

How Industrial Defender closes the OT asset visibility gap behind NIS2 compliance — across every member state's transposition.

NIS2 BACKGROUND

A Unified Baseline, Enforced Nationally

The NIS2 Directive (EU) 2022/2555 strengthens cybersecurity across essential and important entities in energy, water, transport, manufacturing, digital infrastructure, and other critical sectors.

Member states were required to transpose it into national law by October 17, 2024; enforcement is ongoing. Essential entities face fines up to €10M or 2% of global revenue — important entities, €7M or 1.4% — depending on national transposition.

The Commission Implementing Regulation (EU) 2024/2690 operationalizes Article 21, specifying 13 technical and methodological measures that form the compliance baseline — detailed below alongside how Industrial Defender supports each one.

13

Annex measures

27Member states,
one directive**2012**

Serving EU DSOs since

3Frameworks
reported natively

The Annex's 13 Technical and Methodological Measures

01Policy on security of network
& information systems**08**Basic cyber hygiene & security
training**02**

Risk-management policy

09

Cryptography

03

Incident handling

10

Human-resources security

04Business continuity & crisis
management**11**

Access control

05

Supply-chain security

12

Asset management

06Security in system acquisition,
dev & maintenance**13**

Environmental & physical security

07Effectiveness assessment of risk
measures

ENISA's non-binding NIS2 Technical Implementation Guidance complements the Regulation with practical mappings to ISO/IEC 27001 and NIST CSF 2.0.

THE CHALLENGE

One Directive. 27 Different Realities.

NIS2 is a directive, not a regulation — it sets a minimum-harmonization floor, and member states are free to “gold-plate” on top of it. For operators running assets across borders, the program that satisfies one national authority may not satisfy the next.

Germany

One of the most prescriptive transpositions in the EU — in-scope entities must register directly with the BSI, with compliance proof requirements that go beyond the Annex floor.

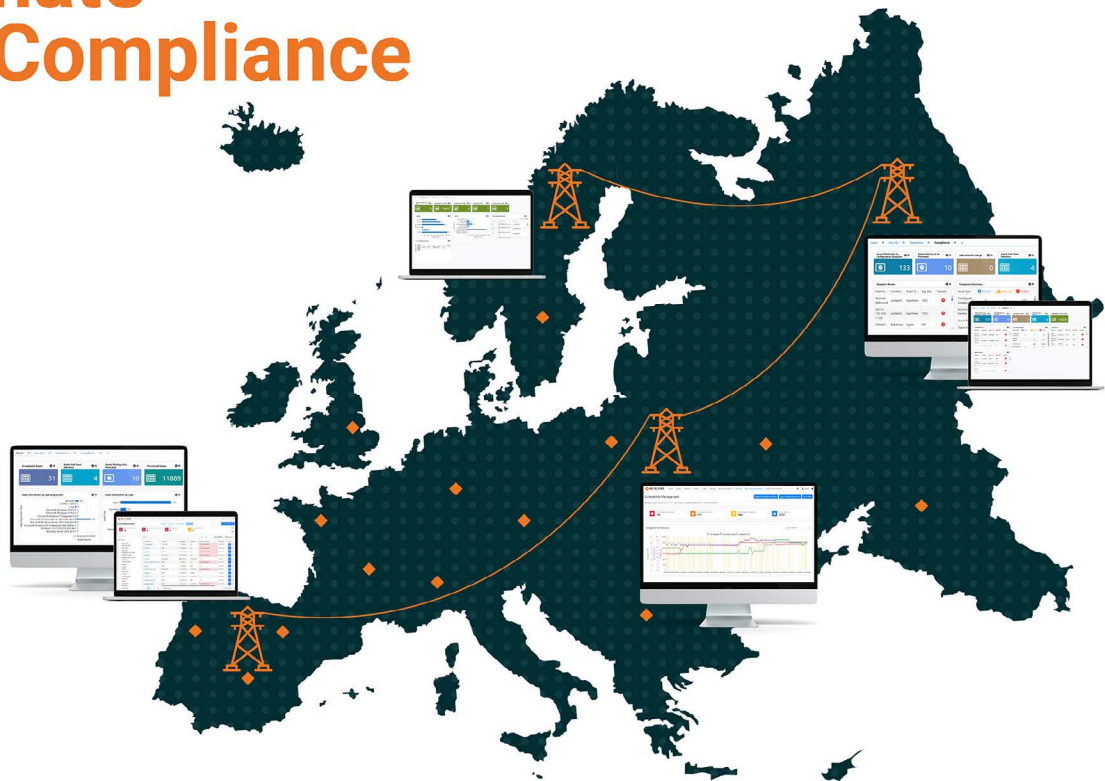
Denmark

A materially different approach to scope and supervisory structure than Germany’s — proof that transposition details, not just enforcement dates, diverge in ways operators can’t assume are interchangeable.

The Other 25+

Every remaining member state sets its own thresholds, audit and testing requirements, and reporting timelines within the Annex floor — with no unified EU registry to cross-reference status outside digital service providers.

Automate NIS2 Compliance



The practical result for cross-border operators: build one evidence base — grounded in complete OT asset data — that holds up regardless of which national authority is asking.

HOW INDUSTRIAL DEFENDER SOLVES NIS2

One Data Set, Mapped to the Full Annex

Industrial Defender's continuous OT asset, configuration, and vulnerability data maps to the Annex's 13 measures across five operational pillars:

Governance & Risk Management

Annex 1, 2.1, 2.2, 7

Reporting aligned to major frameworks; a risk dashboard combining asset context with threat intelligence; dashboards and trend reports to demonstrate control effectiveness over time.

Incident Handling & Continuity

Annex 3, 4

Integrated monitoring and logging enriched with asset context for detection and escalation; historical OT asset data to validate recovery states against known-good baselines.

Technical Controls & Vulnerability Management

Annex 5, 6, 9

Continuous configuration baselining and change detection; risk-based vulnerability management by exploitability and criticality; network visibility across firewalls and OT protocols.

People & Access

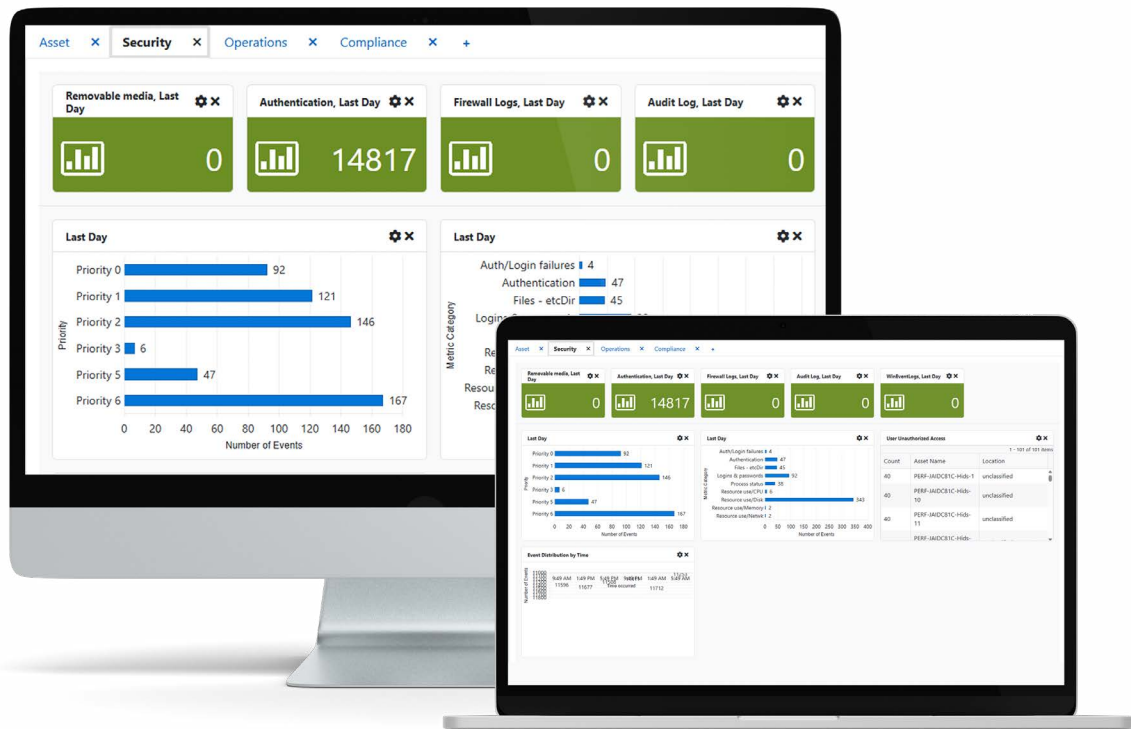
Annex 8, 10, 11

Identifies misconfiguration and drift against hardening baselines; monitors account activity and access changes; visibility into privileges and MFA enforcement evidence.

Asset Management

Annex 12

Continuously updated inventory built from Passive, IDC, and Agent collection — type, firmware, role, location — the foundation every other measure depends on.

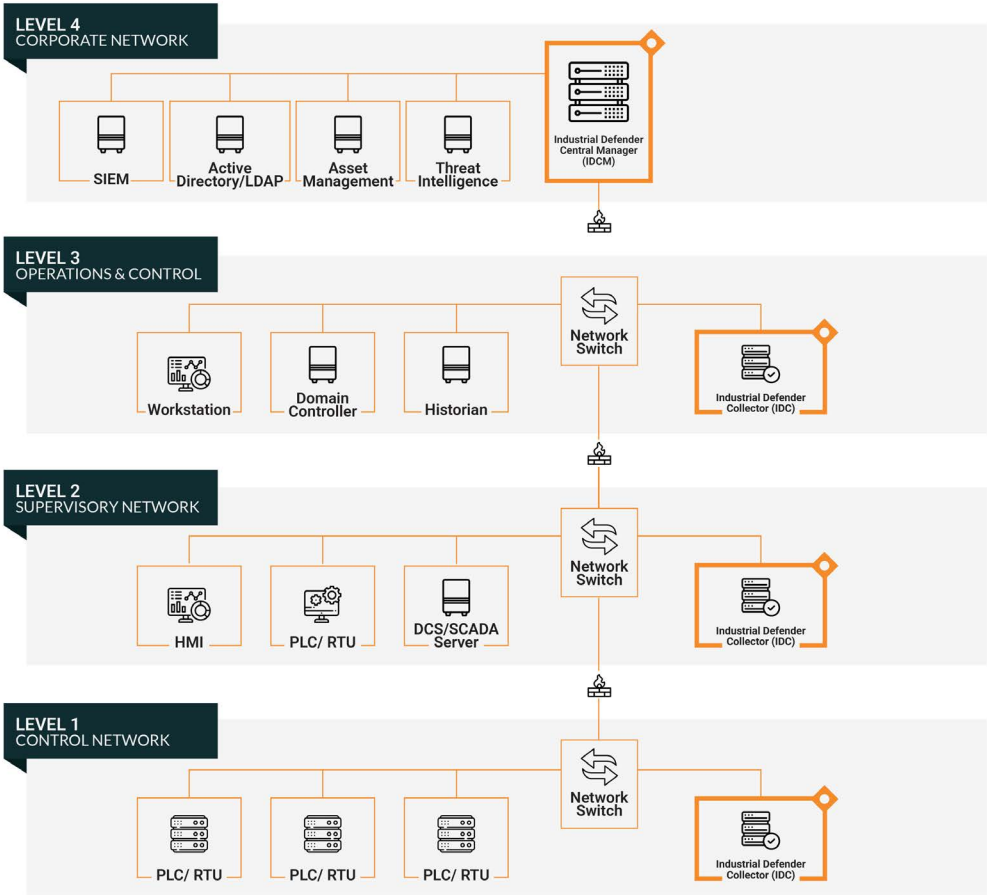


DEPLOYMENT

Three Methods, Matched to Your Environment

Annex 12.4 requires a continuously updated inventory of every OT asset. Passive-only monitoring sees what talks on the wire; closing the gap means reaching down to Level 1, where dormant, air-gapped, and protocol-native controllers actually live.

Method	Where It Fits	Footprint
Passive Monitoring	Network traffic analysis: Interprets industrial protocols on the wire to identify devices and capture abnormal events	No direct device interaction
IDC (Agentless Active Collection)	The Industrial Defender Collector queries devices directly via native OT protocols (DNP3, Modbus, S7) and IT protocols (SSH, SNMP, HTTPS)	No software installed on the device
Agent	Windows, Linux, Unix endpoints; ID Reach provides the same depth as a portable, no-persistent-service option for air-gapped or sensitive assets	Under 1% CPU



< 8 wks

Deployment timeline

\$3M

Avoided upgrade costs

Since 2006

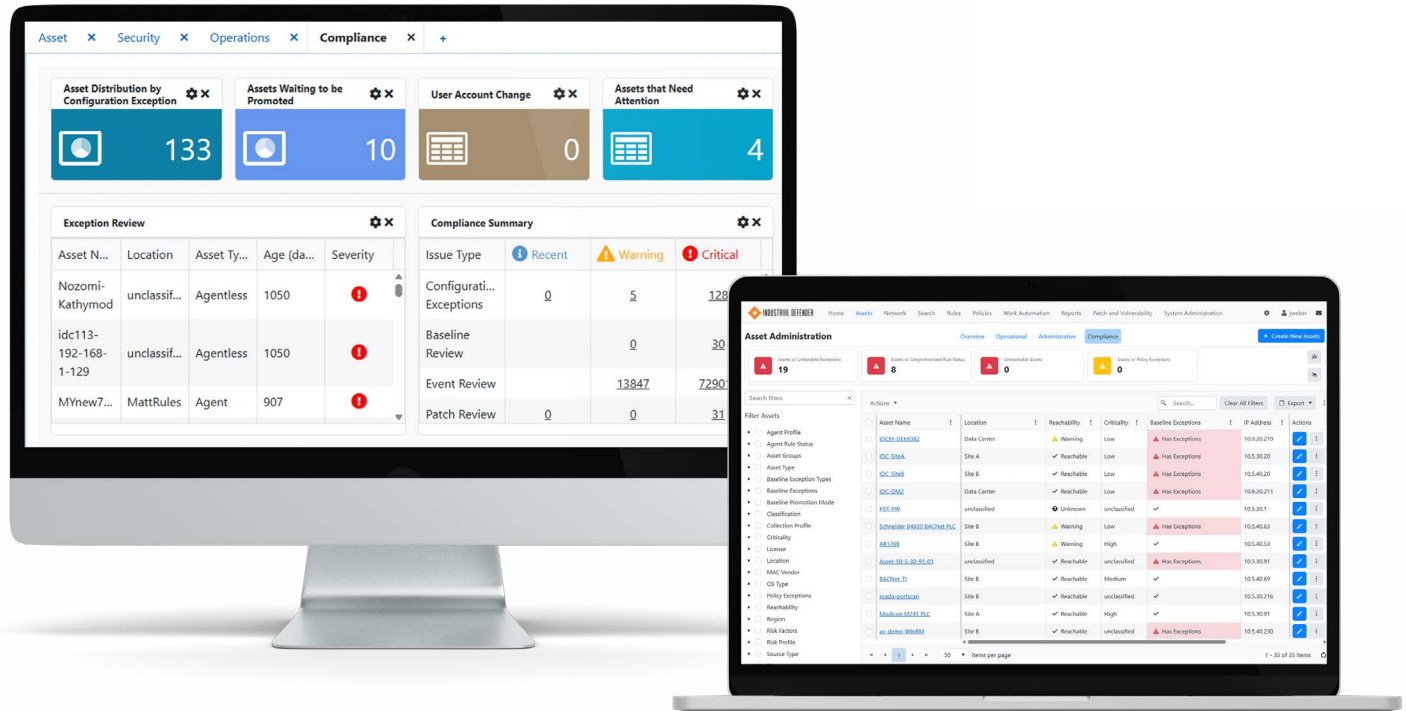
Active collection, operationally safe

INDUSTRIAL DEFENDER

Conclusion

NIS2 and its Implementing Regulation establish a unified baseline for cybersecurity across the EU — an EU-level framework overlaying each member state's national laws. But “unified” applies to the floor, not the details: 27 transposition models mean the compliance program that works in one country may fall short in the next.

With a decade of production experience securing European critical infrastructure and two decades running active OT collection safely, Industrial Defender is equipped to help operators automate the evidence collection NIS2 requires — regardless of which national authority is asking.



[SCHEDULE A DEMO](#)

CONTACT

1 (877) 943-3363 • (617) 675-4206
info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
[industrialdefender.com](https://www.industrialdefender.com)

© 2026 iDefender, LLC

