padanet

AI & Cybersecurity

STRUCTURED TRANSFORMATION PROGRAM

PHASE I	PHASE II	PHASE III
Clarity	Structure	Continuous Deployment
2 days	2 weeks	2 months
Structured executive alignment on AI security posture and regulatory obligations	Evidence-driven assessment of security posture, compliance gaps, and remediation	Full governance, compliance architecture, and deployment-backed transformation

Phase I — Clarity

A concentrated structural intervention that equips leadership with a clear understanding of the cybersecurity landscape as it relates to AI adoption, European regulatory obligations, and the risks of deploying agentic AI systems in enterprise environments.

> **Structured executive alignment sessions.**
> C-suite, CTO/CIO/CISO, transformation leads, IT directors.

THE LANDSCAPE

- **Regulatory environment** — EU AI Act, NIS2, DORA, GDPR: obligations, timelines, and enforcement reality
- **French & international standards** — ANSSI, CNIL, ISO 27001/42001, NIST AI RMF, OWASP Top 10 for LLMs, MITRE ATLAS
- **AI-specific vulnerabilities** — Prompt injection, data poisoning, model extraction, supply chain attacks
- **Agentic AI risks** — Uncontrolled tool use, memory poisoning, goal drift, excessive autonomy
- **Enterprise deployment risks** — Shadow AI, data leakage, IP contamination, vendor lock-in

FROM RISK TO ARCHITECTURE

- **The deployment gap** — Why 87% of enterprise AI pilots never reach production
- **Structural prerequisites** — Data sovereignty, identity management, auditability, governance, trust
- **The trust paradox** — Employees distrust company AI but freely use external AI
- **Padanet trust architecture** — Realm separation, agent boundaries, memory sovereignty, consent-first design
- **Capability mapping** — Effort/impact matrix, structural priorities, deployment roadmap

Approach & Deliverables

Focused diagnostic and applied structural analysis. Each session combines evidence-driven assessment with structured application: risk classification, tabletop scenarios, compliance gap identification, and capability mapping.

DELIVERABLES

EXECUTIVE BRIEFING
Regulatory landscape, risk assessment, and positioning

RISK MATRIX
Organization-specific risk classification with severity and likelihood

PRIORITY ROADMAP
Ranked structural priorities with effort/impact assessment

COMPLIANCE GAP SUMMARY
Current posture vs. EU AI Act, NIS2, GDPR obligations

KEY TOPICS COVERED

EU AI ACT · NIS2 · DORA · GDPR · ANSSI · CNIL · ISO 27001 · ISO 42001 · OWASP LLM · MITRE ATLAS · NIST AI RMF

Progression

PHASE II — STRUCTURE
Full risk register, compliance gap analysis, and remediation architecture over two weeks.

PADANET DEPLOYMENT
Deploy Padanet's trust architecture in a controlled scope to validate structural guarantees.

Phase I: 2 days. Includes preparation, delivery, and deliverables.

Powered by Padanet

Every engagement is anchored in Padanet — a continuous skills intelligence system that sustains visibility beyond intervention.

FOR INDIVIDUALS

- Real-time visibility into skills evolution
- Contextual guidance grounded in actual work
- Full control over what is shared

FOR ORGANIZATIONS

- Living view of real capabilities, not inferred roles
- Anti-surveillance guarantees by design
- Sovereign deployment: cloud, hybrid, or on-premise

Your Cybersecurity Expert

Senior Cybersecurity & AI Transformation Specialist

Seasoned cybersecurity and AI transformation expert with 20+ years of experience in enterprise security architecture, risk management, and digital transformation. Deep technical expertise combined with deployment-backed leadership at the intersection of AI adoption and security governance.

padanet.com

Let's talk.