

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Cybersécurité et IA : les nouvelles menaces à connaître

CT07 · Module de spécialisation

Ce module de 21 heures permet aux professionnels des TPE et PME d'identifier, d'évaluer et de contrer les nouvelles menaces cyber amplifiées par l'intelligence artificielle, tout en sécurisant l'usage des outils d'IA au sein de leur organisation. Il prépare aux certifications RS6986 et RS7029 et suit un fil rouge concret : une PME industrielle confrontée à des attaques par deepfake, hameçonnage généré par IA et fuite de données via des outils grand public.

VOLUME HORAIRE	COURS	BLOCS
21 h	6	3

01 · PRÉSENTATION

La formation en bref

Intitulé	Cybersécurité et IA : les nouvelles menaces à connaître
Code	CT07
Type	Module de spécialisation
Certificateur	Hors répertoire
Durée	21 h, 6 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026

Le métier et les compétences visées

La compétence visée est celle d'un professionnel capable de piloter la cybersécurité d'une TPE ou d'une PME dans un contexte où l'intelligence artificielle transforme à la fois les attaques et les usages internes. Sans occuper forcément un poste dédié, il inventorie le système d'information et analyse les risques. Il définit les règles de sécurité et gère les identités. Il sensibilise les collaborateurs aux fraudes par deepfake et à l'hameçonnage personnalisé, puis organise la réponse aux incidents. Il encadre également le déploiement des outils d'IA générative : conformité à l'AI Act et au RGPD, prise en compte de l'éthique, accompagnement du changement et coordination avec le DSI, le DPO et le référent RSE.

Public visé

- Responsables informatiques de TPE et PME chargés de la démarche de cybersécurité
- Directeurs techniques (CTO) de PME
- Consultants en systèmes informatiques et techniciens support intervenant pour des TPE et PME
- Managers et cadres dirigeants pilotant l'introduction d'outils d'intelligence artificielle dans leur organisation

Prérequis

- Pour la certification RS7029 : être manager ou cadre dirigeant et justifier d'une expérience professionnelle d'au moins 1 an
- Connaître le fonctionnement général d'un système d'information d'entreprise (postes, serveurs, messagerie, réseau)
- Utiliser couramment les outils bureautiques et collaboratifs en environnement professionnel

Objectifs pédagogiques

À l'issue du parcours, l'apprenant est capable de :

- Identifier les principales menaces cyber amplifiées par l'IA (hameçonnage génératif, deepfakes, logiciels malveillants automatisés, attaques de chaîne d'approvisionnement) et mettre en place une veille adaptée
- Réaliser l'inventaire du système d'information, y compris les outils et API d'IA, puis analyser les risques avec les méthodes EBIOS RM et ISO 27005
- Établir un état des lieux du niveau de sécurité et des obligations réglementaires, puis présenter un plan de sécurisation à la direction
- Définir une politique de sécurité intégrant la surveillance (EDR, SIEM), les mises à jour, les sauvegardes et les règles d'usage de l'IA générative

- Organiser la gestion des identités et des contrôles d'accès des personnes, équipements, prestataires et services d'IA reliés au SI
- Concevoir, tester et ajuster un prompt pour optimiser une tâche de cybersécurité sans exposer de données sensibles
- Vérifier la conformité d'un projet d'IA au regard de l'AI Act, du RGPD, de la propriété intellectuelle et des cadres américain et chinois, en mobilisant les référents internes
- Évaluer l'impact éthique et environnemental d'un outil d'IA ainsi que ses risques de biais
- Concevoir une action de sensibilisation et d'accompagnement du changement accessible à tous les collaborateurs, y compris en situation de handicap
- Piloter la gestion d'une crise cyber et conduire une réponse à incident sans destruction de traces, jusqu'au rapport et au retour d'expérience

02 · FIL ROUGE PÉDAGOGIQUE

Ateliers Morvane Industrie

JK

Julien Kerbrat

Responsable informatique, seul en charge du SI et désormais référent cybersécurité

Sous-traitance industrielle en usinage de précision pour l'aéronautique et le ferroviaire (PME de 85 salariés, deux sites)

Ateliers Morvane Industrie est une PME familiale qui travaille pour de grands donneurs d'ordre exigeants en matière de sécurité. Sa dirigeante, Claire Morvane, souhaite déployer un assistant d'IA générative pour accélérer la rédaction des devis et des dossiers techniques. Plusieurs commerciaux utilisent déjà des outils grand public sans aucun cadre. Un vendredi soir, la comptable reçoit un appel vocal imitant parfaitement la voix de Claire et lui demandant un virement urgent. Le virement est bloqué de justesse. Peu après, un donneur d'ordre exige un plan de cybersécurité formalisé avant le renouvellement de son contrat. Julien Kerbrat, responsable informatique, doit structurer en quelques mois une démarche complète. Il lui faut comprendre les menaces liées à l'IA, sécuriser le SI, encadrer le projet d'assistant IA, mobiliser les équipes et se préparer à gérer une crise.

Chaque cours se termine par une mise en situation dans cette entreprise : l'apprenant accompagne Julien dans des situations professionnelles réalistes, de plus en plus complexes, jusqu'à la préparation des épreuves.

La progression

1. Bloc M1 : Julien analyse la tentative de fraude par deepfake, organise une veille sur les menaces liées à l'IA, cartographie le SI et ses outils d'IA non déclarés, conduit une analyse de risques EBIOS RM et présente un plan de sécurisation à Claire Morvane.
2. Bloc M2 : Julien rédige la politique de sécurité et la charte d'usage de l'IA, refond la gestion des accès des salariés et des prestataires, puis vérifie avec le DPO externe et la référente RSE la conformité et l'éthique du futur assistant IA.
3. Bloc M3 : Julien déploie un programme de sensibilisation accessible à tous et accompagne l'arrivée de l'assistant IA. Il pilote ensuite la cellule de crise lors d'une compromission de messagerie, puis rédige le rapport d'incident et le plan anti-récidive.

03 · ARCHITECTURE

Organisation du parcours

Le parcours est construit sur les compétences visées : chaque bloc regroupe les cours qui préparent à son évaluation.

N°	Bloc et cours	Durée
M1 · Comprendre les menaces liées à l'IA et évaluer les risques du système d'information		**7 h**
1	Panorama des nouvelles menaces cyber amplifiées par l'intelligence artificielle	3 h 30
2	Cartographier le SI, analyser les risques et établir l'état des lieux de sécurité	3 h 30
M2 · Protéger le système d'information et encadrer l'usage de l'IA		**7 h**
3	Politique de sécurité, surveillance et gestion des identités à l'ère de l'IA	3 h 30
4	Déployer un outil d'IA en conformité : cadre juridique, éthique et sécurité	3 h 30
M3 · Mobiliser les collaborateurs et réagir aux incidents cyber		**7 h**
5	Sensibiliser les collaborateurs et accompagner le changement face aux menaces liées à l'IA	3 h 30
6	Gérer une crise cyber et conduire la réponse à incident	3 h 30
Total du parcours		**21 h**

Répartition des modalités pédagogiques

Chaque sous-chapitre s'ouvre sur une vidéo de 3 à 5 minutes. La vidéo représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies, des études de cas, des mises en situation et des QCM.



- Vidéos : 6 h 30
- Cours texte et infographies : 6 h 30
- Études de cas et mises en situation : 5 h
- QCM et évaluations : 3 h

04 · PROGRAMME DÉTAILLÉ

Contenu des cours

M1 · 7 h

Comprendre les menaces liées à l'IA et évaluer les risques du système d'information

Cours 1 · Panorama des nouvelles menaces cyber amplifiées par l'intelligence artificielle

3 h 30

OBJECTIFS

- Identifier les modes opératoires d'attaque renforcés par l'IA et leurs cibles privilégiées dans une TPE ou une PME
- Reconnaître les attaques visant spécifiquement les systèmes d'IA et la chaîne d'approvisionnement logicielle
- Élaborer une politique de veille sur les menaces internes et externes

ÉVALUATION FORMATIVE

QCM de reconnaissance des menaces et étude de cas : analyse commentée de trois messages suspects (courriel, message vocal, demande fournisseur)

CONTENUS

- Hameçonnage génératif et ingénierie sociale personnalisée à grande échelle
- Deepfakes audio et vidéo : fraude au président, usurpation d'identité, faux entretiens
- Logiciels malveillants automatisés et polymorphes, accélération de la recherche de vulnérabilités
- Attaques contre les systèmes d'IA : injection de prompt, empoisonnement de données, extraction de modèles
- Attaques de chaîne d'approvisionnement : altération de code, bibliothèques et modèles compromis, détournement d'applications légitimes
- Shadow AI : fuites de données via les outils d'IA grand public utilisés sans cadre
- Construire une veille sur les menaces : sources institutionnelles (ANSSI, CERT-FR, Cybermalveillance.gouv.fr), fréquence, diffusion interne

Fil rouge · Julien reconstitue la chronologie de l'appel deepfake reçu par la comptable et identifie les informations publiques ayant permis l'imitation de la voix de Claire Morvane. Il formalise ensuite une fiche de veille hebdomadaire destinée à la direction.

Cours 2 · Cartographier le SI, analyser les risques et établir l'état des lieux de sécurité

3 h 30

OBJECTIFS

- Réaliser l'inventaire des équipements, logiciels, interconnexions et services d'IA du SI
- Évaluer les risques avec EBIOS RM et ISO 27005, et identifier les périmètres où l'IA peut renforcer la défense
- Dresser un état des lieux réglementaire et présenter un plan de sécurisation à la direction

ÉVALUATION FORMATIVE

Exercice pratique : remplir une matrice d'inventaire et une cartographie des risques à partir du dossier de l'entreprise fictive, avec un corrigé commenté

CONTENUS

- Inventaire du SI : équipements, logiciels, comptes, interconnexions externes, API et outils d'IA
- Identification des vulnérabilités et des menaces rapportées au SI de l'entreprise
- Méthode EBIOS Risk Manager appliquée à une PME : ateliers, scénarios stratégiques et opérationnels
- Norme ISO 27005 : appréciation, évaluation et traitement des risques
- Opportunités de l'IA pour la cybersécurité : plus-value, modalités d'exploitation technique, limites
- Responsabilités juridiques de l'entreprise et obligations réglementaires (RGPD, exigences contractuelles des donneurs d'ordre, directive NIS 2 selon l'assujettissement)
- Plan de sécurisation du SI et sensibilisation de la direction aux mesures de protection et à la conduite à tenir en cas de crise

Fil rouge · Julien découvre lors de l'inventaire que quatre outils d'IA non déclarés traitent des plans clients. Il conduit un atelier EBIOS RM simplifié avec Claire Morvane et le responsable de production, puis présente un plan de sécurisation priorisé.

M2 · 7 h

Protéger le système d'information et encadrer l'usage de l'IA

Cours 3 · Politique de sécurité, surveillance et gestion des identités à l'ère de l'IA

3 h 30

OBJECTIFS

- Définir les règles de sécurité de l'entreprise et préconiser une solution de surveillance adaptée
- Organiser la gestion des identités et des accès des personnes, équipements et services connectés au SI
- Concevoir, tester et ajuster un prompt pour optimiser une tâche de sécurité

ÉVALUATION FORMATIVE

Mise en situation guidée : rédaction d'un extrait de politique de sécurité et d'une matrice des droits d'accès, puis grille d'auto-évaluation du prompt conçu

CONTENUS

- Règles d'utilisation du SI et charte d'usage de l'IA générative (données autorisées, outils validés)
- Mises à jour des appareils et des logiciels, antivirus, gestion des correctifs
- Stratégie de sauvegarde : règle 3-2-1, sauvegardes hors ligne, tests de restauration
- Solutions de surveillance (EDR, SIEM) : critères de choix pour une PME, apports et limites de l'IA dans la détection
- Gestion des identités : moindre privilège, authentification multifacteur résistante à l'hameçonnage, cycle de vie des comptes
- Contrôle des prestataires, équipements tiers, comptes de service et clés d'API des outils d'IA
- Atelier prompt : concevoir, tester et ajuster un prompt d'aide à l'analyse de journaux ou à la rédaction de règles, sans données sensibles

Fil rouge · Julien rédige la charte d'usage de l'IA et supprime les accès d'un ancien prestataire de maintenance encore actifs. Il met au point un prompt permettant de synthétiser les alertes hebdomadaires de l'EDR pour la direction.

Cours 4 · Déployer un outil d'IA en conformité : cadre juridique, éthique et sécurité

3 h 30

OBJECTIFS

- Vérifier la conformité d'un projet d'IA au regard de l'AI Act, du RGPD et de la propriété intellectuelle
- Situer le projet par rapport aux cadres réglementaires américain et chinois
- Intégrer les critères éthiques (biais, impact environnemental) en mobilisant les référents internes

ÉVALUATION FORMATIVE

Étude de cas : compléter une grille de conformité et d'éthique pour un projet d'IA, suivie d'un QCM sur l'AI Act et le RGPD

CONTENUS

- AI Act : classification des systèmes par niveau de risque, obligations des fournisseurs et des déployeurs
- RGPD et IA : bases légales, minimisation, analyse d'impact (AIPD), transferts de données hors Union européenne
- Propriété intellectuelle des contenus produits par l'IA et protection des secrets d'affaires
- Panorama des cadres internationaux : États-Unis et Chine, conséquences pour le choix d'un fournisseur
- Rôles du DPO, du référent RGPD, du DSI et du référent RSE dans un projet d'IA
- Éthique : biais cognitifs et algorithmiques, impact environnemental, critères de déploiement responsable
- Sécuriser le déploiement : hébergement, clauses contractuelles, journalisation, tests avant mise en production

Fil rouge · Claire Morvane souhaite choisir entre deux assistants d'IA pour le service commercial. Julien prépare avec le DPO externe et la référente RSE une grille de conformité, puis recommande l'outil le plus adapté.

M3 · 7 h

Mobiliser les collaborateurs et réagir aux incidents cyber

Cours 5 · Sensibiliser les collaborateurs et accompagner le changement face aux menaces liées à l'IA

3 h 30

OBJECTIFS

- Établir un code de bonne conduite et diffuser les règles d'hygiène fondamentales de la cybersécurité
- Concevoir une démarche d'acculturation et d'accompagnement du changement accessible aux collaborateurs en situation de handicap
- Vérifier la compréhension des enjeux par l'ensemble des parties prenantes

ÉVALUATION FORMATIVE

Production guidée : concevoir le plan d'une action de sensibilisation accessible et son questionnaire de vérification, avec une grille d'auto-évaluation

CONTENUS

- Code de bonne conduite : comportements adaptés, précautions techniques et juridiques
- Règles d'hygiène fondamentales : mots de passe, mises à jour, supports amovibles, mobilité
- Reconnaître un deepfake et un hameçonnage génératif : signaux d'alerte et procédures de vérification
- Conséquences d'une attaque : impact sur la réputation et conséquences financières
- Accessibilité des actions de sensibilisation et adaptation pour les collaborateurs en situation de handicap
- Méthodologie d'accompagnement du changement lors du déploiement d'un outil d'IA : diagnostic, relais, outils de gestion et de communication
- Mesurer la compréhension : quiz, simulations d'hameçonnage, indicateurs de suivi

Fil rouge · Julien organise une campagne de sensibilisation sur les deepfakes et une procédure de double validation des virements. Il adapte les supports pour un collaborateur malvoyant de l'atelier et prépare le plan de communication de l'assistant IA.

Cours 6 · Gérer une crise cyber et conduire la réponse à incident

3 h 30

OBJECTIFS

- Gérer une situation d'urgence par l'alerte, la sécurisation et la mise en place d'une cellule de crise
- Réaliser les opérations de réponse à incident sans destruction de données ou de traces
- Rédiger un rapport d'incident et outiller les collaborateurs pour éviter la récidive

ÉVALUATION FORMATIVE

Simulation de crise séquencée avec choix à chaque étape, suivie d'une rédaction guidée d'un rapport d'incident et d'un QCM final

CONTENUS

- Premiers réflexes : sécuriser les collaborateurs, les lieux et les équipements, évacuer les lieux si nécessaire
- Alerter les autorités et les organisations pertinentes : CNIL, banques, assureur, personnes dont les données sont exposées, dépôt de plainte
- Cellule de crise et outils de communication indépendants du système attaqué
- Déclenchement du plan de continuité d'activité, prise en compte des difficultés observées et des optimisations
- Indicateurs de compromission issus des données de surveillance, évaluation de l'étendue et de la nature de l'incident
- Isolement de l'élément compromis, préservation des preuves, plan d'action et restauration des opérations
- Rapport d'incident détaillé, retour d'expérience et mesures contre la récidive

Fil rouge · Une boîte de messagerie commerciale est compromise après un hameçonnage généré par IA visant un client. Julien active la cellule de crise, isole le compte sans effacer les traces, notifie la CNIL puis rédige le rapport d'incident.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

Correspondance entre les compétences visées et les cours du parcours.

Compétence	Bloc	Cours
RS6986 C1 : Analyser la vulnérabilité de l'entreprise (inventaire, menaces, veille chaîne d'approvisionnement, EBIOS RM, ISO 27005)	M1	1, 2
RS6986 C2 : Établir un état des lieux de sécurité et des obligations réglementaires, plan de sécurisation et sensibilisation de la direction	M1	2
RS6986 C3 : Définir une politique de sécurité (surveillance EDR/SIEM, règles d'usage, mises à jour, sauvegardes)	M2	3
RS6986 C4 : Gérer les identités et contrôles d'accès	M2	3
RS6986 C5 : Sensibiliser les collaborateurs et infuser une culture de la cybersécurité, y compris pour les collaborateurs en situation de handicap	M3	5
RS6986 C6 : Gérer une situation d'urgence par l'alerte, la sécurisation, la cellule de crise et le plan de continuité	M3	6
RS6986 C7 : Réaliser les opérations de réponse à incident sans destruction de données ou de traces	M3	6
RS7029 C1 : Définir les périmètres où l'IA présente une opportunité d'optimisation (plus-value, exploitation technique, limites)	M1	2
RS7029 C2 : Optimiser une tâche à l'aide d'un outil d'IA générative (concevoir, tester, ajuster un prompt)	M2	3
RS7029 C3 : Accompagner la mise en œuvre d'un outil d'IA (conduite du changement, handicap, outils de communication)	M3	5
RS7029 C4 : S'assurer du respect du cadre juridique (AI Act, RGPD, propriété intellectuelle, États-Unis, Chine, DPO)	M2	4
RS7029 C5 : S'assurer du respect des critères éthiques (impact environnemental, biais, référent RSE)	M2	4
RS7029 C6 : S'assurer du déploiement d'une politique de cybersécurité efficace (risques, sollicitation du DSI)	M1	1, 2, 6

Évaluations formatives

Chaque sous-chapitre se termine par un QCM de validation des acquis avec une correction commentée. Chaque cours comprend une évaluation formative ancrée dans le fil rouge Ateliers Morvane Industrie : étude de cas, exercice de cartographie, rédaction guidée d'un livrable professionnel (politique de sécurité, grille de conformité, plan de sensibilisation, rapport d'incident) ou simulation de crise à choix séquencés. Les grilles d'auto-évaluation et les corrigés types permettent au stagiaire de mesurer sa progression. Le formateur de l'organisme de formation peut également s'appuyer sur ces productions pour assurer un suivi individualisé.

Modalités de certification

Bloc	Modalité d'évaluation
RS6986	Les modalités d'évaluation sont définies par le certificateur (ECOLE SUP INFORM COMMERCE) et publiées sur la fiche RS6986 de France Compétences. L'organisme de formation habilité doit en vérifier la version en vigueur et en organiser la passation.
RS7029	Les modalités d'évaluation sont définies par le certificateur (SKEMA BUSINESS SCHOOL) et publiées sur la fiche RS7029 de France Compétences. L'organisme de formation habilité doit en vérifier la version en vigueur et en organiser la passation.

Le parcours couvre l'intégralité des capacités attestées des deux référentiels, comme le montre la matrice de couverture. Il fait produire au stagiaire les livrables professionnels attendus d'un référent cybersécurité et d'un pilote de projet d'IA : inventaire et analyse de risques EBIOS RM, plan de sécurisation, politique de sécurité, matrice des droits

d'accès, prompt documenté, grille de conformité juridique et éthique, plan de sensibilisation accessible et rapport d'incident. Ces productions, réalisées dans un fil rouge cohérent, peuvent être transposées à l'entreprise réelle du stagiaire. L'organisme de formation reste responsable de l'inscription, de la préparation spécifique aux épreuves et de la certification auprès des certificateurs.

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche, accessible 24h/24 sur ordinateur, tablette et smartphone, avec suivi de progression et traçabilité des connexions
- Une vidéo de 3 à 5 minutes par sous-chapitre, soit 30 % du volume horaire, complétée par un cours texte enrichi
- Infographies de synthèse et fiches pratiques téléchargeables (checklist d'inventaire, procédure de double validation des virements, réflexes en cas de crise)
- Études de cas et mises en situation dans le fil rouge Ateliers Morvane Industrie
- Modèles de livrables réutilisables : charte d'usage de l'IA, matrice de risques, grille de conformité AI Act et RGPD, trame de rapport d'incident
- QCM de fin de sous-chapitre avec correction commentée et grilles d'auto-évaluation
- Contenus conçus selon les principes d'accessibilité numérique (sous-titres, transcriptions, contrastes, navigation clavier)

Débouchés et évolutions

- Responsable informatique de TPE ou de PME en charge de la cybersécurité
- Directeur technique (CTO) de PME
- Consultant en systèmes informatiques accompagnant des TPE et PME
- Technicien en support informatique chargé de comptes TPE et PME
- Manager ou cadre dirigeant pilotant l'introduction de l'intelligence artificielle dans son organisation

Accessibilité

Contenus sous-titrés en français, contrastes conformes WCAG AA, navigation au clavier sur les écrans interactifs. L'organisme de formation qui diffuse le parcours adapte les modalités d'accompagnement aux personnes en situation de handicap avec son référent handicap.

Livrables fournis à l'organisme de formation

- Package SCORM 1.2 / 2004 et xAPI, compatible avec les principaux LMS
- Sources éditables des cours, scripts vidéo et banques de QCM
- Livret apprenant et grilles d'évaluation
- Licence marque blanche à vie, stagiaires illimités, maintenance 24 mois

School For Mate
On crée vos formations, vous n'avez plus qu'à les diffuser.
contact@schoolformate.com · catalogue-2026-sfm.netlify.app

La délivrance de la certification relève exclusivement du certificateur et de l'organisme de formation habilité. Document non contractuel, susceptible d'évoluer avec le référentiel.