

Finance - Banque & Assurance

Journée d'immersion - Résilience cyber & conformité

Une journée destinée à des profils déjà expérimentés : construire des outils opérationnels directement réutilisables, sans reprendre les fondamentaux.



NOVAMIND

CADRE DE LA JOURNÉE

Une journée immersive, concrète et opérationnelle

Public cible

- RSSI, DSI confirmés et responsables infrastructure souhaitant se spécialiser, issus de la finance, de la banque et de l'assurance.
- TPE / PME du secteur.

Prérequis

- Avoir cartographié l'existant de son entreprise.
- Recenser tous les actifs TIC et les processus critiques.
- Hiérarchiser les vulnérabilités de l'entreprise.

Objectifs

- Construire une feuille de route de conformité croisant DORA et NIS2 sans dupliquer audits et preuves.
- Maîtriser les exigences DSP2 et PCI-DSS propres aux paiements et infrastructures de marché.
- Identifier les vulnérabilités des systèmes d'IA en finance et évaluer un outil d'IA défensive.
- Vivre une simulation de crise complète sous contrainte DORA, prioriser les décisions et repartir avec un plan d'action concret.

Format pédagogique

Apports théoriques

Sous-groupes

Simulation de crise

DURÉE

1 journée d'immersion

EFFECTIF

Jusqu'à 30 personnes

LIEU

Centre Novamind, Paris 03

FORMAT

Présentiel

TARIF

Sur mesure

FINANCEMENT

OPCO possible

DATES

Nous consulter pour les dates de formation

Le rythme de la journée

- **8h** Accueil
- **8h30** Plénière
- **9h30** DORA / NIS2
- **11h** Cyber & IA
- **12h15** Déjeuner
- **14h15** Crise Supply Chain
- **17h** Retex
- **18h45** Retex éditeur
- **19h15** Cocktail

Déroulé de la journée

8h00 - 12h15 | MATIN - RÉGLEMENTATION, RÉSILIENCE & IA

8h00 - 8h30 Accueil

Petit-déjeuner d'accueil : viennoiseries, fruits frais, café et thé.

8h30 - 10h45 | Plénière & feuille de route DORA / NIS2

- Panorama des menaces et obligations du secteur financier : DORA, NIS2 et consolidation du marché de la cybersécurité.
- Présentation des cinq piliers de DORA : gouvernance, risques TIC, incidents, tests de résilience et risques tiers.
- Articulation avec NIS2 pour éviter la duplication des preuves ; cas d'une banque de taille intermédiaire et construction d'un registre des prestataires TIC critiques.
- Tests de résilience opérationnelle numérique (TLPT) pour les entités identifiées comme critiques.
- Notification d'incident majeur en trois jalons : rapport initial, intermédiaire et final.
- Clauses contractuelles renforcées : droit d'audit, réversibilité et localisation des données.

10h45 - 11h00 Pause

Transition vers le module cybersécurité et intelligence artificielle.

11h00 - 12h15 | Cybersécurité & intelligence artificielle

- Démonstration live d'une attaque par injection de prompt sur un agent IA fictif.
- Travail sur les risques du OWASP Top 10 LLM et le repérage du Shadow AI en entreprise.
- Utilisation d'une grille structurée pour challenger un outil d'IA défensive présenté dans une fiche produit volontairement orientée commercialement.
- Cinq risques majeurs : injection de prompt, fuite de données d'entraînement, empoisonnement de modèle, sur-permission des agents et dépendance fournisseur.

12h15 - 14h00 Déjeuner business

Servi à table dans l'espace privatisé, pour favoriser les échanges entre pairs.

14h15 - 18h00 | APRÈS-MIDI - SIMULATION DE CRISE SUPPLY CHAIN

14h15 - 17h00 | Défaillance d'un prestataire Cloud critique

- Contexte : le prestataire Cloud gérant la double authentification et les signatures électroniques subit une panne mondiale après une mise à jour corrompue ; les serveurs de la banque fonctionnent mais clients et conseillers ne peuvent plus valider les opérations.
- Phase 1 : les clients ne reçoivent plus les notifications PUSH / SMS ; identifier que le problème n'est pas interne, activer la cellule de crise et contacter le prestataire SaaS.
- Phase 2 : dysfonctionnement confirmé et échec des transactions e-commerce ; activer le PCA prestataire Cloud, évaluer les solutions techniques et gérer la pression du COMEX et de la presse.
- Phase 3 : dépassement du temps de coupure toléré ; le régulateur demande l'évaluation DORA du prestataire et une déclaration d'incident majeur sur la chaîne d'approvisionnement ; rédiger le rapport DORA axé sur le risque tiers.
- Phase 4 : restauration annoncée ; préparer le PRA, exiger une preuve d'intégrité, reconnecter progressivement les clients, rejouer les transactions échouées et communiquer sur la fin de la cellule de crise.

17h00 - 18h00 | Retour d'expérience

- Temps de parole pour les participants et partage d'expérience sur l'exercice de simulation de crise.

CLÔTURE

18h45

Retex éditeur

19h15

Soirée cocktail de clôture

Livrables remis aux participants

- Feuille de route DORA et NIS2 construite par les participants selon leur entreprise respective.
- Pistes de certification associées : EBIOS Risk Manager ; ISO 27001 Lead Implementer / Lead Auditor.