
6 AREAS WHERE NIS2 REQUIRES HARD EVIDENCE

And why most OT operators struggle with each one.

Swipe →



01 ASSET INVENTORY

A current, complete asset inventory

Most sites have a procurement list. NIS2 asks for something different: a live, protocol-aware view of every device on your industrial network, with firmware versions, communication paths, and business criticality. If that inventory was last updated during a project handover, it isn't the evidence a regulator is looking for.

“Across close to one million OT devices analysed, 12% contained known exploited vulnerabilities, and 40% of organisations had some of those assets insecurely connected to the internet.”

Claroty Team82 · State of CPS Security 2025

02 REMOTE ACCESS

Authorised access, with an evidence trail

Remote access is the single most common OT incident entry point. NIS2 expects you to demonstrate who connected, when, from where, and what they did. Session logs, MFA enforcement, and vendor access controls aren't optional extras. They're what separates a documented security posture from a verbal one.

“Half of OT incidents in 2025 began with unauthorised external access, often through third-party remote maintenance.”

SANS ICS/OT Cybersecurity Survey 2025

03 DETECTION

Detection you can act on

NIS2 sets a 24-hour early warning requirement from the moment you become aware of a NIS2-relevant significant incident. Detection is improving for operators who invest in OT monitoring. For those who don't, the gap is widening, and "becoming aware" can still mean a production stop rather than an alert.

"Organisations with comprehensive OT visibility detected and contained ransomware in an average of 5 days, against an industry-wide average of 42 days."

Dragos 2026 OT/ICS Cybersecurity Report

04 SEGMENTATION

Tested segmentation between IT and OT

Many sites believe they have IT/OT segmentation. Passive monitoring regularly finds something different: legacy machines with direct internet exposure, PLCs reachable from corporate networks, maintenance laptops bridging zones. Segmentation that's never been verified is a policy position, not a security control. Regulators are starting to treat it that way.

“In recent OT assessments, unexpected IT/OT network paths were found in 7 of 10 environments.”

Nautilus OT field data • 2025–2026

05 INCIDENT RESPONSE

An exercised incident response plan

Policies aren't evidence. Supervisory authorities increasingly ask for exercise records: tabletop sessions, OT-specific scenarios, documented outcomes, named roles with sign-off. An IRP written for IT and stretched to cover OT is a common gap. Operational failure modes are different, and the response timeline is compressed by production pressure.

“Fewer than 30% of OT operators had run a formal ICS-specific incident response exercise in the past 12 months.”

SANS ICS/OT Cybersecurity Survey 2025

06 NOTIFICATION

A 72-hour detailed notification capability

After the 24-hour early warning, NIS2 requires a comprehensive notification within 72 hours: scope of impact, systems affected, likely cause, initial remediation. Meeting that isn't a communications challenge. It's an operational one, and it assumes detection, classification, and escalation already work. The clock runs whether you're ready or not.

“Most OT operators have not formally mapped which incidents trigger NIS2 notification obligations.”

Nautilus NIS2 readiness assessments · Netherlands & Belgium, 2025

We help OT operators build the evidence, not just the policies.

From asset inventory to incident response readiness, we work alongside your team to close the gaps before the auditor does. Whether you're preparing for a NIS2 supervisory review, running a first OT security assessment, or translating IT controls into OT reality, we'd like to hear what you're working with.

DM us or book a 30-minute session. No commitment.