Jems
User Group meeting #8

Interact | 20.10.2026

Interact

Co-funded by
the European Union
Interreg

Agenda first day



01	02	03	Lunch break	04	17:00
State of play	Cyber act	Programme own developments		Looking into Jems 28	

Agenda second day

01 Good morning!

02 The future of Monitoring systems

12:30 **Lunch break***

*Lunch **only** for participants in IT Monitoring systems network event

Lyon

History

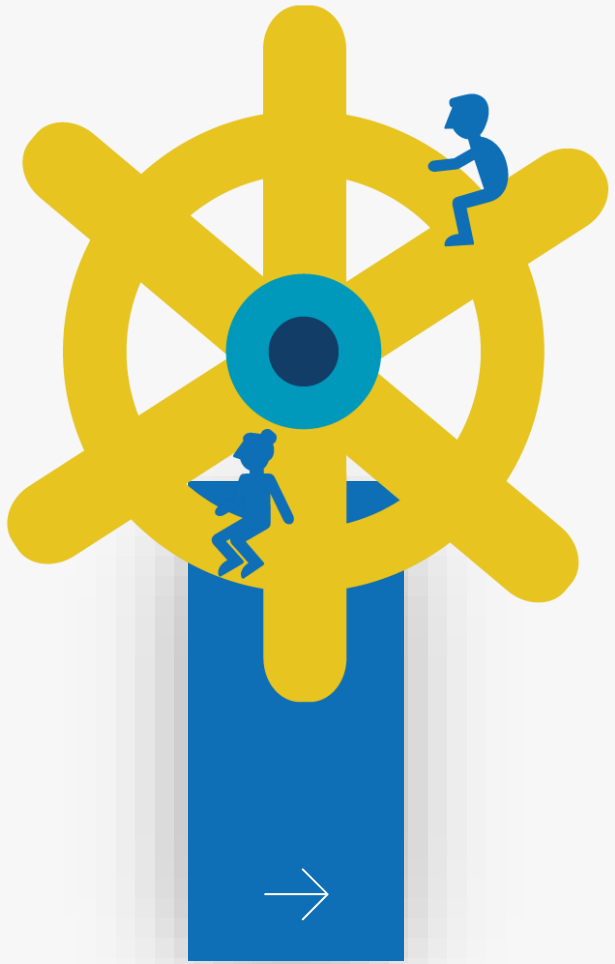
Cuisine & Bouchons

Jems.interact.eu/Lyon

Evening meetup at 8pm

Boston tavern in place des Terreaux

Activities outside agenda are not covered by Interact



State of play

Maintenance

The team



Jose Almeida

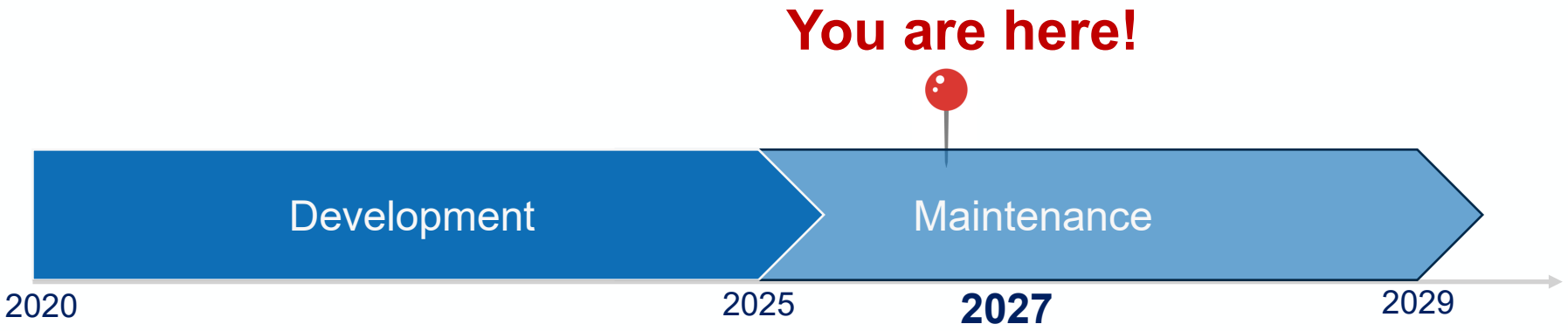


Alexandra Kulmer



Pieter Louwers

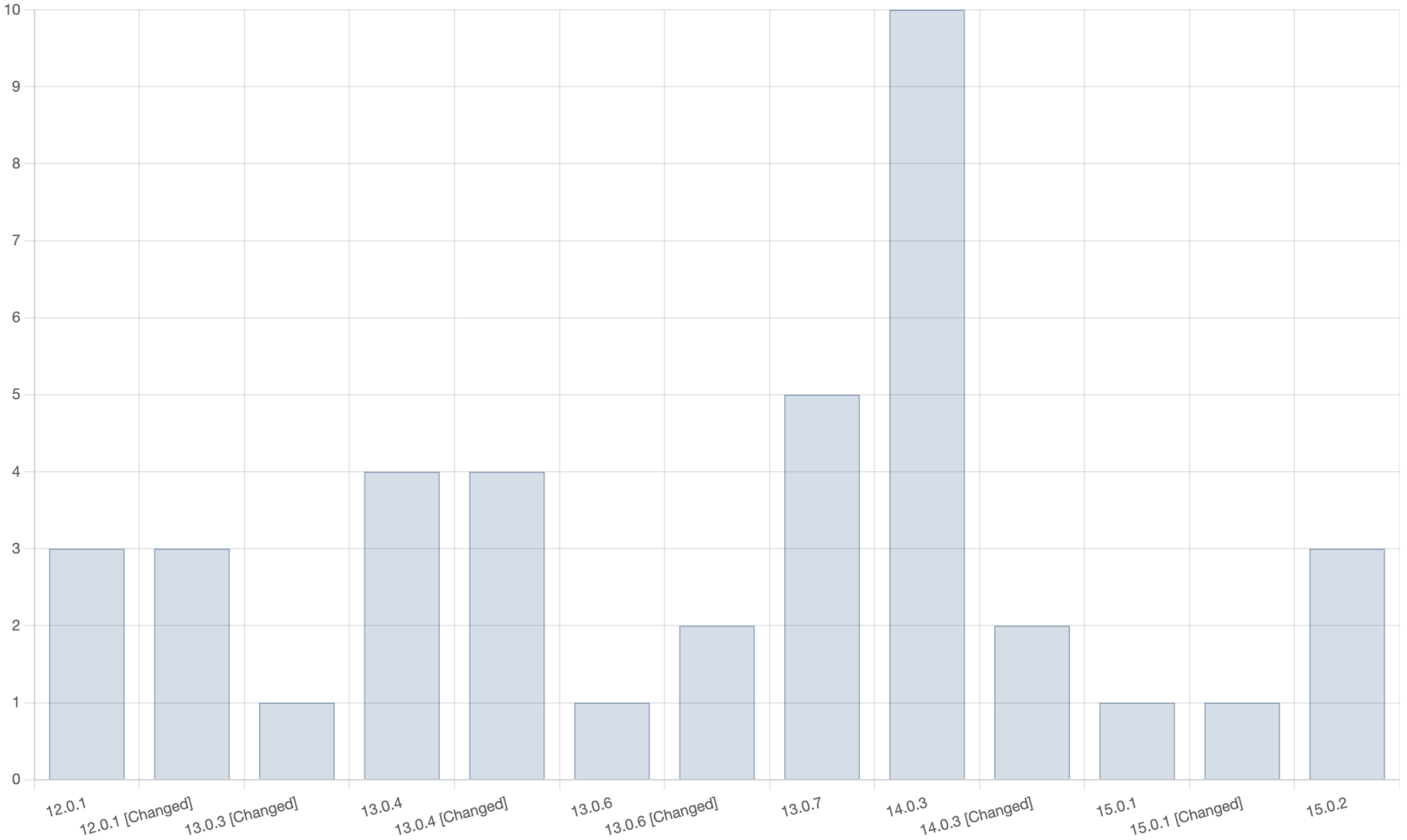
Where are we ?



Where are we ?

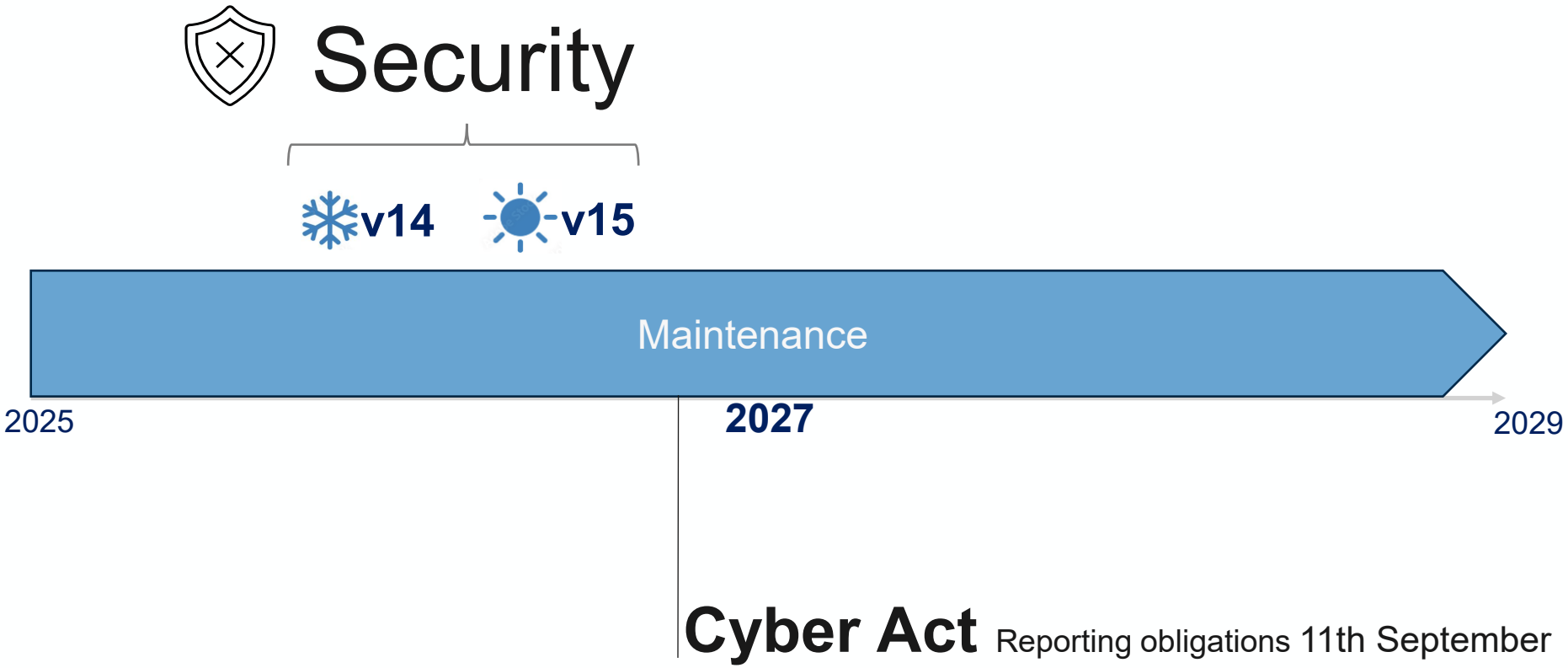


* Minor releases are hidden

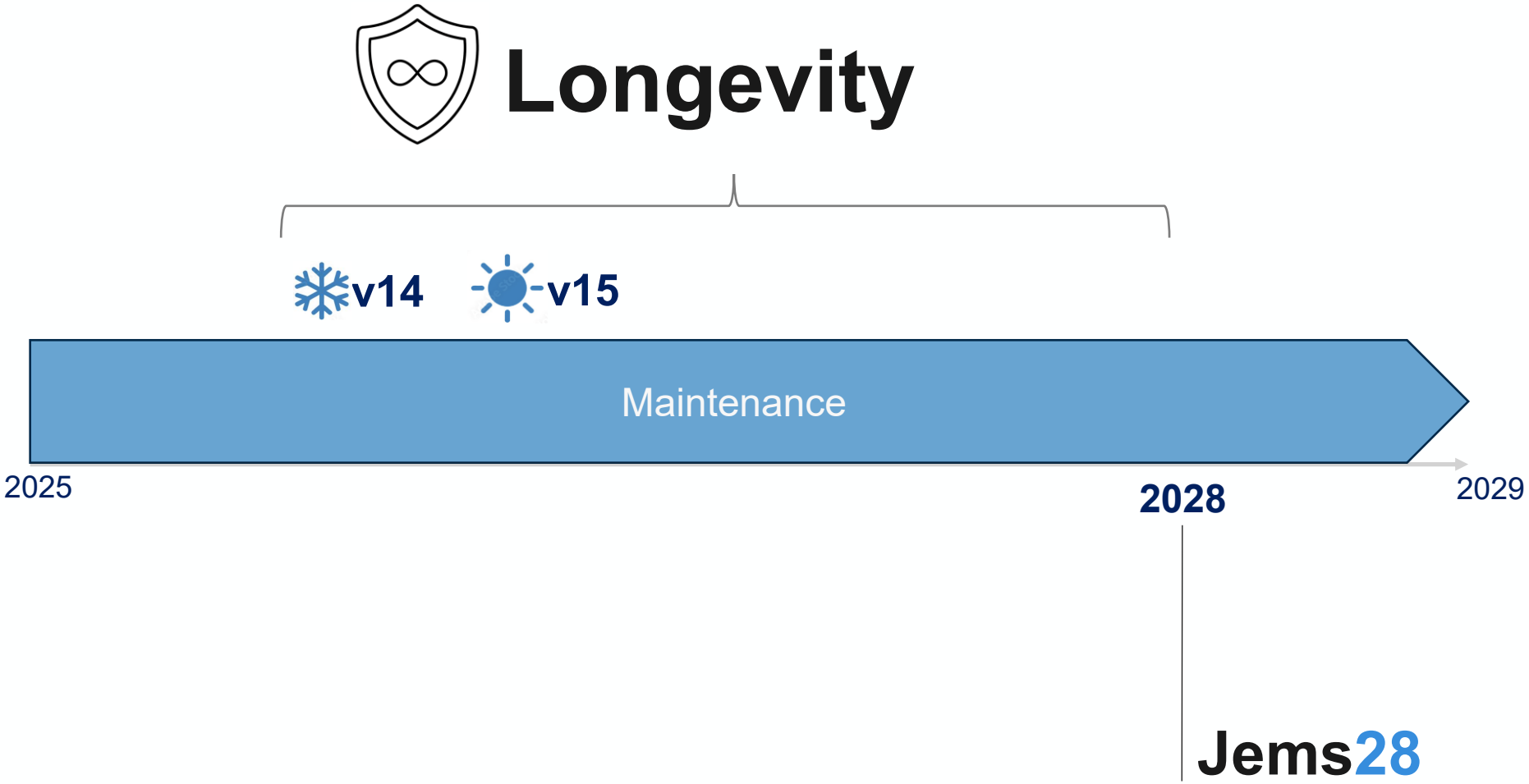


Jems.interact.eu/stats

Main focus…


Security
v14
v15
Maintenance
2025
2027
2029
Cyber Act
Reporting obligations 11th September

Looking forward...



Next...

V16

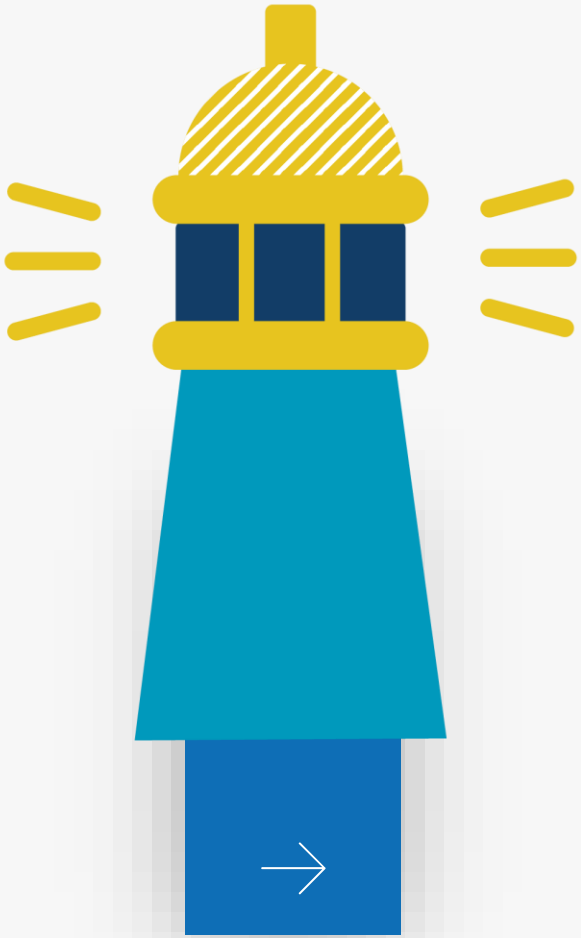
1) Critical Bugs

2) SpringBoot 4

3) Multifactor authentication (MFA)

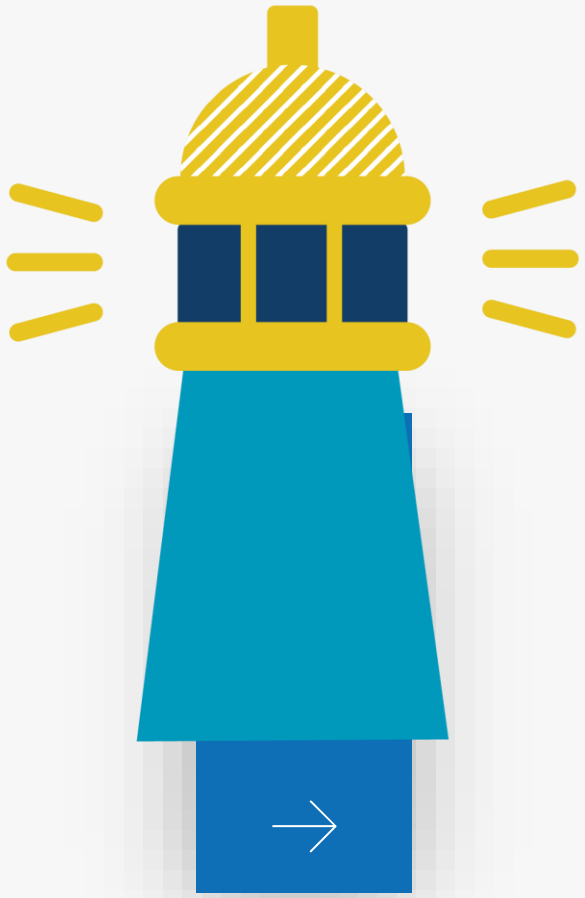
* Prioritization follows the established order but does not guarantee development.

Questions…?



Cyber ACT

Cybersecurity and Cyber Resilience Act



Security

Two sides:

- **Product** (Jems, Interact as manufacturer)
- **Consumers** (Interreg Programmes)



Product (Jems)

Manufacturer must build it with mandatory safety features: seatbelts, airbags…

Consumer (Programmes)

Ensure car is safe to drive (no cracked windows), regular inspections, obbey speed limits and report accidents.



Product (Jems)

Manufacturer must build it with mandatory safety features: seatbelts, airbags…

Cyber ACT

makers must build their products **"secure by design"**, fix vulnerabilities, and put a **CE mark** on them *before* they can be sold on the EU market.

Consumer (Programmes)

Ensure car is safe to drive (no cracked windows), regular inspections, obbey speed limits and report accidents.

NIS2 directive

Organizations must run the software securely, manage access rights, train staff, and report cyber incidents to authorities.

Cyber ACT

Designed to strengthen defense against digital threats.

It aims to protect consumers and critical infrastructure.

Cyber ACT

Cybersecurity and Cyber Resilience Act

Software manufacturer compliance requirements:

Risk Assessment: Conduct and document cybersecurity risk assessments before release.

Free Updates: Provide security patches throughout support.

SBOM: Maintain a machine-readable inventory of all software and dependencies.

Vulnerability Reporting: Report exploited vulnerabilities to CSIRTs/ENISA

CVD: Publish a vulnerability disclosure policy.

Conformity & CE: Self-assess conformity, issue an EU Declaration, and apply CE marking.

Transparency: Provide secure-use instructions, support end-dates, and technical documentation.

Jems vs Cyber ACT

Article 3(22) CRA, which defines "making available on the market" as the supply of a product with digital elements for distribution or use on the Union market in the course of a **commercial activity (...)**

Jems exists to directly support the implementation and administration of Interreg programmes rather than a commercial product or any nature of commercial activity.

Jems vs Cyber ACT

Jems non-commercial activity facts:

- **Jems is supplied exclusively to Interreg Managing Authorities and Joint Secretariats**
- **Interact does not charge license fees, subscription fees, hosting fees, support fees, maintenance fees or integration fees**
- **Jems is not marketed to commercial customers or to the public at large**
- **Interact provides Jems within the framework of its publicly funded statutory mandate**

Facts over CRA and the Commission Guidance of 27 July 2026, in particular sections 2.1, 3.2.5 and 3.3

Jems vs Cyber ACT

Key take aways:

- Jems is not under Cyber ACT
- Jems will follow Cyber ACT as reference
- New Jems shall have budget allocation aligned with security compliance

NIS2

Aims to help organizations strengthen their cybersecurity, manage risks, and respond effectively to cyber threats and incidents.

.

Directive (EU) 2022/255 (In application since October 2024)

Programmes vs NIS2

Coverage: **Depends on national transposition laws** in your member state.

Criticality

a) **Essential Entities:** proactive, unannounced audits and inspections.

b) **Important Entities:** reactive supervision (audits triggered after an incident or complaint).

Programmes vs NIS2

Comply with the 10 Core Security Measures (Article 21)

1. **Risk Management & Policies:** Set clear security rules and know your risks.

2. **Incident Handling:** Have a clear plan to detect, stop, and recover from cyber attacks.

3. **Business Continuity:** Back up your data regularly and plan for disaster recovery.

4. **Supply Chain Security: Ensure your third-party vendors and software meet high security standards.**

5. **Secure Systems Development:** Build security into your IT systems from purchase to maintenance.

6. **Effectiveness Assessment:** Regularly test and review how well your security measures work.

7. **Training & Cyber Hygiene:** Practice basic security habits and train your staff regularly.

8. **Encryption & Cryptography:** Protect sensitive data using encryption.

9. **Access Control & HR Security:** Control who can access your systems, manage your assets, and secure HR processes.

10. **MFA & Secure Comms:** Use Multi-Factor Authentication (MFA) and secure communication channels.

Programmes vs NIS2

Meet Incident Reporting Deadlines (to national competent authorities)

24 Hours: Early warning notification after becoming aware of a significant incident

72 Hours: Update of the early warning, providing an initial assessment and indicators of compromise.

1 Month: Detailed final report containing root-cause analysis and mitigation measures.

Questions…?

Coffe break!

Programmes own developments

1. **Keep.eu & Index,** Interact
2. **Elegant project report export,** Central-Europe
3. **AI Jems assistant,** Rechenwerk GmbH

Lunch time

See you at 2pm

Interact

Co-funded by the European Union

Interreg

Disclaimer

Publisher	Interact Programme
Date updated	20 October 2026
Primary knowledge area	Monitoring systems
Author(s)	Jose Almeida, Alexandra Kulmer, Pieter Louwers

Unless otherwise stated,
licensed under CreativeCommons.org.
For more information visit **creativecommons.org**

CC BY NC SA