29 January

2026

{code & compliance}

FOSDEM EDITION

libelium

29 January
2026

Operationalising the Cyber Resilience Act: From Legal Requirements to Lifecycle Security Engineering for IoT and Critical Infrastructures

Paper authors:
M. A. Ortega, A. J. Jara, I. Cuevas

Speaker:
César López

libelium

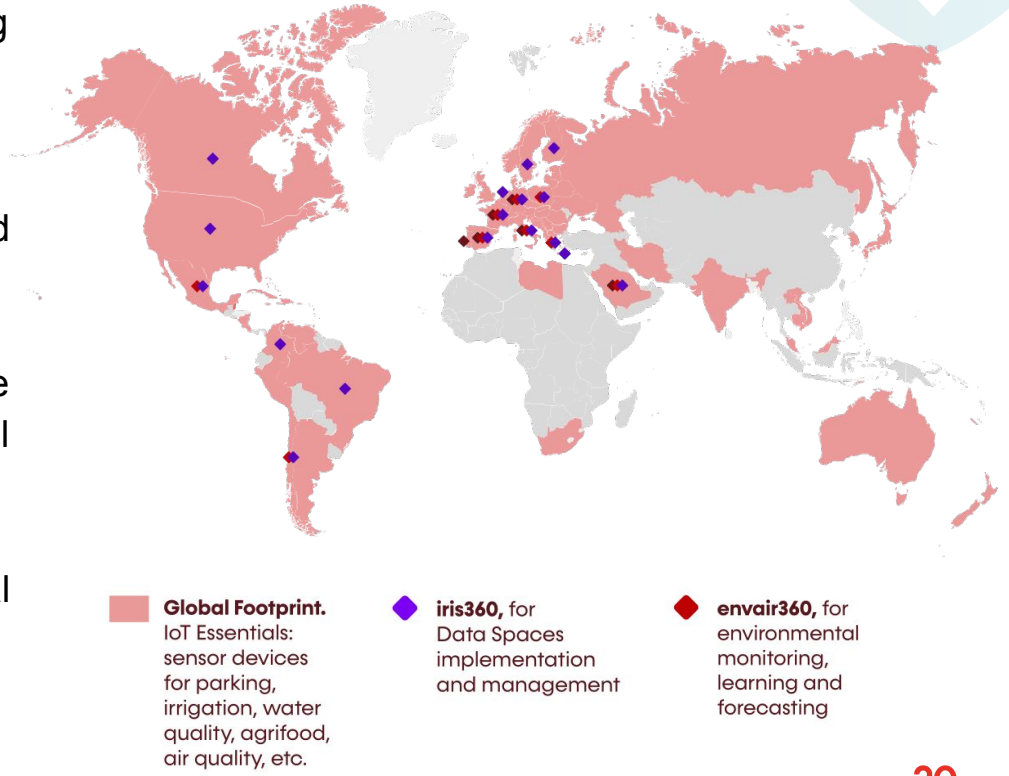
Libelium: Beyond the Challenge

Who We Are: Global IoT enablers transforming cities and industries through data.

Our Track Record: Over 120 countries reached; powering Smart Cities, Agrifood, and Critical Infrastructure.

Our Mission: Delivering high-quality, actionable data to build accurate Digital Twins of the real world.

The Focus: Bridging the gap between physical operations and digital security.



libelium
20 years behind the change

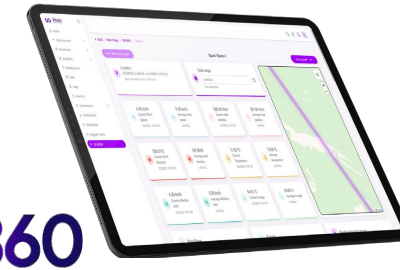
Our Technology: The IoT Ecosystem

Hardware Excellence:

- **Libelium One:** Modular node for critical sectors (Agri-Food, Water) .
- **Smart Spot:** Advanced environmental (Air/Noise) and **Crowd Monitoring** .
- **Smart Parking:** High-precision dual-detection nodes (Radar + Magnetic) .

Intelligent Platform (iris360):

- **Governance:** Unified device management and **Data Spaces connector** (GAIA-X/FIWARE) .
- **Security:** Certified **ENS High** (National Security Scheme) & ISO 27001 .



Connectivity: LwM2M End-to-End for secure, scalable operations.

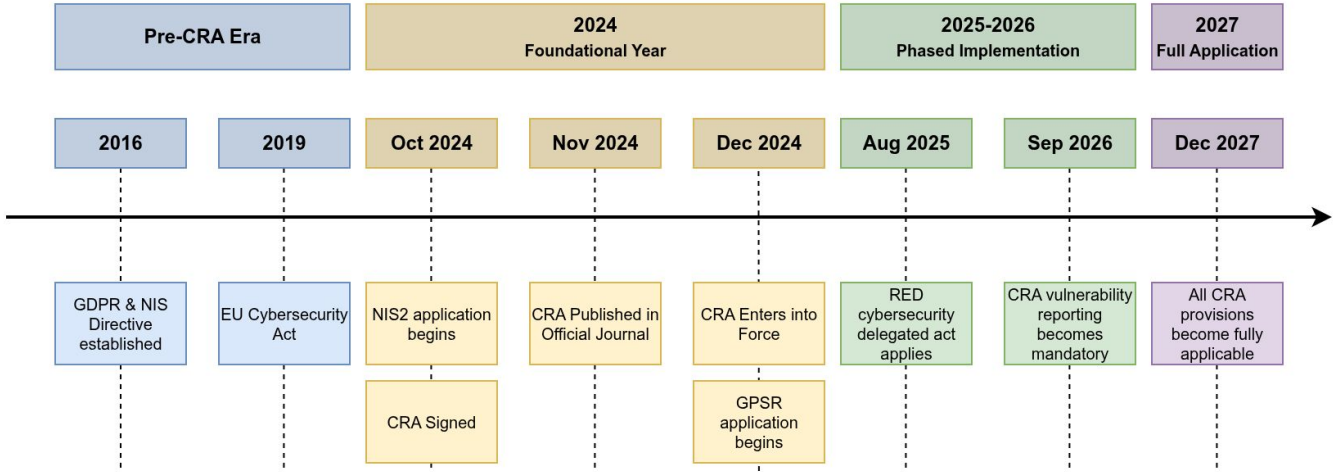
iris360
Powered by Libelium

libelium
20 years behind the change

The New Reality: The Cyber Resilience Act

Regulatory Tsunami: The EU is shifting from voluntary frameworks to binding laws.
Scope: Applies to *all* products with digital elements (PDEs), not just critical networks.
Key Deadlines:

- **2024:** Entry into force.
- **2026:** Mandatory vulnerability reporting (24h early warning).
- **2027:** Full enforcement (CE marking blocked for non-compliance).



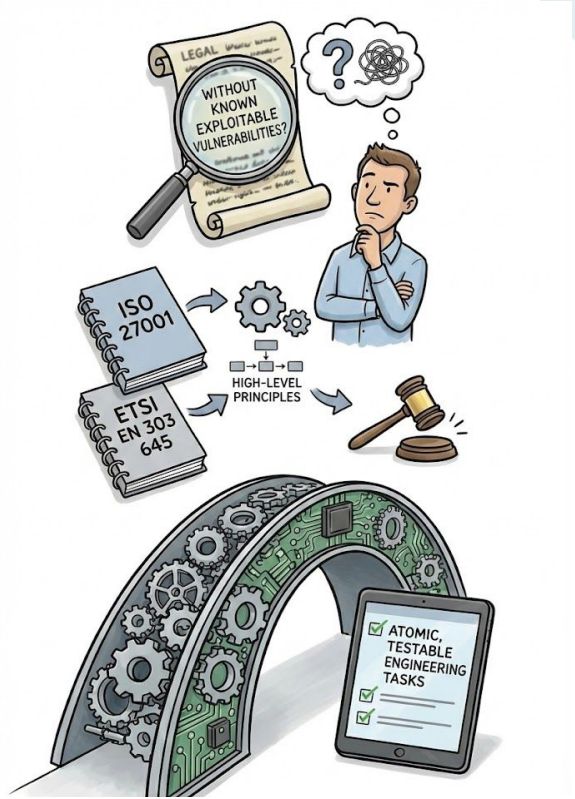
libelium
20 years behind the change

The Translation Gap: Legal vs. Engineering

Ambiguity in Mandates: Legal terms such as "without known exploitable vulnerabilities" often lack precise technical definitions for implementation.

Limitations of Standards: Existing frameworks like ISO 27001 or ETSI EN 303 645 provide high-level principles but fail to map specific legal articles directly to auditable engineering workflows.

Bridging the Gap: A systematic framework is required to translate abstract "Legalese" into atomic, testable engineering tasks.

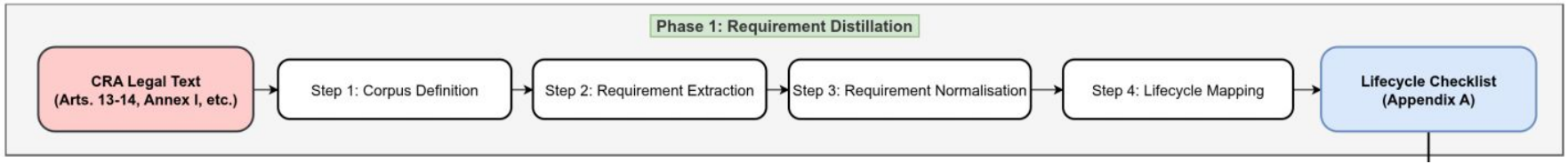


libelium
20 years behind the change

Methodology Phase 1 – Requirement Distillation

Structured Translation: We propose a transparent, four-step pipeline to convert regulatory text into a verifiable checklist:

1. **Corpus Definition:** Scoping relevant Articles (13-14) and Annexes.
2. **Extraction:** Identifying subjects, modals, and mandatory actions within the text.
3. **Normalisation:** Creating atomic, verifiable requirement statements (e.g., "Manufacturer shall provide updates").
4. **Lifecycle Mapping:** Assigning specific tasks to phases such as *Plan, Build, or Operate*.



Methodology Phase 2 – Quantitative Assessment

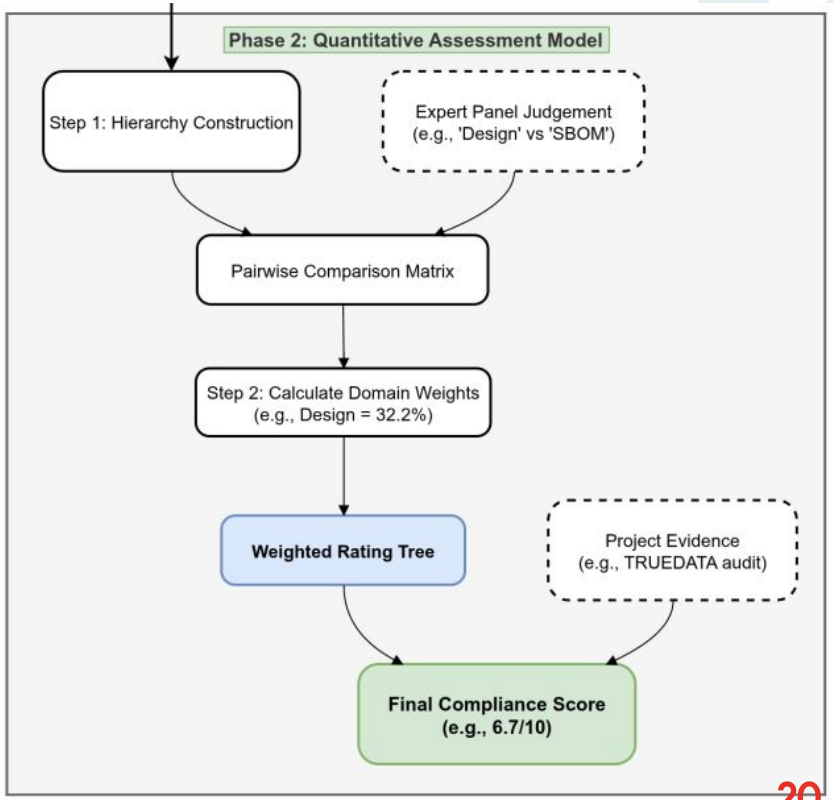
The Challenge: Not all compliance gaps are equal; subjective checklists fail to prioritize critical risks.

The Solution (Phase 2): We apply the **Analytic Hierarchy Process (AHP)** to derive mathematical weights for compliance domains based on expert judgement.

$$\text{Compliance Score} = \sum_{i=1}^{n} (W_i \times S_i)$$

Key Insight: Our model identifies 'Secure by Design' (32.2%) and 'Vulnerability Management' (21.9%) as the highest-priority domains, outweighing documentation tasks.

Outcome: A defensible **Readiness Score** (0-10) that quantifies compliance.



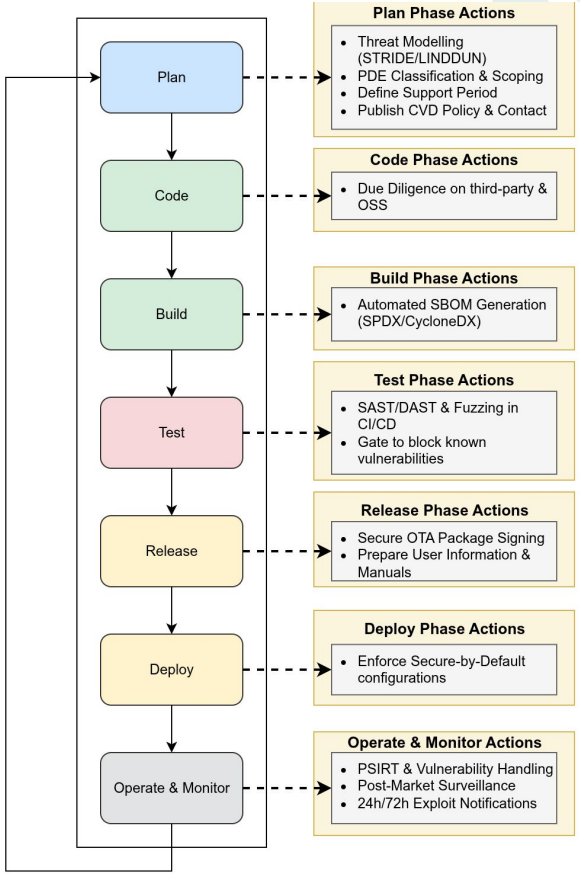
libelium
20 years behind the change

The Result: A CRA-Compliant Lifecycle

Integrated Security: Security tasks are no longer an afterthought but embedded steps.

Key Checkpoints:

- **Pre-Design:** Formal product classification and governance setup.
- **Build Phase:** Automated generation of machine-readable SBOMs (Software Bill of Materials).
- **Operate Phase:** Mandatory 24-hour early warning and 72-hour reporting for exploited vulnerabilities.
- **End-of-Life:** Implementation of secure data erasure and user notification procedures.



libelium
20 years behind the change

Validation Context: The TRUEDATA Project

Context: Validation was conducted within a high-stakes critical infrastructure environment funded by INCIBE/NextGenEU.

The Problem: Digitalisation of the water cycle exposes Operations Technology (OT) to IT threats, such as ransomware and sabotage.

The Objective: To ensure secure traceability and reliability of hydrological data using IoT, AI, and Blockchain.

Criticality: The system operates in environments where failure disrupts vital resources, such as Drinking Water Treatment Plants.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

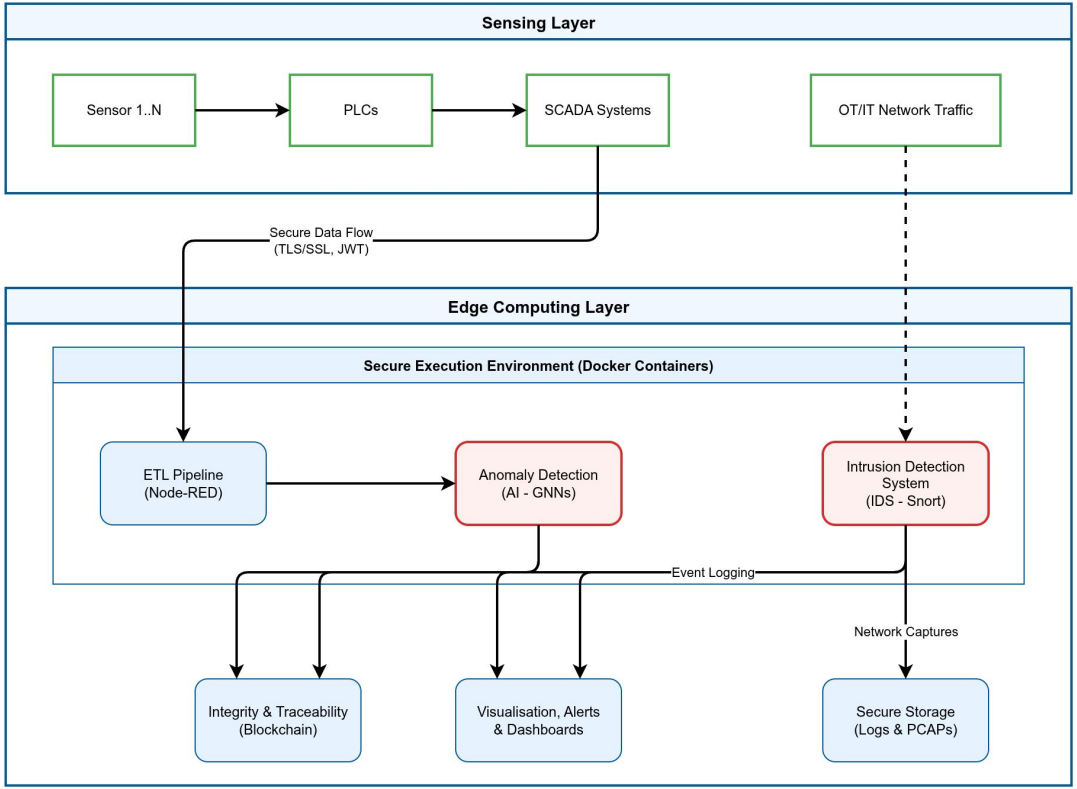
NextGenEU

libelium
20 years behind the change

TRUEDATA Technical Architecture

Hybrid Defence: A robust architecture designed for resilience and auditability:

- **Edge Computing:** AI-driven anomaly detection is performed locally to ensure low latency and continuous operation during network failure.
- **Blockchain Integration:** Guarantees the immutability of security logs for forensic validity and audit trails.
- **IDS (Snort):** Provides deep packet inspection for industrial protocols (Modbus, OPC-UA) to detect specific command injections.

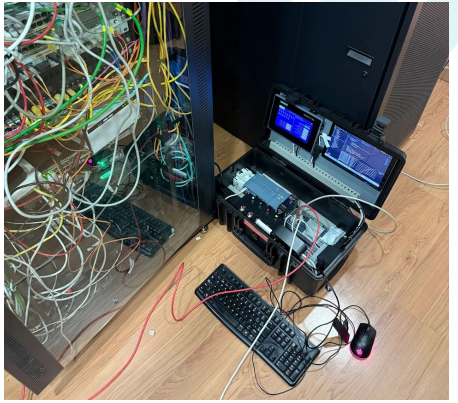


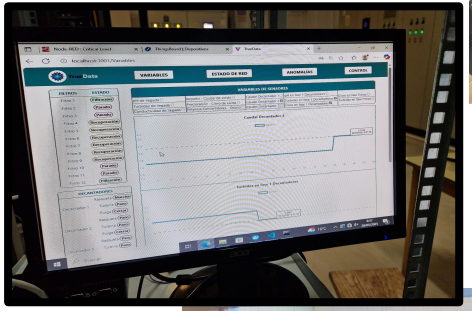
libelium
20 years behind the change

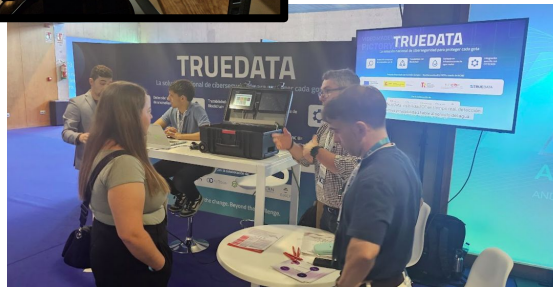
TRUEDATA Real-World Deployment: 3 Use Cases

Real-World Validation: The technology was deployed across diverse industrial scenarios:

- **Use Case 1 (Public Utility):** Drinking Water Treatment Plant (ETAP), protecting PLCs and SCADA systems from external manipulation.
- **Use Case 2 (Sanitation):** Wastewater Treatment Plant (EDAR), monitoring critical variables in complex biological processes.
- **Use Case 3 (Industry 4.0):** Private chemical production plant, securing the water supply chain for manufacturing.







libelium
20 years behind the change

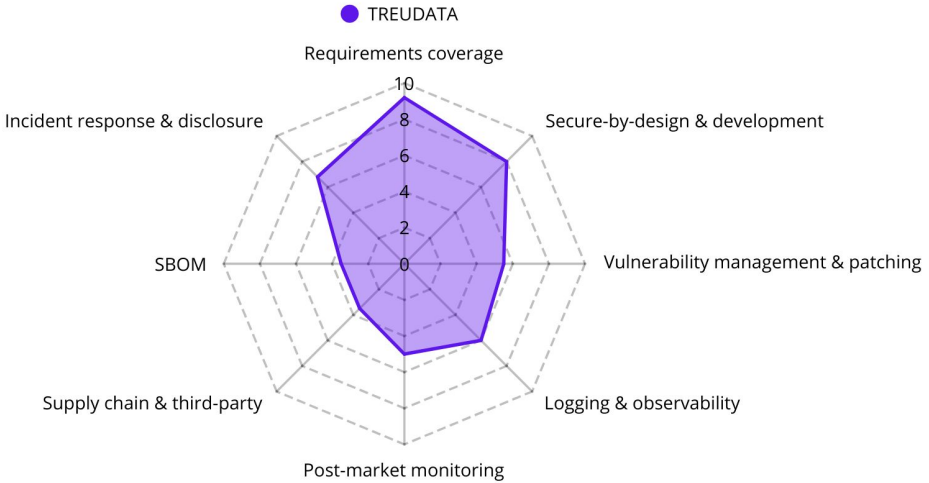
The Verdict: Compliance Scoring

Audit Result: The methodology applied to TRUEDATA yielded a score of **6.7/10** (Partial Compliance).

Insight:

- **Strong Technical Security (9.2):** Robust architecture and monitoring.
- **Weak Governance (3.5):** Lack of automated SBOMs and formal CVD policies.

Value: The tool successfully identified *process* gaps despite *technical* maturity.



libelium
20 years behind the change

Open Challenges & Lessons Learned

Ambiguity: Manufacturers struggle with the lack of harmonised standards for terms like "Limited Attack Surface".

Supply Chain: Generating accurate, machine-readable SBOMs for deep dependency trees remains operationally difficult.

Cost of Support: The 5-year mandatory support period poses a significant financial challenge for low-cost IoT business models.

Strategic Shift: The CRA should be treated as a governance layer for Zero-Trust engineering, rather than a simple checklist.

Conclusions & Key Takeaways

Operationalised Compliance: We have successfully translated abstract legal text into actionable engineering requirements.

Validated Framework: The methodology is proven effective in high-stakes critical infrastructure environments (TRUEDATA).

Strategic Advantage: Adopting CRA standards early transforms regulatory pressure into a competitive edge for hardware manufacturers.

Final Thought: Compliance is not a bureaucratic checklist; it is a core engineering discipline.

Link: Integrating the CRA into the IoT Lifecycle: Challenges, Strategies, and Best Practices

29 January

2026

{code & compliance}

FOSDEM EDITION

libelium