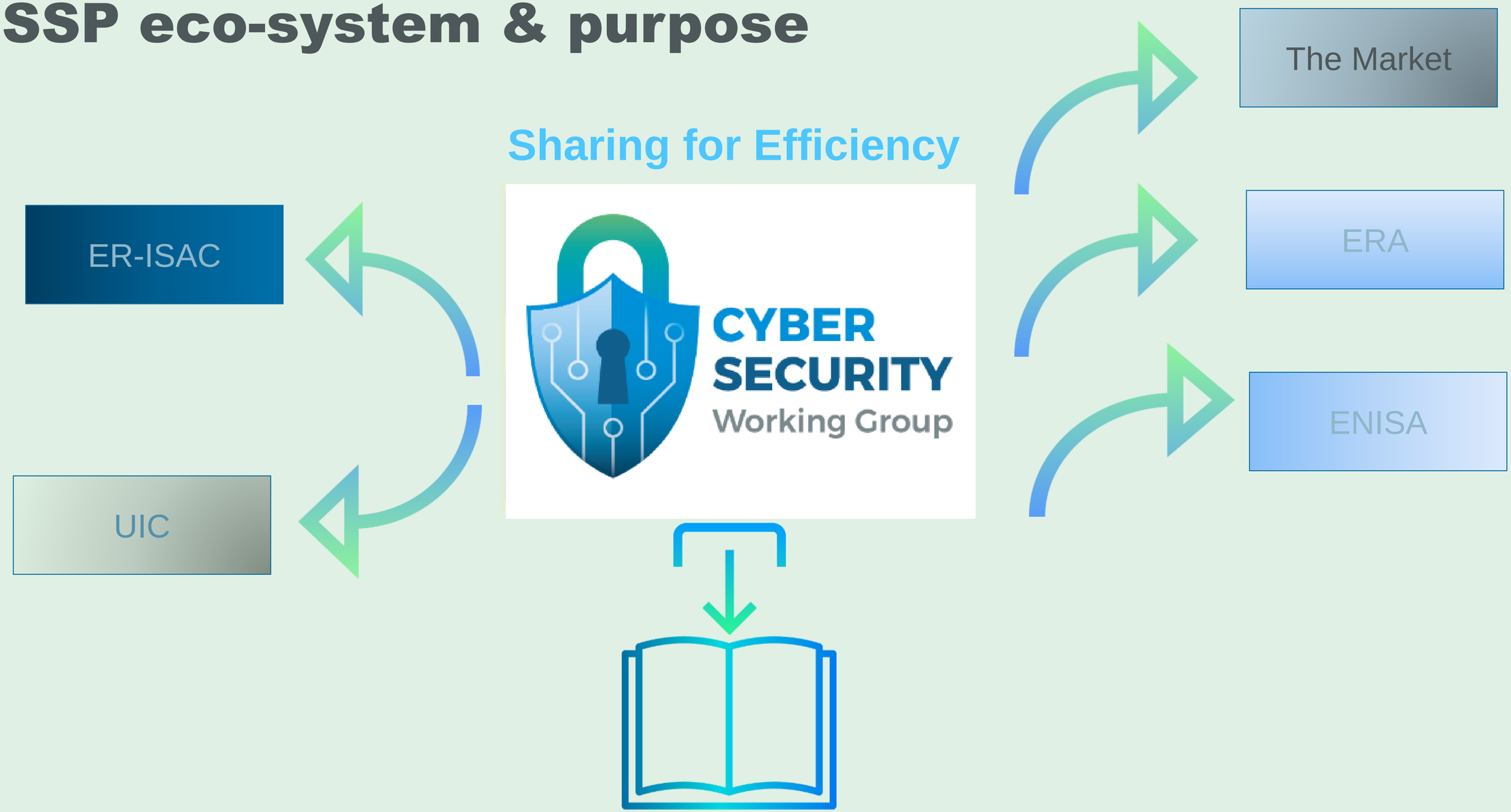
- Our suppliers proact[illegible]ome with new state-of-the–art p[illegible] that solve our problems (tha[illegible]ave brought into our systems)

- The market p[illegible] solutions & new trends
- We check the market t[illegible]d
- We make POC, pilots & dep[illegible]..





CSSP eco-system & purpose

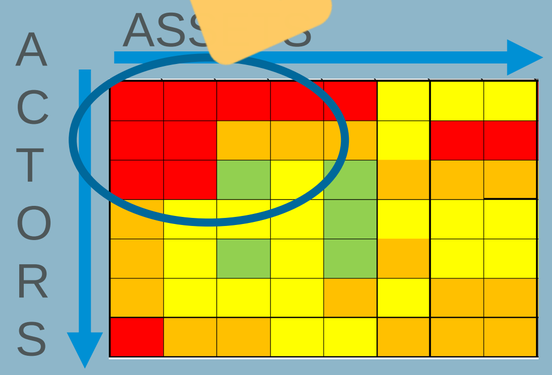


CSSP Solution catalog : Inputs & Activities

Our Inputs & Main Activities

Our Focus

CSSP Threat Landscape Heatmap



Expert Talks on technical approaches

- Product implementation
- Risk analyse process
- Risk Assurance Process

CYBER SECURITY Working Group

Best Practices

- SBOM
- SOC implementation
- Maturity assessment

Supplier Slots

- Solutions presentations
- Products discussions
- Technical use cases

CSSP Solution catalog : Main Chapters

Our main Chapters

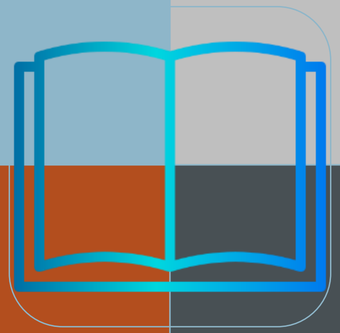
CSSP Threat landscape Report

- Our inputs
- Our conclusions
- Our recommendations

- Our process (Build, Validate, Maintain & Communicate)

Workshops' inputs

- Experts Presentations
- Project Presentations
- Assessment Results



Guidelines

- Members' Best Practices
- Members' Example of Architecture
- New Railway standard

Solutions

- Solutions & Products used
- Solutions & Products being assessed
- Future Solutions

How to navigate through the catalog

- Use Cases
- Vulnerabilities
- Heatmap



https://cssp.uic.org

- Solutions
- Best Practices
- Recommendations

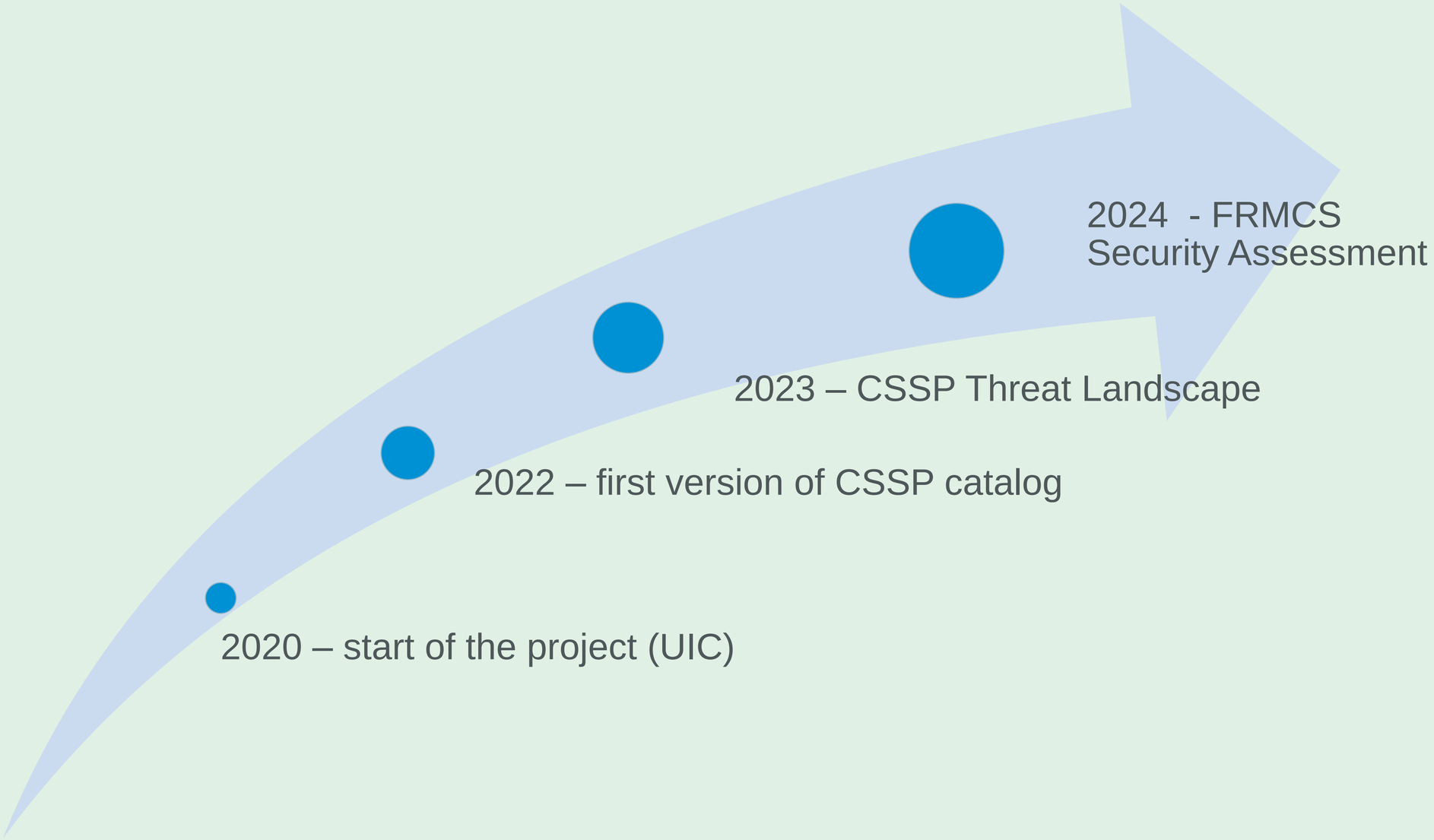
Cyber Security Solutions Platform Next Activities

CYBER SECURITY Working Group

1. Deliver Threat Landscape Report for 2024
2. Complete the catalogue for the products gathered
3. Complete Cloud Paper
4. Assess Artificial Intelligence Impact
5. Zero Trust Architecture
6. Build a platform of expertise & develop our processes

A pragmatic approach related to solutions

CSSP Roadmap



ER-ISAC in its context

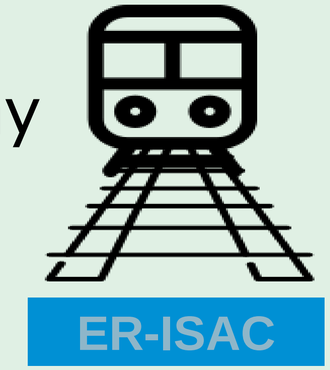
ER-ISAC was created (from scratch) in **2018**

- Triggered by the project **Empowering ISACS** from **ENISA**
- Promote the creation of
  Information **S**haring and **A**nalyze **C**enters
  across **Essential** Services **Industry Sectors in Europe**

ER-ISAC is hosted by UIC

but it remains **independent** on the content it produces

ER-ISAC gathers Railways **I**nfrastructure **M**anagers & **R**ailway **U**ndertakers



Organisation in 2024



Every 3 weeks

EU Concil of ISACs

ENISA

4 Co-Chairs

Facilitation Team

Members

General Assembly
+ Stakeholders



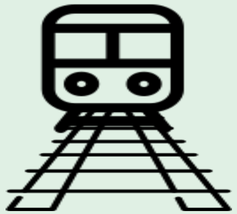
1 x month



Every 3/4 weeks



1 x year



ER-ISAC

OPERATION
&
Governance

CISO FORUM
Since 2022

RW CyberSec
Strategy



2 x year

The European Railway Cybersecurity (future) eco-system

CISO Forum

ER-ISAC

- Threat intelligence
- Vulnerabilities
- Incident information

Analyse & Share

- The risks for Railways
- Rail operations response
- Best Practise
- Return of experience



CISO Forum

UIC CSSP

- Cybersecurity Products & Solutions

Share & Assess

- Maintenance of solutions catalog
- Threat analysis & landscaping
- Assessments of architecture, products, security and project deliverables
- technical share between group members

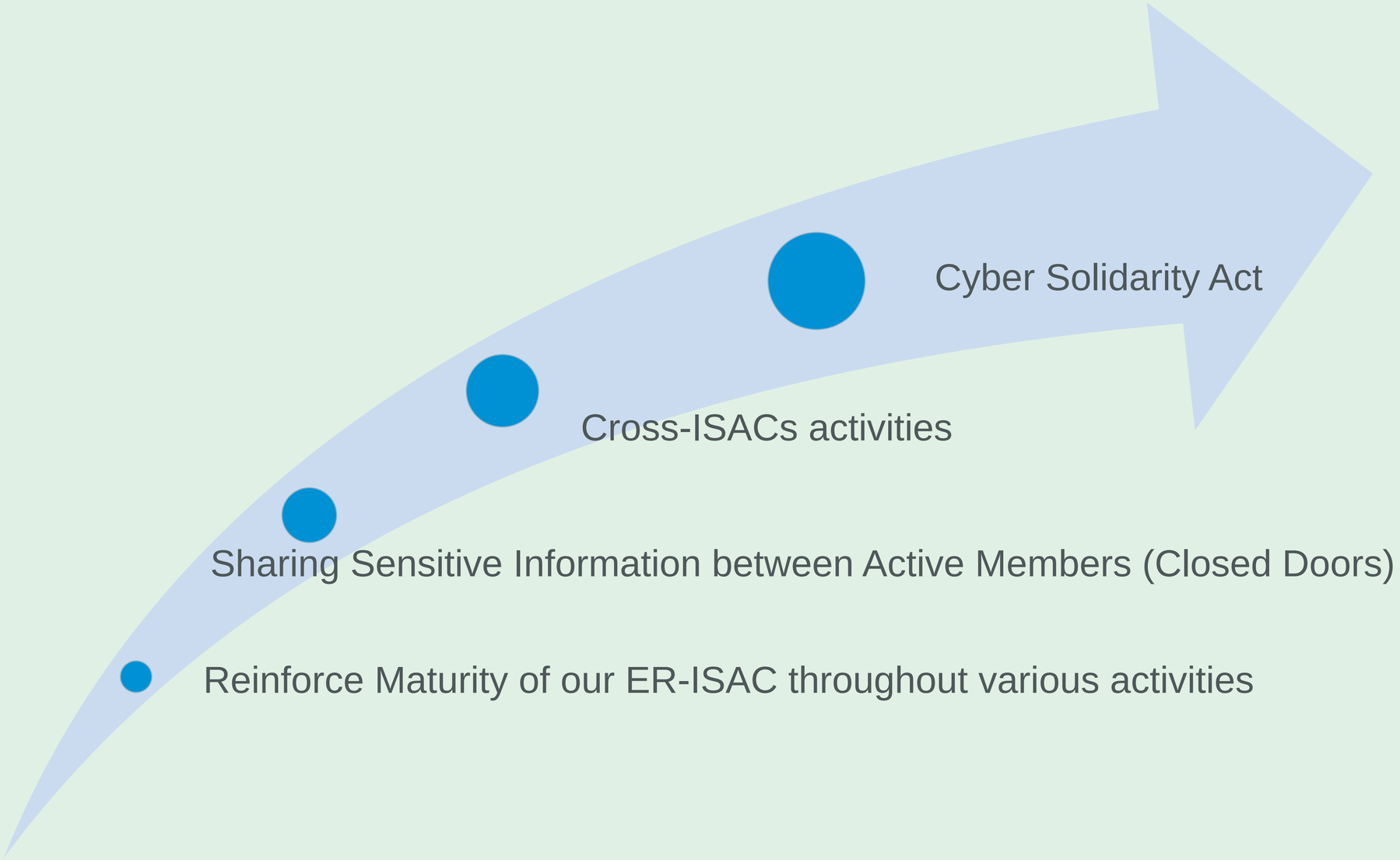
Railway Cybersecurity working groups & Communities of practices

- Cybersecurity initiatives led by Railway representatives or in benefit of Railway

Share

- Standards & regulations
- Cybersecurity initiatives
- R&D initiatives
- Best practices

ER-ISAC Roadmap in 2024



INTERNATIONAL UNION
OF RAILWAYS

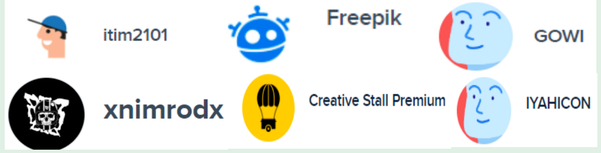
Stay in touch with UIC:

www.uic.org

#UICrail

Houbion@UIC.org
Mandoc@UIC.org

Icons Used



Thank you for your attention.