2026

seceon

France & NIS 2:

Turning a Regulatory Deadline into a Growth Opportunity

How MSPs and MSSPs can get ahead of France's Loi Résilience and help clients across France, the EU, and the UK meet NIS 2 obligations with our aiXDR Platform.

Executive Summary

France is in the final stretch of transposing the EU's second Network and Information Security Directive (NIS 2) through a single, combined law the Loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité (the "Loi Résilience"). The bill folds NIS 2 together with the Critical Entities Resilience (CER) directive and DORA-related provisions into one national framework, supervised by ANSSI, France's national cybersecurity agency.

The Senate adopted the bill in March 2025, the National Assembly's special commission voted it through in September 2025, and final adoption is now expected during an extraordinary parliamentary session in 2026, with implementing decrees to follow. In the meantime, ANSSI has already published a preparatory technical reference (Référentiel Cyber France, or ReCyF) and opened a self-registration portal, MesServicesCyber. ANSSI's own guidance has been consistent: organizations should begin risk assessments and system mapping now, rather than wait for promulgation.

For MSPs and MSSPs, this moment is not just a compliance deadline for clients to worry about it is a direct commercial opening. NIS 2 explicitly brings managed service providers and managed security service providers into scope as regulated entities in their own right, while simultaneously creating a large pool of newly regulated "essential" and "important" entities across France that will need help meeting the law's technical and organizational requirements. Partners who can demonstrate NIS 2 readiness for themselves and for the clients they protect have a clear, time-boxed reason to open new conversations.

> ***Why this matters now***
>
> *France's transposition brings roughly 15,000 additional entities into scope nationally, across sectors from energy and transport to food, waste management, and local government. Whatever the exact promulgation date, the underlying NIS 2 obligations are already shaping procurement conversations, cyber-insurance underwriting, and board-level risk discussions across France, the wider EU, and the UK's parallel Cyber Security and Resilience Bill.*

This paper summarizes where France's NIS 2 transposition stands, what it requires, who it affects, and how our aiXDR Platform built from the ground up for multi-tenant MSP and MSSP delivery maps directly to the law's core obligations. It closes with a straightforward path for partners to package NIS 2 readiness as a service. Sources consulted are listed in the Works Cited section on the final page.

1. Where France Stands on NIS 2

A directive already in force, a national law still in motion

NIS 2 (Directive (EU) 2022/2555) entered into force in January 2023 and required EU member states to transpose it into national law by 17 October 2024. France, like a majority of member states, missed that deadline. The European Commission opened formal infringement proceedings against France in late 2024 and escalated to a reasoned opinion in May 2025 for failure to fully notify transposition. Rather than transpose NIS 2 as a stand-alone act, France chose to fold it into a broader Loi Résilience covering critical-infrastructure resilience (CER) and cybersecurity governance together. Key milestones so far:

- October 2024 — Bill presented to the Council of Ministers.
- 12 March 2025 — Adopted by the Senate in first reading.
- 10 September 2025 — Advanced by the National Assembly's special commission.
- 17 March 2026 — ANSSI publishes the Référentiel Cyber France (ReCyF) as a bridging technical framework ahead of formal promulgation.
- 2026 — Final adoption expected during an extraordinary parliamentary session, with implementing decrees to follow. A draft decree already outlines 20 security objectives for essential entities and 15 for important entities.

Until the law is promulgated, registration on ANSSI's MesServicesCyber portal remains voluntary but ANSSI has publicly urged organizations not to wait, given how much of NIS 2's substance is already settled at EU level and unlikely to change materially in the final French text.

France is not alone and that is exactly the point

As of mid-2026, roughly two-thirds of EU member states have completed transposition, while France, Ireland, Luxembourg, the Netherlands, and Spain remain in active legislative process. The United Kingdom, no longer bound by NIS 2 as an EU directive, is running its own parallel update: the Cyber Security and Resilience Bill was introduced to Parliament and adopted at first reading in November 2025.

For any partner or prospect operating across borders which describes most mid-market and enterprise organizations in France, the wider EU, and the UK this creates a patchwork of entry-into-force dates, competent authorities, and reporting channels layered on top of a shared set of underlying obligations. That complexity is itself a sales conversation: organizations need a single security operations platform that can produce the evidence and reporting each jurisdiction expects, regardless of exactly when each national law lands.

2. Who Is Affected - Including MSPs and MSSPs Themselves

Two tiers, a much wider net

France's transposition follows the EU's two-tier structure: Entités Essentielles (EE) for higher-criticality sectors such as energy, transport, banking, and health, and Entités Importantes (EI) for a broader range of sectors including postal services, waste management, food, chemicals, and digital providers. A defining shift from the earlier NIS 1 regime is scope: obligations generally apply to an organization's entire information system, not just a narrowly designated critical server or service.

Crucially for this audience, NIS 2's Annex I explicitly lists "ICT service management (business-to-business)" covering managed service providers and managed security service providers as an in-scope sector in its own right. MSPs and MSSPs operating in France, or serving clients there, should assume they may be directly regulated, independent of whether their end customers are also in scope.

> ***The dual exposure***
>
> *An MSP/MSSP serving French or EU clients can be in scope twice over: once as a regulated entity itself, and again as a supply-chain dependency that its essential- and important-entity clients must now formally assess under NIS 2's Article 21 supply-chain security requirement. Being demonstrably NIS 2-ready is fast becoming table stakes to keep and win regulated accounts.*

What non-compliance costs

The directive sets minimum fine ceilings that member states may raise: up to €10 million or 2% of global annual turnover for essential entities, and up to €7 million or 1.4% for important entities whichever is higher. France's enforcement model, as currently drafted, follows a graduated path: ANSSI issues a written warning (mise en demeure), then a formal order (injonction) that can carry a daily penalty of up to €5,000, before a separate sanctions commission imposes the administrative fine itself. Organizations that correct course between warning and order generally avoid the fine which rewards partners and platforms that can demonstrate rapid remediation.

Article 20 also introduces personal accountability for management bodies, including the possibility of temporary director disqualification in serious cases. That single provision tends to move NIS 2 from an IT-department concern to a board-level agenda item and a natural opening for partner-led briefings.

3. What NIS 2 Actually Requires

Stripped of jurisdictional detail, NIS 2's substantive obligations fall into four groups that any in-scope organization and any MSP/MSSP supporting one needs to operationalize:

Article 21 Ten minimum security measures

Organizations must implement a documented, risk-based set of measures, including: risk analysis and information-system security policies; incident handling; business continuity and crisis management (including backup and disaster recovery); supply-chain security covering suppliers and service providers; security in the acquisition, development, and maintenance of systems; policies to assess the effectiveness of security measures; basic cyber hygiene and staff training; policies on cryptography; human-resources security, access control, and asset management; and the use of multi-factor authentication or continuous authentication solutions.

Article 23 — Fast, tiered incident reporting

In-scope entities must notify their national CSIRT or competent authority (ANSSI, in France) of significant incidents on a strict clock: an early warning within 24 hours of becoming aware of an incident, a fuller incident notification within 72 hours, and a final report within one month. Getting this timeline wrong or missing it is itself a compliance failure, independent of the underlying incident.

Article 20 — Governance and personal accountability

Management bodies must approve the organization's cybersecurity risk-management measures, oversee their implementation, and complete cybersecurity training themselves. This requires reporting that a board can actually read and act on, not just SOC dashboards built for analysts.

Supply-chain and registration obligations

Entities must assess and manage cybersecurity risk in their supplier and service-provider relationships, and once France's law is promulgated, register core organizational and network details (contact points, IP ranges, sectors of activity) through ANSSI's MesServicesCyber portal under Articles 3 and 27.

4. Our aiXDR Platform: Architecture, Compliance Fit, and Economics

This section goes deeper into what actually sits behind the platform: the engines it's built from, a measure-by-measure mapping against NIS 2's Article 21 requirements, the operating economics that matter to an MSP/MSSP business, and field evidence of the platform in production.

4.1 Platform architecture at a glance

Our Open Threat Management (OTM) platform is built around a small number of core engines that ingest, correlate, and act on telemetry, rather than a bundle of loosely connected point products:

- **aiSIEM** — collects and analyzes logs and events from across the environment, using AI/ML rather than static correlation rules alone to identify anomalies and prioritize alerts.
- **aiXDR** — extends detection and automated response across endpoints, network, and cloud, correlating signals across domains to catch multi-stage attacks that any single tool would miss.
- **SOAR** — orchestrates and automates response workflows (containment, ticketing, notification) so that remediation happens in seconds rather than waiting on manual analyst action.
- **UEBA** — baselines normal user and entity behavior and flags deviations such as credential abuse, privilege escalation, and insider misuse.
- **Dynamic Threat Models (DTM)** — apply contextual, continuously updated risk scoring so alerts are prioritized by actual business risk, not just raw signal volume.
- **aiCompliance CMX360** — the compliance engine, covered in detail in Section 4.5, that automatically maps existing security telemetry to controls across NIS 2, DORA, ISO 27001, and dozens of other frameworks.
- **Analytics & Policy Engine (APE) and Collection & Control Engine (CCE)** — the underlying components that MSSPs deploy per tenant; our hosted APE options let partners offload infrastructure management and patching to us.

We built this stack to replace the disconnected SIEM, XDR, SOAR, NDR, UEBA, and vulnerability-management tools many MSSPs previously had to license and integrate separately.

4.2 Measure-by-measure: Article 21 mapped to the platform

NIS 2's Article 21 sets out ten categories of risk-management measure. The table below maps each one directly to the platform capability that addresses it the level of detail a partner needs when walking a prospect's compliance or audit team through a gap assessment.

NIS 2 Obligation	How the aiXDR Platform Delivers It
(a) Risk analysis & information-system security policies	Continuous, AI-driven visibility across endpoints, networks, identities, cloud, and applications replaces point-in-time audits with a continuously updated risk posture, providing the evidence needed to support security policies and ongoing risk management.
(b) Incident handling	aiXDR correlates telemetry across the entire environment and automates detection, investigation, and response through SOAR playbooks, reducing mean time to detect and respond from hours to seconds.
(c) Business continuity, backup, disaster recovery & crisis management	Dynamic Threat Modeling (DTM) detects multi-stage ransomware, credential abuse, and lateral movement before business disruption occurs, supporting resilience and minimizing downtime.
(d) Supply-chain security	Behavioral analytics, network detection, and identity monitoring extend visibility to third-party vendors and external connections, continuously detecting anomalous supplier activity and supply-chain risks.
(e) Security in acquisition, development & maintenance of systems	Continuous asset discovery, vulnerability assessment, and configuration monitoring identify new risks introduced by systems, software updates, or third-party components, enabling proactive remediation.
(f) Policies to assess the effectiveness of cybersecurity risk-management measures	Unified dashboards, compliance reporting, and continuous security metrics provide measurable evidence of control effectiveness, helping organizations perform regular reviews required under NIS 2.
(g) Basic cyber hygiene practices & cybersecurity training	User and Entity Behavior Analytics (UEBA) identifies risky user behavior such as password misuse, suspicious access, and policy violations, providing actionable insights to strengthen user awareness and security training.

NIS 2 Obligation	How the aiXDR Platform Delivers It
(h) Policies and procedures regarding the use of cryptography and encryption	Network and endpoint monitoring continuously identifies unencrypted communications, insecure protocols, and encryption policy violations, helping organizations enforce secure communications across the environment.
(i) Human resources security, access control policies & asset management	Identity-centric analytics monitor privileged access, compromised credentials, insider threats, and asset usage while maintaining continuous visibility into managed assets and access rights.
(j) Multi-factor authentication (MFA), continuous authentication & secured communications	Continuous authentication monitoring detects suspicious login attempts, MFA bypass attempts, impossible travel, credential misuse, and abnormal authentication behavior to reinforce identity security controls.
Article 23 – 24-hour, 72-hour & 1-month incident reporting	Automated case management, investigation timelines, audit logs, and exportable incident reports enable organizations and MSSPs to produce regulator-ready documentation within mandatory NIS 2 reporting deadlines.
Article 20 – Governance & management accountability	Executive dashboards and business-level risk reporting provide leadership with continuous visibility into cybersecurity posture, supporting governance responsibilities, oversight, and informed decision-making required under Article 20.

4.3 Built for MSP/MSSP economics, not just enterprise IT

A compliance mapping only matters commercially if a partner can deliver it profitably. Our own partner materials report onboarding of new client tenants in hours to days rather than weeks one published case describes a global MSSP bringing its largest client fully onboard in four days, and prebuilt connectors, playbooks, and auto-tuning that cut onboarding time by up to 70%.

- **Tool consolidation**. We replace 10 to 20-plus siloed point tools with the unified OTM platform, reducing licensing overhead and the engineering effort of maintaining custom integrations between vendors

- **Partner economics**. Partners running their own MSSP on our platform can target 60%-plus margins, or resell managed services with a guaranteed profit share around 25%, alongside pricing that does not vary with data-volume growth a common cost trap in legacy SIEM licensing
- **White-label delivery**. Partners can present the platform under their own brand — branded portals, customized reporting, and partner-set pricing which matters for MSPs/MSSPs that want to sell "their own" NIS 2 readiness service rather than resell under our name
- **Flexible business models**. Our platform supports MDR-as-a-Service, SIEM replacement/enhancement, and SOC-automation models side by side, so a partner can layer a NIS 2 offer onto whichever delivery model it already runs

4.4 Proof points from the field

Our partner materials cite production use across MSSPs and enterprises operating in regulated and multi-country environments. Examples include Exertis' "Fortress" managed security offering built on our platform, Exprivia's cybersecurity unit delivering AI/ML-driven, automated security operations across Europe on our platform, and an MSSP reporting the majority of its banking clients across Africa including some of the region's largest institutions running on our platform. Partners are welcome to request direct reference-customer introductions during due diligence.

4.5 Automating compliance evidence with aiCompliance CMX360

NIS 2 is one entry on a fast-growing list of frameworks European and UK organizations now have to prove compliance against, not the only one. DORA has applied to banks, insurers, and other financial entities since 17 January 2025. Cyber Essentials remains a mandatory prerequisite for many UK central-government contracts involving personal data or technical services. ISO 27001 is increasingly treated as a baseline expectation in enterprise and public-sector procurement. And the cost of falling short is real: European data protection authorities issued approximately €1.2 billion in GDPR fines in 2025 alone.

For most compliance teams, the hard part isn't understanding what a framework requires it's proving it. A single audit can mean pulling documentation and evidence together from a couple dozen disconnected systems, a manual process that leaves many regulated organizations unsure where to even start.

aiCompliance CMX360 is built to remove that manual burden by turning security data an organization already has into compliance evidence, rather than starting evidence-gathering from scratch. Because CMX360 sits directly on top of aiSIEM telemetry that's already being collected, it can reach 60–80% compliance readiness instantly across 20+ global and regional frameworks including NIS 2, DORA, ISO 27001, GDPR, and Cyber Essentials without a separate implementation project.

The workflow runs in three phases:

- **Continuous ingestion.** aiSIEM is already ingesting telemetry from every connected source, 24/7, as part of day-to-day security monitoring not a separate compliance exercise layered on top.
- **Automatic control mapping**. The CMX360 engine maps that telemetry to the specific controls each framework requires — NIS 2, DORA, ISO 27001, Cyber Essentials, and other global and regional frameworks — and keeps that mapping current as requirements change, rather than going stale between audits.
- **Audit-ready reporting**. CMX360 generates reports directly from that mapped evidence, turning what used to be a document-assembly project into a report generated from data the platform already has on hand.

> ***What CMX360 changes***
>
> *Seceon reports that this combination cuts evidence-collection time by 90% and audit-completion time by 75%, and can compress SOC 2 readiness timelines from 6–9 months down to 2–3 weeks. For a partner, that turns compliance from a one-time project into a packaged, recurring service: a Compliance Readiness Assessment CMX360 scans the environment, maps controls, and produces a prioritized executive report that naturally leads into Continuous Compliance Monitoring, where CMX360 keeps validating controls, collecting audit evidence, and producing board-ready reports on an ongoing basis.*

Unlike a security project a client might pause once complete, compliance obligations don't go away NIS 2, DORA, and the frameworks layered alongside them are recurring, annual obligations by design. That makes CMX360-based compliance monitoring a natural fit for the subscription-based, recurring-revenue packaging outlined in Section 5.

5. Packaging NIS 2 Readiness as a Partner Offering

NIS 2 gives MSPs and MSSPs a rare combination: a hard compliance deadline, a large and growing pool of newly in-scope prospects, and a credible reason to reopen dormant accounts. Partners are best positioned to turn this into revenue by moving before the law is promulgated, not after, and by packaging readiness as a defined, sellable service rather than an open-ended consulting engagement.

5.1 A three-tier readiness offer built on one platform

Because the underlying platform is the same across all three tiers, partners can sell a land-and-expand motion starting with a fixed-scope assessment and growing the account into a full managed offering without re-platforming the client at any stage.

Service Tier	What's Included
Tier 1 – Assess	A fixed-scope assessment against ANSSI's ReCyF framework and NIS 2 Article 21 requirements. Powered by aiCompliance CMX360, the assessment automatically maps existing security controls against NIS 2, DORA, ISO 27001, and other applicable frameworks, identifies compliance gaps, and generates a prioritized remediation roadmap. Designed as a fast, low-friction entry point for organizations beginning their compliance journey.

Service Tier	What's Included
Tier 2 – Monitor	Deployment and optimization of aiSIEM and aiXDR tailored to the customer's environment. aiCompliance CMX360 continuously validates security controls, monitors compliance posture, collects audit evidence, and tracks remediation progress, providing a continuous audit trail that demonstrates ongoing compliance with NIS 2 Article 21 requirements.
Tier 3 – Respond & Report	A fully managed MDR/MSSP service combining AI-driven detection, SOAR-automated response, and end-to-end incident management. The service supports the complete NIS 2 incident reporting lifecycle (24-hour early warning, 72-hour notification, and one-month final report) while aiCompliance CMX360 generates executive and board-ready compliance reports that support Article 20 governance and management oversight.

5.2 A practical sequence for partner-led outreach

- **Lead with the gap assessment**. Offer a scoped review against ANSSI's ReCyF and the Article 21 security objectives this is where ANSSI itself is telling organizations to start.
- **Make the assessment itself the demo**. A CMX360-powered scan produces a mapped, prioritized findings report directly from the prospect's existing security data a concrete deliverable that does more to close a Tier 1 engagement than a slide deck.
- **Position our platform as the control layer, not another tool**. The value proposition is consolidation: one platform replacing the SIEM, XDR, SOAR, and UEBA point solutions clients would otherwise have to stitch together and separately justify to auditors.
- **Sell the reporting clock, not just detection**. The 24/72-hour/one-month cadence is concrete and easy for a prospect to grasp frame our automated case timelines as the mechanism that keeps them inside it.
- **Address the board, not just the SOC**. Article 20's personal accountability provision is a natural hook for a briefing with the client's leadership team, not only its IT function.

- **Prove it on your own house first**. Because MSPs/MSSPs are themselves in scope, a partner that can show its own NIS 2-aligned controls, running on our platform, has a credibility advantage that generic vendors cannot match.
- **Lead with speed to value**. Onboarding measured in days rather than months means a partner can close a Tier 1 assessment and have Tier 2 monitoring live inside the same sales cycle, rather than losing momentum to a lengthy implementation phase.

> **Cross-border angle**
>
> *Because France's timeline sits alongside Ireland, Luxembourg, the Netherlands, and Spain all still finalizing their own transpositions and the UK's separate Cyber Security and Resilience Bill, partners serving multi-country clients can position our platform as the one platform that keeps pace with whichever jurisdiction's law lands first, without re-architecting security operations each time.*

6. Frequently Asked Questions for Partners

The Loi Résilience isn't promulgated yet isn't it too early to sell against it?"

No. ANSSI's own public guidance is to begin risk assessments, system mapping, and ReCyF alignment now, since the bulk of NIS 2's substance is fixed at EU level and unlikely to change materially in the final French text. Waiting for promulgation just compresses the client's runway before enforcement begins a genuine urgency argument, not a manufactured one.

"Our client already has a SIEM. Do they need to rip it out?"

Not necessarily but it is worth surfacing what that SIEM cannot do alone. Traditional, rule-based SIEM tools were not built for the cross-domain correlation, automated response, or multi-tenant reporting that NIS 2 compliance increasingly assumes. Position us as the layer that closes those gaps, whether that means augmenting or replacing the incumbent tool the conversation should follow the client's constraints, not a fixed script.

"Is our MSP/MSSP itself really in scope, or just our clients?"

Both, in most cases. NIS 2's Annex I explicitly names ICT service management (B2B) managed service providers and managed security service providers as an in-scope sector. Even a partner whose clients are outside regulated sectors should assume its own operations may be directly regulated once France's national thresholds are finalized.

"How fast can we actually get a client live?"

Our published partner accounts describe onboarding measured in hours to days rather than weeks, including a case where a global MSSP's largest client was fully onboarded in four days. Actual timelines will vary by environment complexity and data-source count partners should validate expected timelines for their specific client base with us directly during scoping.

"What if France's final law changes some of these requirements?"

Some technical detail may shift between now and final promulgation and implementing decrees. The core structure Article 21 risk-management measures, Article 23's reporting clock, and Article 20 governance accountability comes from the EU directive itself and is not something France can materially soften in its national transposition. A platform-based approach aligned to the directive's substance is a safer foundation than waiting for every French-specific detail to be finalized.

7. Next Steps

France's NIS 2 transposition will keep moving through 2026 regardless of exactly which month the Loi Résilience is promulgated. The underlying obligations risk-based controls, fast incident reporting, board-level accountability, and supply-chain oversight are already the standard the market is being held to. Partners who help clients meet that standard now, using a platform purpose-built for multi-tenant delivery, will be the ones positioned to win the accounts that move first.

France & NIS 2:
Turning a Regulatory Deadline into a Growth Opportunity

The Scale of the Opportunity

15,000+
Additional entities in scope in France under Loi Résilience

€10M
Max fine for essential entities or 2% of global turnover

24 hrs
Window for early warning to ANSSI after a significant incident

Where France Stands

Oct 2024
Bill introduced

Mar 2025
Senate approved

Mar 2026
ANSSI publishes ReCyF

2026
Final adoption pending

Post-law
Enforcement begins

The problem

Reporting is too slow
Manual processes miss the 24h deadline

Audit prep takes months
Evidence scattered across siloed tools

MSPs are in scope too
Not just clients you're regulated

Boards face liability
Directors need risk visibility, not logs

NIS 2 requires

10 security controls
Risk, access, MFA, supply-chain

24h · 72h · 1 month
Tiered incident reporting to ANSSI

Board accountability
Leadership must approve and oversee

Supplier monitoring
Assess every vendor, continuously

Seceon solves it

Auto-generated reports
SOAR files ANSSI reports instantly

90% less audit effort
CMX360 maps controls automatically

Full-stack visibility
Endpoints, network, cloud, identity

Board-ready dashboards
Plain-language risk for leadership

90%
Evidence-collection time reduction

75%
Audit-completion time reduction

60-80%
Instant compliance readiness across 20+ frameworks

60%
Target MSSP margin on platform delivery

To discuss co-marketing this white paper, request a partner briefing deck, or scope a joint NIS 2 readiness offer for your client base, contact your Seceon partner representative or visit seceon.com.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

References and Citations:

This whitepaper is based on research and data from:

- European Commission. "NIS2 Directive implementation in France." Shaping Europe's Digital Future. digital-strategy.ec.europa.eu.
- Reglyze. "NIS2 France — Transposition, Fines & Compliance Guide 2026." reglyze.com.
- Seceon. "How an MSSP Transformed Scaled Global Security Operations with Seceon." info.seceon.com.
- Seceon. "MSSP Security Platform | AI-Powered Cybersecurity for Managed Security Providers." seceon.com.
- Seceon. "Seceon aiCompliance CMX360: Instant, Security-Driven Compliance." seceon.com/aicompliance-cmx360/.
- Seceon. seceon.com (home page — partner testimonials and platform metrics).

References and Citations:

- SentinelOne. "What Is NIS2? EU Cybersecurity Directive Explained." sentinelone.com. May 2026.
- SPAC Alliance. "NIS2 Transposition in France – Where Things Stand." spac-alliance.org. January 2026.
- Viktoria Compliance. "NIS2 Transposition in 2026: Where Every EU Member State Stands (and What It Means for Cross-Border Business)." viktoria-compliance.eu. April 2026.
- Wavestone. "NIS 2 directive: transposition status and what companies must do." wavestone.com. Updated January 1, 2026.

About the Author

Shikha Pandey

Principal, Product Strategy & Partnerships, Seceon Inc.

Shikha leads Product Strategy, Global Marketing, and Partnerships at Seceon, where she drives go-to-market strategy, brand growth, channel expansion, and strategic partnerships. Before joining Seceon, she was a Senior Technical Program Manager at Meta, leading backend infrastructure programs supporting Facebook, WhatsApp, and Instagram, with a focus on automation, advanced tooling, and GenAI to improve engineering productivity.