ENFORCERS

ENHANCED COOPERATION FOR CYBERSECURITY

COORDINATED CYBER RESILIENCE FOR INDUSTRIAL ENVIRONMENTS

CHALLENGES

A cyberattack on an industrial system can halt production, endanger people, and cause lasting damage. As factories and plants become more connected and software-defined, the risk of vulnerabilities and cyberattacks grows, and so does the need to act. When a vulnerability is discovered, speed matters. But updating software across complex industrial environments is slow, difficult, and risky.

REQUIREMENTS

Industrial organizations need better ways to gather threat intelligence, coordinate response, and restore secure operations before damage spreads. Real resilience demands trusted cooperation across the entire value chain, from manufacturers, operators, and Security Operations Center (SOCs) to technology providers, certification bodies, and public stakeholders.

SOLUTION

ENFORCERS brings industrial cybersecurity together in one trusted platform, connecting Operational Technology (OT)-level detection, SOC coordination, secure data exchange, and reliable software updates in a seamless end-to-end workflow.

The payoff: faster response, lower recovery costs, and a clear competitive edge through stronger compliance readiness for Cyber Resilience Act (CRA), Network and Information Security 2 (NIS2), and certification — without disrupting operations.

FROM DETECTION TO RESOLUTION — IN ONE TRUSTED WORKFLOW

ENFORCERS connects the key steps of industrial cybersecurity into a coordinated lifecycle:

1. MONITOR

Relevant system behavior and vulnerability data are continuously monitored to capture cybersecurity-relevant information at an early stage.

2. DETECT AND CLASSIFY

Threat information is filtered, enriched, and classified, supported by Artificial Intelligence (AI)-driven analysis.

3. REPORT AND COORDINATE

Vulnerability and incident information is received, correlated and shared between private SOCs to enable a coordinated response.

4. MITIGATE

Identified vulnerabilities and threats are addressed through structured workflows and secure software supply chain practices.

5. REDEPLOY SECURELY

Renewed software is delivered through trusted Points of Deployment to ensure secure and authorized rollout.

6. IMPROVE THE LIFECYCLE

Operational insights are used to strengthen product security and long-term lifecycle resilience.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

EXPECTED IMPACT

ENFORCERS creates measurable impact across the industrial cybersecurity ecosystem accelerating incident handling, strengthening trusted cooperation, enabling secure software updates, and improving regulatory readiness and long-term cyber resilience.

FOR MANUFACTURERS

Clear, practical pathways to lifecycle security, regulatory compliance (e.g. CRA, NIS2), and Software Bill of Materials (SBOM) integration.

FOR OPERATORS

Shorter downtime, lower recovery effort, and verified, authorized software updates.

FOR CYBERSECURITY COMMUNITIES

Stronger cross-border cooperation and better alignment between private SOCs, Computer Security Incident Response Teams (CSIRTs), and public response structures.

FOR EUROPE

Greater cybersecurity capacity, stronger digital sovereignty, and more resilient industrial infrastructure, contributing to Europe's strategic autonomy in critical sectors.

STAKEHOLDER CONTRIBUTIONS

ENFORCERS is a collaborative project built on strong stakeholder engagement. Achieving this vision requires active involvement of experts across industry, cybersecurity, research, certification, and public policy.

Get involved and share your perspective!

Stakeholder contributions may include:

- ✓ **Manufacturers of industrial automation and control systems** can contribute real-world requirements, processes, and challenges.
- ✓ **Operators of industrial and critical infrastructures** can share operational insight into deploying secure software updates in live environments.
- ✓ **Cybersecurity communities** can contribute expertise in incident workflows, escalation models, and vulnerability classification.
- ✓ **Certification, standardization, and regulatory stakeholders** can provide guidance on compliance and emerging industrial cybersecurity standards.
- ✓ **Technology providers** can add practical expertise and valuable market perspectives.
- ✓ **Research organizations** can contribute scientific expertise and help to ensure the platform's forward-looking development.

CONSORTIUM

ENFORCERS brings together complementary expertise from industrial automation, cybersecurity, software engineering, semiconductor technology, secure elements, SOC operations, AI, certification, standardization, and applied research.

ENFORCERS

CONTACT

Project Coordinator

WIBU-SYSTEMS AG

project-info@enforcers.eu

FUNDING DISCLAIMER

The project funded under Grant Agreement No. **101249745** is supported by the **European Cybersecurity Competence Centre.**

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 the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.