AKADEMIA
FORMATION

PROGRAMME DE FORMATION
RÉF. N17

INTELLIGENCE ARTIFICIELLE | NIVEAU INTERMÉDIAIRE

Cybersécurité à l'ère de l'IA : *phishing et deepfakes.*

Deux jours pour transformer la menace en plan de défense. Hameçonnage hyper-personnalisé, voix clonées, visioconférences truquées, fraude au faux dirigeant : vous décortiquez des cas réels sourcés, cartographiez l'exposition de votre structure, rédigez vos procédures anti-fraude — double validation des virements, contre-appel systématique — et les éprouvez en simulation ; puis vous cadrez les usages de l'IA de votre équipe et repartez avec votre charte, un exercice de sensibilisation prêt à rejouer en interne et votre plan de défense consolidé.

DURÉE	FORMAT	PUBLIC	CERTIFICATION
2 jours 14 heures	**Inter · Intra** Présentiel ou distanciel	**Dirigeants, managers & équipes**	**Attestation**

À PROPOS DE LA FORMATION

Cybersécurité à l'ère de l'IA : phishing avancé, deepfakes et protection des données.

Deux jours pour transformer la menace en plan de défense. Hameçonnage hyper-personnalisé, voix clonées, visioconférences truquées, fraude au faux dirigeant : vous décortiquez des cas réels sourcés, cartographiez l'exposition de votre structure, rédigez vos procédures anti-fraude — double validation des virements, contre-appel systématique — et les éprouvez en simulation ; puis vous cadrez les usages de l'IA de votre équipe et repartez avec votre charte, un exercice de sensibilisation prêt à rejouer en interne et votre plan de défense consolidé.

DURÉE	FORMAT	NIVEAU	PÉDAGOGIE	CERTIFICATION
2 jours	**Inter · Intra**	**Intermédiaire**	**Active**	**Attestation**
14 heures	Présentiel ou distanciel		Petits groupes	Attestation délivrée

Objectifs pédagogiques

- Cartographier l'exposition de sa structure aux fraudes facilitées par l'IA — personnes susceptibles d'être usurpées (voix et image publiques, signataires), fonctions ciblées, flux financiers sensibles (virements, changements de RIB, paie), informations publiques exploitables — et hiérarchiser les trois scénarios de risque les plus plausibles pour son organisation.
- Analyser la mécanique des attaques amplifiées par l'IA — hameçonnage hyper-personnalisé, deepfakes audio et vidéo (fraude au faux dirigeant, faux ordres de virement, usurpation en visio-conférence) — à partir de cas réels documentés et de chiffres officiels datés, et qualifier une sollicitation suspecte à ses trois constantes : pression d'urgence, autorité usurpée, canal unique.
- Rédiger les procédures anti-fraude de sa structure, conformes aux recommandations officielles (fiche « faux ordres de virement » de Cybermalveillance.gouv.fr) : double validation des virements avec rôles séparés et seuils, contre-appel systématique sur un numéro déjà connu, vérification des changements de RIB, code de vérification interne et validation hiérarchique non dérogeable — y compris face à une demande « urgente et confidentielle » de la direction.
- Éprouver ses procédures en simulation — jeux de rôle scriptés, sans aucun outil offensif — puis les amender à partir des failles constatées, en consignant le compte rendu du test : ce qui a tenu, ce qui a cassé, les corrections apportées.
- Dérouler la conduite à tenir en cas de fraude avérée, dans l'ordre et sans délai : identifier l'ensemble des virements exécutés et en instance, alerter sa banque et demander le retour des fonds, préserver les preuves, déposer plainte et signaler — à l'aide d'une fiche réflexe personnalisée aux contacts de sa structure.
- Cadrer les usages de l'IA de son équipe en rédigeant une charte d'usage sûre — outils validés, catégories de données autorisées et interdites, comptes professionnels, signalement sans blâme du « shadow AI » — articulée avec le RGPD et les recommandations de la CNIL, et au regard des exigences de littératie IA prévues par l'AI Act (Règlement (UE) 2024/1689, art. 4, applicable depuis le 2 février 2025 ; cf. module 4).
- Concevoir un exercice de sensibilisation interne prêt à rejouer avec son équipe — scénario adapté à sa cartographie, déroulé minuté, quiz et débrief capacitant — et consolider son plan de défense d'ensemble avec un calendrier de mise en œuvre.

Public visé

Dirigeants de TPE, PME et ETI, managers et responsables d'équipe, et fonctions exposées aux flux financiers et aux demandes sensibles : direction administrative et financière, comptabilité et trésorerie, assistanat de direction, office managers, ressources humaines et services achats. La formation s'adresse aussi aux référents internes (qualité, informatique de proximité) chargés de déployer les procédures anti-fraude et de sensibiliser les équipes. Elle est conçue pour un public non technique : le niveau visé est organisationnel et humain — aucune compétence en sécurité informatique n'est requise au-delà des fondamentaux.

Prérequis

Prérequis conseillé : avoir suivi la formation « Cybersécurité et hygiène numérique : les fondamentaux au quotidien » (N16) ou maîtriser des réflexes équivalents — mots de passe robustes avec gestionnaire, double authentification, repérage d'un hameçonnage courant, vérification par un canal indépendant. Ces fondamentaux font l'objet d'un rappel express en ouverture ; ils ne sont pas ré-enseignés. Usage courant d'un ordinateur et d'une messagerie ; aucune pratique de l'IA n'est exigée. Chaque participant apporte un ordinateur portable et sa connaissance des circuits de paiement de sa structure (qui demande, qui valide, qui exécute) : le plan de défense est construit sur SA structure réelle. Une fiche de préparation transmise en amont invite à réunir — sans transmettre aucun document confidentiel — le schéma actuel de validation des virements et des changements de RIB, la liste des fonctions habilitées, les usages d'assistants IA constatés ou supposés dans l'équipe, ainsi que les contacts utiles en cas de fraude : numéro direct du conseiller bancaire, numéro d'urgence ou d'opposition de la banque, contact de l'assurance si un contrat couvre la fraude ou le risque cyber.

PROGRAMME DÉTAILLÉ

Quatre modules progressifs pour monter en compétences.

JOUR 1

Jour 1 — Comprendre la menace, verrouiller sa structure

Des attaques amplifiées par l'IA — cas réels et chiffres officiels à l'appui — à la cartographie de son exposition et aux procédures anti-fraude rédigées.

MODULE

01.

3H30

Ce que l'IA change à la menace : hameçonnage hyper-personnalisé, deepfakes et cartographie de son exposition

OBJECTIF OPÉRATIONNEL

« Analyser la mécanique des attaques amplifiées par l'IA sur des cas réels documentés, puis cartographier l'exposition de SA structure — personnes usurpables, flux financiers, informations publiques — et hiérarchiser ses trois scénarios de risque. »

CONTENU PÉDAGOGIQUE

- L'état de la menace, en position d'équilibre officielle : à ce jour, l'ANSSI n'a pas connaissance de cyberattaque menée contre des acteurs français à l'aide de l'IA, ni de système d'IA capable de conduire seul une attaque de bout en bout — mais l'usage de l'IA par les attaquants pour amplifier leurs opérations est jugé plausible et déjà observé (CERT-FR, synthèse du 4 février 2026) ; dans son Panorama de la cybermenace 2025 (mars 2026), l'ANSSI observe l'usage de capacités d'IA chez l'ensemble des profils d'attaquants, améliorant le niveau, la quantité, la diversité et l'efficacité des attaques. Ni déni, ni panique : la réponse est d'abord organisationnelle — c'est l'objet de ces deux jours.
- L'hameçonnage hyper-personnalisé : ce que l'IA générative change concrètement — des messages sans fautes, adaptés au contexte et à la cible à partir de ses informations publiques, déclinés en dizaines de langues et produits en volume ; l'honnêteté officielle en contrepoint : les campagnes de masse entièrement pilotées par IA ne sont pas attestées à ce stade (Cybermalveillance.gouv.fr, rapport d'activité 2025) ; côté attaquant, un coût d'entrée devenu dérisoire : services de deepfake facturés quelques dizaines de dollars et modèles criminels dédiés à l'hameçonnage documentés (CERT-FR, février 2026).

- Deepfakes audio et vidéo, du clonage de voix à la visioconférence truquée — anatomie de cas réels documentés : la fraude Arup (janvier 2024, environ 25,6 millions de dollars virés en quinze virements après une visioconférence dont tous les participants, « directeur financier » compris, étaient des deepfakes — point de départ : un simple e-mail d'hameçonnage) ; la voix clonée du ministre italien de la Défense (février 2025, environ 1 million d'euros viré par un dirigeant — fonds retrouvés sur un compte néerlandais et gelés grâce à un signalement rapide) ; les entretiens d'embauche en visioconférence truqués documentés par le FBI (rapport IC3 2025).
- Les chiffres officiels, datés et sourcés : la fraude au virement s'intensifie fortement — +93 % de diagnostics pour les entreprises en 2025, entrée dans le top 3 des menaces professionnelles (13,5 % des assistances), l'hameçonnage restant le deuxième motif à 16 % (Cybermalveillance.gouv.fr, rapport d'activité 2025, publié en mars 2026) ; aux États-Unis, plus de 3 milliards de dollars de pertes déclarées sur la fraude aux ordres de virement et plus de 30 millions de dollars sur des fraudes de ce type impliquant explicitement l'IA (FBI, rapport IC3 2025).
- La mécanique commune des arnaques facilitées par l'IA — fraude au faux dirigeant, faux fournisseur et changement de RIB, usurpation en visioconférence, faux candidats, faux support : trois constantes à repérer systématiquement — la pression (urgence, confidentialité exigée), l'usurpation (autorité invoquée, voix ou image imitée) et le canal unique (impossibilité de recouper) ; pourquoi « reconnaître la voix » ou « voir le visage » ne constitue plus une preuve d'identité.
- Cartographier l'exposition de sa structure : qui peut être usurpé (dirigeants dont la voix et l'image sont publiques — interviews, webinaires —, signataires), qui sera ciblé (comptabilité, trésorerie, assistanat de direction), quels flux financiers (virements, RIB fournisseurs, paie), quelles périodes de vulnérabilité (congés des valideurs, clôtures) et quelles informations publiques alimentent l'attaque (site, réseaux sociaux, organigramme) ; hiérarchiser ses scénarios de risque.
- Cadre déontologique de la formation, posé dès l'ouverture : les cas sont étudiés sur extraits documentés publics uniquement — aucun outil offensif, aucune recette d'attaque, aucune génération de deepfake en séance ; rappel express des fondamentaux en ouverture (acquis de la formation « Cybersécurité et hygiène numérique » ou équivalent), sans ré-enseignement ; confidentialité entre participants cadrée dès l'accueil.

MISE EN PRATIQUE

Quiz flash de rappel des fondamentaux (une dizaine de questions, correction commentée), puis étude de cas guidée sur le dossier de cas sourcés (anatomie croisée des fraudes Arup et « voix du ministre » : ce qui a marché côté attaquant, ce qui a sauvé côté défense) ; atelier « Cartographie de MON exposition » : à partir de la fiche de préparation remplie en amont, chaque participant cartographie sur gabarit guidé les personnes usurpables de sa structure (voix et image publiques comprises), les fonctions ciblées, les flux financiers sensibles et les informations publiques exploitables, puis hiérarchise ses trois scénarios les plus plausibles ; restitution flash de deux cartographies challengées par le groupe (« qu'est-ce qui manque ? »).

LIVRABLE

Cartographie d'exposition de sa structure (personnes usurpables, fonctions ciblées, flux financiers sensibles, informations publiques exploitables) avec ses trois scénarios de risque hiérarchisés.

MODULE

02.

3H30

Verrouiller les flux financiers : procédures anti-fraude et réaction à la fraude avérée

OBJECTIF OPÉRATIONNEL

« Rédiger les procédures anti-fraude de SA structure — double validation des virements, contre-appel systématique, vérification des changements de RIB, code interne — conformes à la fiche officielle de Cybermalveillance.gouv.fr, ainsi que sa fiche réflexe en cas de fraude avérée. »

CONTENU PÉDAGOGIQUE

- Le principe fondateur : face à des voix et des visages falsifiables, l'authentification ne repose plus sur le jugement individuel (« j'ai reconnu la voix ») mais sur des procédures écrites, connues de tous et non dérogeables ; le référentiel de travail de la formation : la fiche réflexe « escroquerie aux faux ordres de virement » de Cybermalveillance.gouv.fr (mise à jour du 18 mai 2026).
- La double validation des virements : séparation des rôles (demandeur, valideur, exécutant), seuils en euros adaptés à sa structure, validation hiérarchique interne non dérogeable — y compris, et surtout, pour une demande « urgente et confidentielle » émanant de la direction : c'est précisément le scénario de la fraude au président.
- Le contre-appel systématique : rappeler l'émetteur de toute demande sensible sur un numéro déjà connu (annuaire interne, contrat) — jamais sur les coordonnées fournies dans le message lui-même ; la vérification des changements de RIB directement auprès du fournisseur par un canal indépendant ; les codes de vérification internes pour les demandes inhabituelles entre direction et fonctions financières.
- Réduire la surface d'attaque : limiter les informations publiées sur les personnes habilitées aux paiements, sécuriser les messageries des fonctions exposées (double authentification — acquis des fondamentaux, non ré-enseigné), préparer les périodes de vulnérabilité : congés des valideurs et suppléances nommées, clôtures comptables, fins de semaine.
- Réagir à la fraude avérée — la course contre la montre, dans l'ordre : identifier immédiatement l'ensemble des virements exécutés, en instance ou à venir vers les coordonnées frauduleuses ; alerter sa banque et demander le retour des fonds ; préserver les preuves ; déposer plainte — le dépôt de plainte conditionne les chances de récupération auprès de la banque (conduite à tenir de la fiche officielle) —, avec l'appui du dispositif public 17Cyber pour être guidé dans ses démarches ; le gel des fonds dans le cas italien de février 2025 — retrouvés sur un compte néerlandais — comme preuve que la réaction rapide paie.

- Le réalisme comme critère de qualité d'une procédure : applicable par la personne seule au bureau un vendredi à 17h50 — suppléances prévues, et adaptation aux petites structures où le dirigeant est aussi le valideur : contre-appel obligatoire à partir d'un seuil et délai de réflexion imposé sur toute demande pressante.

MISE EN PRATIQUE

Démonstration commentée : un scénario de fraude au président scripté, déroulé pas à pas contre la procédure type — le groupe constate où l'attaque casse (au contre-appel) ; ateliers « Mes procédures anti-fraude » : chaque participant rédige sur gabarits les procédures de SA structure (procédure virements et changements de RIB avec seuils et rôles nommés, protocole de vérification d'identité), puis sa fiche réflexe « fraude avérée » (contacts bancaires et internes réels, étapes chronologiques) ; revue croisée en binôme avec test de complétude : « et si le valideur est en congé ? », « et si c'est le dirigeant qui demande ? ».

LIVRABLE

Procédures anti-fraude rédigées et adaptées à sa structure (virements et changements de RIB, protocole de vérification d'identité) et fiche réflexe « fraude avérée » personnalisée.

JOUR 2

Jour 2 — Éprouver, cadrer, transmettre

Des procédures testées en simulation à la charte d'usage IA sûre et à l'exercice de sensibilisation prêt à rejouer en interne.

MODULE

03.

3H30

Éprouver ses défenses : limites de la détection, vérification et simulations

> **OBJECTIF OPÉRATIONNEL**
>
> *« Situer les limites réelles de la détection des deepfakes, installer le réflexe de vérification par canal indépendant, puis éprouver SES procédures en simulation scriptée et les amender à partir des failles constatées. »*

CONTENU PÉDAGOGIQUE

- Les limites honnêtes de la détection automatique : sur des deepfakes réels circulant en ligne, la performance des meilleurs détecteurs ouverts s'effondre par rapport aux conditions de laboratoire — baisse de l'ordre de 45 à 50 % de la mesure de discrimination selon le média, vidéo, audio ou image (benchmark académique Deepfake-Eval-2024) ; un jeu du chat et de la souris permanent entre générateurs et détecteurs (NIST, rapport AI 100-4, novembre 2024) ; un contenu synthétique de plus en plus difficile à détecter et facile à produire (FBI, rapport IC3 2025) — conclusion : pas de détecteur miracle sur lequel bâtir sa défense.
- Les indices humains : utiles, jamais suffisants — désynchronisation entre les lèvres et le son (indice documenté par le FBI pour les visioconférences truquées), artefacts d'image, refus d'un geste imprévu à l'écran ; et surtout les incohérences de contexte : demande inhabituelle, canal inhabituel, urgence injustifiée, confidentialité exigée.
- Le basculement de posture : de « détecter le faux » à « vérifier l'identité et la demande par un canal indépendant » — la procédure rédigée au module 2 comme seul rempart qui ne dépend pas de la sophistication de l'attaque.
- Concevoir une simulation qui teste la procédure, jamais les personnes : scénarios scriptés (l'appel du « dirigeant pressé », le changement de RIB fournisseur, la visioconférence suspecte), distribution des rôles — attaquant tenu au script, cible, observateur —, grille d'observation, critères de réussite, débrief sans blâme ; aucun outil offensif, aucune voix clonée : le script suffit, et ce cadre déontologique est aussi celui que les participants réutiliseront en interne.

- Lire les résultats d'une simulation : distinguer les failles de rédaction (le cas n'était pas prévu), de diffusion (la procédure existait mais n'était pas connue) et d'application sous pression (connue mais non appliquée dans l'urgence) — chaque type de faille appelle un remède différent.
- Amender et consigner : le cycle rédiger → simuler → amender → rejouer, réutilisable en interne à rythme régulier ; le compte rendu de simulation comme trace du test et pièce du plan de défense.

MISE EN PRATIQUE

Mini-défi collectif « authentique ou deepfake ? » sur extraits documentés publics, pour ancrer l'humilité face à la détection (vote à main levée, sans score individuel) ; simulations en trinômes avec rotation des rôles : chaque participant éprouve SES procédures rédigées la veille face aux scénarios scriptés (l'appel du « dirigeant pressé », le changement de RIB fournisseur) pendant que l'observateur note sur grille ; débrief structuré par les observateurs et typologie des failles constatées ; puis chacun amende ses procédures et consigne son compte rendu de simulation — ce qui a tenu, ce qui a cassé, les corrections apportées.

LIVRABLE

Procédures anti-fraude éprouvées en simulation et amendées, avec compte rendu de simulation (failles constatées et corrections apportées).

MODULE

04.

3H30

Cadrer les usages de l'IA et embarquer son équipe : charte d'usage sûre et exercice de sensibilisation

OBJECTIF OPÉRATIONNEL

« Cadrer les usages de l'IA de son équipe par une charte d'usage sûre, assembler SON exercice de sensibilisation interne prêt à rejouer et consolider son plan de défense avec un calendrier de mise en œuvre. »

CONTENU PÉDAGOGIQUE

- La fuite par l'usage : des données confidentielles (fichiers clients, RIB, données RH, éléments contractuels) saisies dans des assistants IA en ligne, souvent via des comptes personnels non cadrés ; le « shadow AI » — ces usages non déclarés qui échappent à toute maîtrise ; pourquoi l'interdiction pure nourrit le phénomène au lieu de le réduire, et ce qui fonctionne : des règles claires, des outils validés et un signalement sans blâme.
- La charte d'usage IA sûre, pièce de gouvernance : liste des outils validés et conditions d'utilisation (comptes professionnels, paramètres de confidentialité vérifiés), catégories de données autorisées et interdites nommées (RIB, paie, fichiers clients…), circuit de validation d'un nouvel outil, signalement des usages hors cadre sans blâme, revue périodique datée.
- Usage responsable et cadre réglementaire : distinguer la confidentialité contractuelle (secret des affaires) et la protection des données à caractère personnel (RGPD, recommandations CNIL) ; situation au regard de la littératie IA prévue par l'AI Act (Règlement (UE) 2024/1689, art. 4, applicable depuis le 2 février 2025) : en cadrant l'usage d'assistants IA, l'organisation agit comme déployeur et l'obligation de littératie concerne son personnel ; cette formation y contribue sans constituer une prestation de mise en conformité. À la date de conception (juillet 2026), la formulation de l'art. 4 évolue (« Digital Omnibus » adopté par le Parlement européen le 16 juin 2026 puis par le Conseil le 29 juin 2026 : « garantir » → « soutenir ») ; ce texte n'étant pas encore publié au JOUE, le règlement (UE) 2024/1689 reste la base, ses règles de surveillance s'appliquant à compter du 2 août 2026.
- Frontière assumée : la charte cadre l'usage sûr des assistants en ligne ; pour les données qui ne doivent transiter par aucun service externe, l'option d'une IA installée en local relève des formations dédiées du catalogue Akademia (IA locale), présentées en perspective de clôture sans être entamées.

- L'exercice de sensibilisation interne : des formats courts et rejouables (30 à 45 minutes — cas à trier, jeu de rôle scripté, quiz, débrief) ; les règles d'or : exercice annoncé et collectif, jamais de piège individuel ni de campagne surprise humiliante, débrief capacitant centré sur la procédure ; mesurer la progression et rejouer à rythme régulier — le kit complet est fourni (scénarios, quiz, grilles de débrief, exemple rempli).
- Le plan de défense consolidé : articuler cartographie, procédures amendées, charte et exercice en un document unique, avec calendrier de mise en œuvre — dates nommées, responsables désignés — et évaluation des acquis sur les livrables du fil rouge.

MISE EN PRATIQUE

Ateliers de consolidation : chaque participant rédige SA charte d'usage IA sûre sur gabarit guidé (outils validés, données autorisées et interdites, signalement sans blâme), avec revue croisée éclair en binôme (« et un CV reçu, je peux le résumer dans l'assistant ? ») ; puis assemble SON exercice de sensibilisation — scénario choisi en cohérence avec sa cartographie du jour 1, déroulé minuté, quiz personnalisé, plan de débrief — et consolide son plan de défense, prérempli au fil des deux jours à chaque bilan de module, avec calendrier de mise en œuvre ; présentation de clôture de deux minutes par participant : son exposition, ses procédures, sa charte, son exercice et la date de sa première session interne.

LIVRABLE

Charte d'usage IA sûre rédigée, exercice de sensibilisation interne prêt à rejouer (scénario, déroulé minuté, quiz, plan de débrief) et plan de défense consolidé avec calendrier de mise en œuvre.

MÉTHODES PÉDAGOGIQUES

Apprendre par la pratique, avec un formateur expert à vos côtés.

- Pédagogie active et apprentissage par le faire : la pratique occupe la place centrale — de l'ordre de 40 à 45 % du temps en ateliers individuels accompagnés, simulations scriptées et revues croisées portant sur la structure réelle du participant (fil rouge), et plus de 60 % du temps consacré à la pratique au sens large en y ajoutant le quiz de rappel, les études de cas guidées, le défi de détection et les démonstrations commentées ; le reste en apports méthodologiques cadrés.
- Pédagogie positive et capacitante : chaque menace présentée est immédiatement suivie de la parade organisationnelle à la portée de la structure ; pas de catastrophisme, pas de culpabilisation — on repart outillé, pas inquiet.
- Méthode magistrale : apports structurés courts, appuyés sur des supports visuels et sur des faits sourcés et datés (ANSSI, CERT-FR, Cybermalveillance.gouv.fr, FBI, NIST).
- Études de cas guidées et démonstrations scriptées : les cas réels sont étudiés exclusivement sur extraits documentés publics et les scénarios d'attaque sont déroulés au script — jamais d'outil offensif, de recette d'attaque ni de génération de deepfake en séance.
- Méthode active : simulations en trinômes avec rotation des rôles (attaquant tenu au script, cible, observateur), revues croisées en binôme et restitutions favorisant l'ancrage du réflexe de vérification.
- Accompagnement individualisé : le formateur adapte le niveau de soutien selon le profil (dirigeant de TPE sans service financier ou manager d'une structure outillée, à l'aise ou non avec les sujets numériques), sur la base du test de positionnement et de la fiche de préparation.
- Approche par compétences : chaque module produit un livrable directement réinvestissable, l'ensemble étant assemblé en plan de défense final.

Profil du formateur

Formateur expert à double compétence : prévention de la fraude et sécurité organisationnelle (ingénierie sociale, fraude aux ordres de virement, référentiels Cybermalveillance.gouv.fr, ANSSI et CNIL) et usages de l'IA générative — capacités réelles et détournements documentés. Il justifie d'une expérience concrète de sensibilisation de dirigeants et d'équipes non techniques, et met à jour avant chaque session le dossier de cas réels et les chiffres officiels : sur ce sujet, l'état de la menace évolue en quelques mois.

Moyens & supports

- En présentiel : salle équipée d'un vidéoprojecteur avec diffusion audio (enceintes ou sonorisation) pour les extraits vidéo et audio du dossier de cas, et permettant d'éloigner deux sous-groupes pour les simulations (ou disposant d'un espace de dégagement attenant) ; paperboard, connexion internet et un poste par participant.
- En distanciel : classe virtuelle synchrone via les outils Akademia (partage d'écran, sous-groupes en salles virtuelles pour les simulations et revues croisées — les appels scriptés se jouent caméra coupée pour le réalisme du scénario vocal).
- Plateforme LMS Akademia (FormAI) : test de positionnement en ligne, fiche de préparation et mise à disposition de l'ensemble des ressources (supports, gabarits, dossier de cas, kits de simulation et d'exercice).
- Dossier de cas réels sourcés et datés : extraits documentés publics commentés (articles de presse, rapports officiels) — aucun outil de génération de deepfake ni outil offensif n'est utilisé ni montré pendant la formation.
- Kit de gabarits remis à chaque participant : cartographie d'exposition, procédures anti-fraude, fiche réflexe « fraude avérée », kit de simulation, charte d'usage IA, kit d'exercice de sensibilisation et plan de défense consolidé.

Modalités d'évaluation

- Test de positionnement en ligne réalisé sur la plateforme LMS avant le début de la formation (acquis des fondamentaux, exposition de la structure, pratiques IA de l'équipe), complété par un tour de table des attentes et par la fiche de préparation (schéma de validation des virements existant, fonctions habilitées).
- Évaluation formative continue : les livrables de chaque module, le quiz de rappel des fondamentaux, les simulations observées sur grille et les revues croisées en binôme permettent au formateur de vérifier la progression sur chaque objectif et d'apporter une remédiation immédiate.

- Outils IA abordés en démonstration commentée uniquement (paramètres de confidentialité des assistants grand public, posture multi-éditeurs) : aucun assistant IA n'est requis pour les ateliers, qui portent sur l'organisation et les procédures.

- Évaluation sommative : grille critériée d'atteinte des objectifs, renseignée au fil des ateliers, restituée individuellement à chaque participant, puis consolidée en fin de session, appliquée aux productions réalisées sur la structure fil rouge (cartographie d'exposition avec scénarios hiérarchisés ; qualification d'une sollicitation suspecte à ses trois constantes — pression d'urgence, autorité usurpée, canal unique — observée en situation de simulation sur la grille d'observation et reprise dans le quiz de l'exercice de sensibilisation ; procédures anti-fraude rédigées puis amendées après simulation ; compte rendu de simulation ; fiche réflexe « fraude avérée » personnalisée ; charte d'usage IA sûre ; exercice de sensibilisation assemblé ; plan de défense consolidé avec calendrier), intégrant un critère d'usage responsable observable (aucune donnée confidentielle réelle exposée pendant les ateliers — schémas anonymisés si nécessaire —, respect du cadre déontologique : extraits documentés publics uniquement, confidentialité entre participants), complétée par un auto-positionnement de sortie reprenant les items du test amont pour objectiver la progression.
- Évaluation de satisfaction à chaud en fin de session et évaluation à froid à distance, à 1 à 3 mois, mesurant le transfert en situation de travail : procédures anti-fraude effectivement déployées, première session de l'exercice de sensibilisation animée en interne, sollicitations suspectes détectées et signalées — à titre indicatif et non garanti.

Documentation remise aux stagiaires

- Le support de formation complet
- Le dossier de cas réels sourcés et datés (extraits documentés publics commentés)

Équipements à apporter

- Ordinateur portable

- Le gabarit de cartographie d'exposition et la fiche de préparation
- Les gabarits de procédures anti-fraude : virements et changements de RIB, protocole de vérification d'identité, avec la checklist de complétude pour la revue croisée
- La fiche réflexe « fraude avérée » à personnaliser (chronologie, contacts bancaires et internes)
- Le kit de simulation : trois scénarios scriptés, grille d'observation, trame de débrief et compte rendu type
- Le gabarit de charte d'usage IA sûre avec exemple commenté
- Le kit d'exercice de sensibilisation interne : scénarios, quiz, grilles de débrief et déroulé type de 30 à 45 minutes, avec exemple rempli
- Le gabarit de plan de défense consolidé avec calendrier de mise en œuvre
- Attestation de fin de formation mentionnant les objectifs et le résultat de l'évaluation des acquis

Accessibilité & handicap

Les besoins d'adaptation sont recensés dès l'inscription. Un référent handicap Akademia est identifié et joignable pour étudier, au cas par cas avec le participant, les aménagements possibles (rythme, supports, modalité). Les conditions d'accès sont vérifiées selon la situation.

Modalités & délais d'accès

Formation en petit groupe (4 à 6 participants), pour garantir un accompagnement individualisé sur le plan de défense de chaque structure et des simulations en trinômes réalistes. Inscription en ligne ou auprès du service formation, entrée à date fixe selon le calendrier des sessions. Une fiche de préparation est transmise en amont (schéma actuel de validation des virements et des changements de RIB, fonctions habilitées, usages d'assistants IA dans l'équipe, contacts bancaires et assurance utiles en cas de fraude) — sans transmettre aucun document confidentiel : les éléments sensibles restent dans l'entreprise et peuvent

être anonymisés. La convocation comporte un engagement de confidentialité entre participants : les cartographies d'exposition et les procédures travaillées en séance ne sont ni diffusées ni discutées hors du groupe. Pour les financements OPCO, l'inscription doit intervenir suffisamment tôt pour respecter les délais d'instruction du dossier ; Akademia accompagne le participant dans ses démarches.

Tarif

SESSION INTER-ENTREPRISES

1 490 € net de taxe

par participant · 2 jours (14 h)

Exonération de TVA · art. 261-4-4° a du CGI

SESSION INTRA-ENTREPRISE

Tarif sur devis

Session dédiée à vos collaborateurs, dans vos locaux ou à distance. Contactez-nous pour une proposition chiffrée personnalisée selon l'effectif et les modalités.

Prise en charge possible par votre OPCO ou France Travail. Nos équipes vous accompagnent dans le montage du dossier de financement.

PASSONS À L'ACTION

Construisons ensemble votre session sur-mesure.

Dites-nous vos contraintes (format, lieu, dates, nombre de participants) et recevez une proposition personnalisée sous 24 heures ouvrées.

Akademia Formation

SERVICE ADMINISTRATION DES VENTES

adv@akademiaformation.com

www.akademiaformation.com

Devis personnalisé

RÉPONSE SOUS 24 H OUVRÉES

Format inter · intra

Présentiel ou distanciel

FIN DU PROGRAMME