



ARIÈS ARF

ACCOMPAGNEMENT • RECRUTEMENT • FORMATION

FORMATION SUR MESURE • POUR LES PROFESSIONNELS • INTELLIGENCE ARTIFICIELLE

L'IA et la cybersécurité

Protéger votre entreprise des nouvelles menaces, et utiliser l'IA pour vous défendre.

13

modules

3

e-learning, visioconférence, présentiel

LA FORMATION EN BREF

Ce que vous allez apprendre

Une formation construite pour vous : on part de votre niveau, de vos usages et de vos propres fichiers, pour que chaque heure serve directement votre travail.

En visio ou en présentiel dans vos locaux, en individuel ou pour une équipe, en une ou plusieurs séances. Le programme ci-dessous sert de base : on garde ce qui vous est utile et on approfondit vos cas concrets.

Pour qui

Dirigeants, managers et salariés de TPE/PME.

Prérequis

Aucun prérequis. Un ordinateur avec une connexion internet.

Modalités

E-learning · Visioconférence · Présentiel (présentiel : frais de déplacement en plus)

Le programme

PARTIE 1

Démarrage rapide : Starter Pack cyber (toute entreprise)

- But : démarrer en 48 h ; identifier ce qui compte ; fixer 5 règles non négociables ; livrable final : plan d'actions 30 jours.

Votre surface d'attaque en 10 minutes (inventaire minimal) · Les 5 règles non négociables (cyber-hygiène) · Prioriser avec une matrice Impact/Probabilité · Mettre un responsable (même à temps partiel) et un canal d'alerte · Le tableau de bord cyber du dirigeant (5 indicateurs)

MODULE 1

Menaces 2026 : comprendre pour agir

- But : reconnaître les attaques les plus probables ; savoir quoi vérifier ; livrable : 1 fiche réflexe par menace.

Phishing : les 7 signaux qui ne mentent pas · Rançongiciel : ce qui se passe vraiment (et pourquoi ça bloque tout) · Piratage de compte : password spray, vol de session, réutilisation · Fraude au virement : changement de RIB et fraude au président · Supply chain : l'attaque qui passe par le prestataire · DDoS et indisponibilité : protéger l'activité en ligne

MODULE 2

Comptes, mots de passe, MFA, passkeys : sécuriser l'accès

- But : rendre les comptes difficiles à voler ; livrable : politique d'authentification simple + plan de déploiement.

Passephrase : créer des mots de passe vraiment robustes · Gestionnaire de mots de passe : choisir et déployer sans conflit · MFA partout : la checklist 1 heure · Passkeys : réduire le phishing (sans casser l'existant) · Comptes administrateurs : limiter le blast radius · Fin de contrat : couper les accès (le vrai risque oublié)

MODULE 3

Ingénierie sociale 2026 : phishing, smishing, deepfakes, AiTM

- But : rendre les équipes anti-manipulation ; livrable : protocole de vérification + kit d'entraînement.

La méthode Stop, Vérifie, Confirme (en 60 secondes) · Smishing et QR codes : le piège du téléphone · Deepfakes voix/vidéo : quand le boss appelle · Attaques AiTM (vol de session) : pourquoi le MFA ne suffit pas toujours · Réseaux sociaux : collecte d'informations et usurpation · Entraîner sans lasser : micro-drills (5 min/semaine)

MODULE 4

Postes, serveurs, mises à jour : l'hygiène technique qui évite les drames

- But : réduire l'exploitation de failles ; livrable : plan patching + durcissement minimal.

Patching : la méthode Critique sous 7 jours · Antivirus/EDR : indispensable vs marketing · Chiffrement disque et verrouillage : protéger en cas de vol · USB et périphériques : réduire l'entrée facile · Sauvegarder la config : la base avant tout changement · Journalisation minimale : garder des preuves utiles

MODULE 5

Télétravail, Wi-Fi, visioconférence : sécuriser le quotidien

- But : éviter les fuites par usage ; livrable : charte télétravail + checklist mobilité.

Wi-Fi public : 10 règles simples (sans paranoïa) · Box et routeur : durcissement minimal à la maison · Visioconférence : empêcher l'intrus (et les fuites) · Partage de fichiers en mobilité : lien, droits, expiration · BYOD : règles simples si on n'a pas le choix · Sécurité physique : shoulder surfing et vol d'appareil

MODULE 6

Sauvegardes, restauration, ransomware : construire la résilience

- But : pouvoir restaurer ; livrable : stratégie 3-2-1-1-0 + test de restauration planifié.

3-2-1-1-0 : la règle moderne expliquée simplement · Quoi sauvegarder : données, SaaS, configurations, clés · Chiffrer et protéger les sauvegardes · Tester la restauration (sinon ça ne compte pas) · Ransomware : la checklist des 15 actions préventives · Après attaque : reconstruire proprement (sans réinfecter)

MODULE 7

Données et RGPD : sécuriser, prouver, réagir en 72 h

- But : réduire le risque juridique ; livrable : registre violations + procédure 72 h + décision CNIL.

Classer l'information (4 niveaux) · Minimisation et accès : qui a vraiment besoin de quoi · AIPD : quand c'est obligatoire (et comment faire simple) · Violation de données : décider notification CNIL ou pas · Procédure 72 h : qui fait quoi, quand, avec quels éléments · Pour aller plus loin : sécuriser un formulaire web (erreurs classiques)

MODULE 8

Cloud & SaaS : sécuriser les réglages (messagerie, partage, invités)

- But : fermer les fuites de configuration ; livrable : baseline SaaS + revue mensuelle.

Sécuriser la messagerie : les 8 réglages critiques · Partage de documents : liens, invités, droits, expiration · Comptes externes et prestataires : accès temporaires · Sauvegarder le SaaS : éviter on pensait que c'était inclus · Détection : alertes simples à activer (sans SOC) · Pour aller plus loin : réduire le shadow IT

MODULE 9

Réseau, VPN, segmentation, IoT : éviter la propagation

- But : limiter la casse ; livrable : schéma réseau simplifié + plan de segmentation.

Schéma réseau pour non-techniciens (à faire valider) · VPN : quand c'est utile, quand c'est une fausse sécurité · Segmentation : tout n'a pas le droit de parler à tout · IoT (imprimantes, caméras, badges) : sécuriser sans y passer des jours · Accès Internet : filtrer sans bloquer le business · Pour aller plus loin : Wi-Fi invité en entreprise

MODULE 10

Prestataires & chaîne d'approvisionnement : sécuriser l'écosystème

- But : réduire le risque indirect ; livrable : pack contrat + questionnaire + revue annuelle.

Le questionnaire prestataire 1 page qui marche · Clauses cyber dans un contrat (version light) · Accès prestataire : règles de base (temporaire, tracé, MFA) · Audit simple : demander des preuves sans être expert · Cas réel : compromission via prestataire (leçon actionnable) · Pour aller plus loin : continuité et réversibilité fournisseur

MODULE 11

Réagir à un incident : 0-72 h, preuves, communication, reprise

- But : agir sans paniquer ; livrable : playbook incident + kit communication.

Détection : les signaux qui doivent déclencher une alerte · Containment : isoler sans tout casser · Qui appeler : prestataire, assurance, autorités, banque · Communication : interne, clients, partenaires (sans sur-promesse) · Reprise d'activité : progressive et surveillée · La leçon qui change tout : ne pas payer par réflexe

MODULE 12

Gouvernance & culture : rendre la cybersécurité durable

- But : tenir dans le temps ; livrable : programme annuel + responsabilités + conformité utile.

Programme annuel de sensibilisation (sans fatigue) · Politique et charte informatique : 2 pages utiles · Reporting dirigeant : ROSI, risques, décisions · NIS2 : qui est concerné et que préparer dès maintenant · DORA (finance) : exigences de résilience numérique (si concerné) · IA & cybersécurité : deepfakes, phishing industrialisé, garde-fous

Méthodes et évaluation

Moyens pédagogiques

Précisés lors de l'inscription.

Évaluation

Précisée lors de l'inscription.

Attestation de fin de formation remise à l'issue du parcours.

Comment se déroule votre formation

- 1 Le diagnostic · 150 €, payé à la réservation**
Une heure en visio avec la formatrice : vos objectifs, votre niveau et celui de vos équipes, vos outils et vos cas concrets. Son prix est déduit du devis si vous poursuivez.
- 2 Votre plan de formation et le devis**
Sous 48 heures après le diagnostic, un programme construit pour vous à partir de ce programme de référence.
- 3 La formation**
En visio, ou en présentiel dans vos locaux (les frais de déplacement s'ajoutent alors au devis). En individuel ou en groupe, sur vos propres fichiers. Convention, programme et attestations fournis.

Formations sur mesure réservées aux professionnels : entreprises, indépendants, associations.

Votre formatrice



Cassandra Pannetier, fondatrice d'Ariès ARF, formatrice professionnelle d'adultes diplômée (titre professionnel FPA), Bachelor RH, DUT GEA. Quinze ans de terrain en gestion, ressources humaines et recrutement, au service des dirigeants et des équipes de TPE et PME.

contact@ariesarf.com · 06 87 64 50 96 · ariesarf.com
<https://formation.ariesarf.com/formation/lia-et-la-cybersecurite/>

Ariès ARF · Entreprise individuelle (micro-entreprise) · SIRET 907 931 034 00017 · TVA non applicable, art. 293 B du CGI. Document à jour au 23 octobre 2026.