Cybersécurité & Résilience Numérique

Protéger, décider et rebondir à l'ère des cybermenaces

Formation intensive format hybride

INFOS PRATIQUES

Durée totale : 7h30 nettes (6h présentiel + 1h30 visio à J+15)
Format : Présentiel intensif + visio collective à J+15
Participants : 12 participants maximum
Public : Dirigeants et décideurs dont l'organisation repose sur des SI, données clients ou actifs numériques
Prérequis : Exercer une fonction de direction ou de décision. Aucun prérequis technique.
Inscription : En ligne sur www.leadia.paris ou sur RDV avec un représentant LeadIA
Délai d'accès : 10 jours ouvrés
Tarif : 2 300 € HT par participant (tout inclus)
Financement : OPCO, plan de développement des compétences, FNE-Formation — dossier à prévoir 10 jours avant

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le participant est capable de :

- Identifier les principales cybermenaces et comprendre leur mode opératoire pour mieux les anticiper
- Évaluer l'exposition cyber de son organisation et cartographier ses actifs numériques critiques
- Connaître ses obligations juridiques en tant que dirigeant : RGPD, NIS2, DORA, responsabilité personnelle
- Sélectionner et prioriser les outils et précautions adaptés à son niveau de maturité et son profil de risque
- Construire une culture cyber dans son organisation et préparer une réponse à incident structurée
- Élaborer une feuille de route cyber personnalisée avec des actions concrètes à horizon 30 et 90 jours

PROGRAMME DÉTAILLÉ

Session présentielle — 6h (09h00 – 16h30 avec pauses – horaires après-midi possibles)

09h00 — **Accueil & Cadrage — 20 min**
Kit participant, émargement, quiz d'évaluation initiale (Mentimeter), tour de table — enjeu cyber réel de chaque participant

09h20 — **BLOC 1 — Panorama des menaces — 1h30**
Rançongiciel, phishing, supply chain, espionnage industriel, IA offensive — anatomie d'une attaque en 4 phases — ce que ça coûte réellement (jusqu'à 466 000 €, 60 % de fermetures) — secteurs les plus exposés

10h50 — **BLOC 2 — Responsabilité juridique du dirigeant — 1h (dont 40 min juriste en visio)**
RGPD, NIS2, DORA, AI Act — jurisprudence récente — délégation de responsabilité — assureurs cyber — contractualisation prestataires SI — Q&A ouvert avec le juriste

11h50 — **BLOC 3 — Outils et précautions : la grille du dirigeant — 1h15**
Grille à 3 niveaux — Obligatoires (MFA, sauvegardes 3-2-1, PCA, notification CNIL 72h) — Nécessaires (inventaire actifs, EDR, segmentation réseau) — Souhaitables (audit PASSI, SOC, assurance cyber)

13h05 **Pause déjeuner — 15 min**

13h20 **BLOC 4 — Résilience & culture cyber + Simulation de crise rançongiciel — 1h45**
Les 3 piliers de la résilience — rôle du dirigeant — communication de crise (CNIL, clients, médias) — Simulation : chaque groupe joue le CODIR en cellule de crise, décisions en temps contraint, débriefing collectif

15h05 **BLOC 5 — Feuille de route personnelle — 30 min**
3 priorités à 30 jours par participant : action concrète, ressource nécessaire, indicateur de réalisation — partage en grand groupe — engagement public

15h35 **Clôture — 20 min**
Quiz de sortie (15 questions Mentimeter) — auto-évaluation avant/après — questionnaire satisfaction à chaud — attestations remises nominativement — pack ressources (Grille Outils Cyber, modèle PCA, contacts CERT-FR/ANSSI)

Questionnaire satisfaction à chaud, tour de table des engagements, remise des attestations de suivi et d'acquisition de compétences

Module Visio — J+15 — 1h30 (inclus dans le tarif)
Tour de table (avancement des 3 priorités, blocages rencontrés) — approfondissement collectif — point juriste optionnel — réengagement concret. Même groupe que la session présentielle.

ÉVALUATION DES ACQUIS

- Quiz d'évaluation initiale (10 questions — Mentimeter)
- Vérification orale à chaque fin de bloc (3 questions)
- Quiz de sortie (15 questions — résultats en temps réel)
- Auto-évaluation avant/après sur les 6 objectifs pédagogiques (notation 1 à 5)
- Questionnaire de satisfaction à chaud (clôture) et à froid (J+30)

Deux attestations remises nominativement à la clôture : attestation de suivi de formation (art. L.6353-1 C. trav.) et attestation d'acquisition de compétences.

MODALITÉS PÉDAGOGIQUES

- Apports théoriques structurés (5 blocs + atelier simulation)
- Simulation de crise rançongiciel — sous-groupes, décisions en temps contraint, débriefing
- Supports remis à chaque participant (Grille Outils Cyber A3, modèle PCA, glossaire 40 termes, contacts CERT-FR/ANSSI)
- Intervention d'un juriste spécialisé cybersécurité en visio (Bloc 2, 40 min)
- Session visio collective J+15 incluse (90 min)
- Groupe de 12 participants maximum
- Accompagnement individuel supplémentaire disponible en option payante

Organisme de formation : LeadIA SAS — www.leadia.paris — contact@leadia.paris — 06 19 16 13 45
Direction pédagogique : Denis Ktorza
NDA : En cours d'enregistrement auprès de la DREETS Île-de-France | Référentiel Qualiopi : indicateurs tracés au programme source
Accessibilité handicap : Référente Isabelle Sfez — isabelle@leadia.paris — 06 19 16 13 45 — Toute situation signalée fait l'objet d'une analyse individualisée.