PENTESTERRA

PARTNER SERVICES OVERVIEW

Start the Conversation with NIS2. Let It Open the Rest.

A short guide to the five services your clients need most right now, and how one entry point, a NIS2 technical gap assessment, naturally leads to the other four. Built for partners packaging Pentesterra into their own security and compliance offering.

€10M / 2%

Maximum NIS2 fine for essential entities: €10,000,000 or 2% of global annual turnover, whichever is higher

23 / 27

EU member states had transposed NIS2 into national law as of mid-2026

Live

First NIS2 fines already issued in Belgium, Italy and Hungary, no longer a theoretical deadline

Why lead with NIS2

ENTRY POINT

NIS2 Technical Gap Assessment & Report

→

Vulnerability Assessment
Every unmet technical control becomes a scoped, quotable engagement.

Network Penetration Testing
Gaps that need active proof, not just a scan result, become a pentest.

Phishing & Awareness
NIS2's human-risk-management article becomes a training program.

Compliance, beyond NIS2
The same evidence extends to GDPR, ISO 27001, DORA and 9 more standards.

Talking points for your first client call

- **It's not optional anymore.** Most EU member states have transposed NIS2 into national law, and regulators have already issued the first fines. "We'll deal with it eventually" is no longer a safe answer.
- **The scope is bigger than clients think.** NIS2 covers many mid-sized companies that never had a compliance obligation before, energy, transport, health, digital infrastructure, manufacturing, and their suppliers.
- **One assessment answers the real first question.** Before a client can plan a budget or a roadmap, they need to know where they actually stand, control by control, not a guess.
- **The gap report is the sales tool.** It doesn't just satisfy the client, it hands you, the partner, a prioritized, evidenced list of exactly what to sell next and why.
- **Nothing has to be re-tested.** Every technical finding from the assessment carries straight into the vulnerability, pentest, and compliance work that follows, no duplicated engagements.

FLAGSHIP SERVICE

NIS2 Technical Gap Assessment & Report

A structured, evidence-based read of where a client's organization stands against NIS2's Article 21(2) security measures, sector applicability included. Not a legal opinion and not a certification: a clear, control-by-control map of what's met, what's partial, and what's an open gap, built from real technical evidence wherever evidence can be produced automatically.

WHAT IT COVERS

- ✓ Sector and entity-type applicability (essential vs. important, per national transposition)
- ✓ All Article 21(2)(a)–(j) measures: risk policy, incident handling, business continuity, supply chain, secure development, vulnerability handling, cryptography, access control, and more
- ✓ Automated technical evidence for every control that scanning, pentesting, OSINT, and infrastructure monitoring can answer
- ✓ A guided applicability check by sector, country, and company size before any control work starts

WHAT THE CLIENT RECEIVES

- ✓ An indicative readiness score with counts of controls met, partial, and gap
- ✓ A prioritized gap report, auditor-focus items flagged first
- ✓ A white-label, editable report suitable for their own board or auditor
- ✓ A live assessment they can keep updated, not a static PDF that's stale in a month

WHY THIS IS THE RIGHT FIRST ENGAGEMENT

NIS2 doesn't ask a company to invent a security program from scratch, it asks them to prove one that likely already exists in pieces. The gap assessment surfaces exactly which pieces are missing, in the client's own language and their own auditor's language, before anyone commits budget to fixing anything. That prioritized list is what turns a single assessment into a multi-service engagement.

€7M / 1.4%
Maximum fine for important entities under NIS2, or 1.4% of global turnover

18
High-criticality and other-critical sectors named across NIS2 Annex I and Annex II

3
Member states with confirmed enforcement fines already on the public record

The four services a gap report puts on the table

SERVICE 2

Vulnerability Assessment

Agentless scanning across the external and internal perimeter, with CVE and KEV mapping and non-destructive exploit verification, so every finding is confirmed, not guessed at.

- External and internal attack surface coverage
- Verified findings, not raw scanner noise
- Directly answers NIS2's vulnerability-handling article

Sells from: unmet technical controls

SERVICE 3

Network Penetration Testing

Active, evidenced testing of network and infrastructure security, going beyond a scan result to prove what an attacker could actually do with what was found.

- Internal and external network scope
- Real exploitation evidence, not a theoretical CVSS score
- Feeds directly into NIS2's security-testing requirement

Sells from: gaps needing active proof

SERVICE 4

Phishing & Awareness

Context-aware phishing simulation built from OSINT on the client's own organization, plus the training program NIS2's human-risk-management article expects to see documented.

- Spear-phishing scenarios, not generic templates
- Per-recipient tracking, not just a headline click rate
- Answers the human-layer half of the gap report

Sells from: cyber-hygiene training controls

SERVICE 5

Compliance, Beyond NIS2

Once the evidence exists, it doesn't stop at one framework. The same technical findings extend into a full multi-standard compliance program.

- GDPR, ISO 27001 & 27701, DORA, SOC 2, NIST CSF
- PCI DSS, CMMC, TISAX, EU Cyber Resilience Act
- HIPAA, NYDFS 500, 13 frameworks in one workspace

Sells from: "what else do we need to prove"

One evidence base, thirteen frameworks

Every technical control answered for NIS2 is reusable evidence for these standards, no repeat scanning, no repeat questionnaires for the same underlying proof.

NIS2 · GDPR · ISO 27001 · ISO 27701 · DORA · SOC 2 · NIST CSF · PCI DSS · CMMC · TISAX · EU Cyber Resilience Act · HIPAA · NYDFS 500

Ready to package this for your clients?

Ask us about partner pricing, co-branded reports, and a joint pilot engagement - no exclusivity required, no minimum commitment to start the conversation.

info@pentesterra.com
pentesterra.com/solutions/compliance