MAJ 02/02/2026

Formation « Sécurité des systèmes d'intelligence artificielle »

Réf : SECUIA

Objectifs

À l'issue de la formation, les participants seront capables de :

- **Maîtriser le vocabulaire, les concepts clés et les systèmes d'IA, notamment les modèles de langage (LLM), afin d'en comprendre les problématiques.**
- **Identifier, analyser et qualifier les problématiques liées aux usages de l'IA, incluant les risques cybersécurité, juridiques, éthiques et organisationnels.**
- **Encadrer et gouverner les usages de l'IA au sein de leur organisation, en tenant compte des rôles, des responsabilités et des obligations réglementaires applicables.**
- **Mettre en œuvre des mesures opérationnelles de réduction des risques liés aux systèmes d'IA, fondées sur une analyse de risques structurée et documentée.**
- **Intégrer la cybersécurité, la conformité et l'éthique dès la conception et tout au long du cycle de vie des projets d'IA, afin de déployer des systèmes d'IA maîtrisés, conformes et responsables.**

Durée & horaires

- **4 jours, soit 28 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 18h00**

Nombre de participants

- **Minimum 6 participants – Maximum 16 participants**

Public visé

- **RSSI,**
- **RSSI-adjoint et leurs collaborateurs,**
- **Correspondants locaux de cybersécurité,**
- **Chefs de projet et ingénieurs IA,**
- **Consultants cybersécurité**

Prérequis

- **Disposer d'une expérience au sein d'une direction des systèmes d'information (DSI), en tant qu'informaticien, ingénieur, consultant ou fonction assimilée, ou justifier d'une bonne culture générale des systèmes d'information.**
- **Avoir des notions de base en sécurité des systèmes d'information (comprendre les principes de confidentialité, intégrité, disponibilité, gestion des risques).**

Méthodes pédagogiques

- **Apports théoriques structurés (cours magistral interactif)**
- **Études de cas et exercices pratiques inspirés de situations réelles**
- **Travaux pratiques en groupe (analyse de risques, gouvernance, arbitrage)**
- **QCM d'entraînement tout au long de la formation**
- **Échanges, retours d'expérience et discussions guidées**

Supports

- **Support de cours au format papier en français en mode présentiel et au format numérique en mode distanciel (sous réserve de la signature du règlement intérieur)**
- **Documents pédagogiques complémentaires en français ou en anglais**
- **Feuille d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification HS2 SECUIA. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 1h30 en français. L'examen est de type QCM.**

Programme

Jour 1 – Matin

1.A.1 Accueil des participants

- Présentation de la formation, des formateurs et des stagiaires
- Recueil des besoins

1.A.2 Fondamentaux de l'Intelligence Artificielle

1.A.2.1 Introduction à l'Intelligence Artificielle

- Définitions et périmètre : IA, Machine Learning, Deep Learning, IA générative, agentique
- Brève histoire de l'IA : des systèmes experts aux LLM
- L'écosystème actuel : acteurs, usages, tendances, perspectives
- Usage de l'IA par les attaquants (très succinctement)

1.A.2.2 Fonctionnement des systèmes d'IA

- Cycle de vie d'un système d'IA
- Les données au cœur de l'IA : jeux d'entraînement, biais, qualité (enjeux éthiques et juridiques)
- Les grands types d'apprentissage
- Focus sur les modèles de langage (LLM) : tokenisation, embeddings, attention
- Modes de déploiement : on-premise, cloud, API, edge
- Du modèle de fondation à la spécialisation : modèles pré-entraînés, fine-tuning, RAG
- Chaîne d'approvisionnement de l'IA : AI software bill of materials, acteurs de la donnée, capacité de calcul
- Interconnexion avec un système d'IA : serveur MCP

Jour 1 – Après-midi

1.B.1 Cartographie des usages de l'IA en entreprise

- Cas d'usage par domaine métier / secteur d'activité
- IA interne vs IA exposée aux clients
- Shadow AI : risques et détection
- Inventaire des systèmes d'IA : lien explicite avec les obligations d'inventaire (AI Act, gouvernance IA)

1.B.2 Objectifs et enjeux de sécurité de l'IA

1.B.2.1 Les critères de sécurité classiques appliqués à l'IA

- Confidentialité
- Intégrité
- Disponibilité
- Confiance

1.B.2.2 Vocabulaire et concepts clés

- Sûreté de fonctionnement (biais, performance) vs sécurité (cyber)
- Définition des concepts d'explicabilité, d'opacité, de déterminisme
- Jailbreak, prompt injection etc.
- **T.P. : Jailbreak**

1.B.3 Conformité et cadre réglementaire de l'IA

1.B.3.1 Structure de gouvernance étatique de l'IA

- Articulation et périmètre de responsabilités des entités de régulation
- AI safety institute
- Stratégie nationale de l'IA (3 phases)
- Gouvernance nationale du RIA (= AI Act)

1.B.3.2 Règlement européen sur l'Intelligence Artificielle (AI Act)

- Genèse, objectifs et calendrier d'application
- Classification des systèmes d'IA par niveau de risque
- Obligations par catégorie : systèmes interdits, haut risque, risque limité, risque minimal - logique par les risques
- Exigences pour les systèmes à haut risque : données, documentation, supervision humaine
- Obligations spécifiques aux modèles d'IA à usage général (GPAI)
- Gouvernance européenne
- Sanctions et mise en conformité
- Positionnement du SIA dans l'écosystème juridique
- Notion clé : la règle applicable dépend du rôle (fournisseur / déployeur), du niveau de risque, du contexte sectoriel

1.B.3.3 Articulation avec les autres réglementations

- AI Act et RGPD : protection des données personnelles dans l'IA
- AI Act et NIS2 : systèmes d'IA critiques
- AI Act et règlements sectoriels (focus DORA - résilience opérationnelle/numérique)
- Articulation de l'IA avec CSA, CRA (schéma de certification, surveillance de produit, présomption de conformité)
- Articulation des notifications d'incident
- Comparaison internationale
- Évolution Omnibus ?

1.B.3.4 Normes et référentiels internationaux

- ISO/IEC 42001 : Système de management de l'IA
- ISO/IEC 23894 : Gestion des risques de l'IA
- ISO/IEC 38507 : Gouvernance de l'IA
- ISO/IEC 25059 : Qualité des systèmes d'IA
- ISO/IEC 27090 : Mesures de sécurité pour l'IA
- Articulation avec ISO 27001

1.B.3.5 Référentiels et guides sectoriels

- ANSSI
- ENISA : bonnes pratiques de sécurité de l'IA
- NIST AI Risk Management Framework (AI RMF)

- ISACA : AI Audit Framework
- CSA AI Safety Initiative et Cloud Controls Matrix for AI

1.B.3.6 Responsabilités et qualification des acteurs

- Fournisseur vs déployeur
- Impacts juridiques selon le niveau de risque du SIA
- Responsabilités administrative, contractuelle et pénale (vue d'ensemble)
- Chaîne d'approvisionnement IA : dépendances critiques, responsabilité en cas de défaillance
- Interconnexions → propagation des risques

1.B.3.7 Outil pratique

- **T.P. Checklist juridique : questions clés à se poser face à un SIA**

Jour 2 - Matin

2.A.1 Gestion des risques de l'Intelligence Artificielle

2.A.1.1 Exercice pratique d'évaluation des risques IA / étude de cas

2.A.1.2 État de la menace portant sur les systèmes d'IA

- Reprendre publication ANSSI (février 2026)

2.A.1.3 Typologie d'attaques

- Empoisonnement / Extraction / Évasion
- Focus sur les attaques par injection de prompt
- OWASP Top 10 for LLM : Utiliser ce référentiel pour sécuriser les applications basées sur des modèles de langage
- MITRE ATLAS

2.A.1.4 Vulnérabilités courantes des systèmes d'IA

Jour 2 – Après-midi

2.B.1 Gestion des risques de l'Intelligence Artificielle (suite)

2.B.1.1 Scénarios de risques génériques les plus majeurs

2.B.2 Méthodologie d'analyse de risques applicable

- ISO 27005 / EBIOS RM
- Normes du CEN/CENELEC

Adaptation des méthodes classiques aux spécificités de l'IA :

- Prise en compte du cycle de vie des systèmes d'IA
- Intégration des risques liés aux données, aux modèles et à la chaîne d'approvisionnement
- Articulation entre risques techniques, juridiques et éthiques

Articulation avec le cadre réglementaire :

- Intégration des exigences du AI Act dans la démarche d'analyse de risques
- Cohérence avec la gestion des risques IA au sens de l'ISO/IEC 23894
- Alignement avec les obligations de documentation, de supervision humaine et de gestion des incidents

2.B.3 Risques spécifiques aux systèmes d'IA : lecture technique, juridique et éthique

- Risques liés aux modèles de langage (LLM) : Opacité des modèles : limites d'explicabilité / obligation de supervision humaine (AI Act) / enjeux de responsabilité en cas de décision contestée
- Hallucinations : production d'informations erronées ou trompeuses / risques décisionnels, juridiques et réputationnels / nécessité de mécanismes de validation et de reprise de contrôle humain
- Risques liés aux modes de déploiement : Cloud / API / On-premise
- Autres risques

Jour 3 - Matin

3.A.1 Gouvernance de la sécurité de l'IA

3.A.1.1 Stratégie et organisation

- Positionnement de la sécurité de l'IA dans l'organisation
- Rôles et responsabilités : RSSI, DPO, Chief AI Officer, AI Ethics Officer
- Comitologie : comité IA, instances de gouvernance
- Alignement avec la stratégie d'entreprise et la stratégie SSI

3.A.1.2 Politique de Sécurité des Systèmes d'Information et IA

- Intégration de l'IA dans la PSSI existante
- Politique de sécurité spécifique à l'IA (PSSI-IA)
- Articulation avec les autres politiques (données, cloud, etc.)
- Principes directeurs et exigences minimales

3.A.1.3 Corpus documentaire

- Charte d'utilisation de l'IA
- Charte éthique de l'IA (Rôle stratégique et décisionnel)
- Procédures opérationnelles : validation, déploiement, retrait
- Guide des bonnes pratiques utilisateurs
- Registre des systèmes d'IA
- Questionnaire cadrage projet (en amont de l'AR)
- **T.P. : Cas pratique avec rédaction d'une politique ou charte (sécu) IA**

3.A.1.4 Cadre de gouvernance IA de confiance

- Principes d'une IA responsable
- Supervision humaine des décisions
- Documentation et transparence
- Mécanismes de contrôle et de surveillance continue
- Éthique comme outil d'arbitrage et de gestion des risques
- Arbitrer entre : performance / explicabilité ou automatisation / supervision
- Cas réels d'arbitrage

3.A.1.5 Indicateurs et pilotage

- Définition des KPI spécifiques à l'IA
- Tableaux de bord sécurité IA
- Reporting à la direction et aux instances de gouvernance

Jour 3 – Après-midi

3.B.1 Sécurité de l'IA et gestion de projet

Intégration de la sécurité dans les projets IA

- Security by design pour l'IA
- Privacy by design et by default
- Points de contrôle sécurité dans le cycle projet
- Rôle du RSSI dans les projets IA

Évaluation des projets IA

- Analyse de risques projet
- Évaluation d'impact (AIPD / FRIA)
- Critères de validation sécurité
- Comité de validation des projets IA : les critères concrets - pourquoi dire non ?

3.B.2 Sécurité de l'IA et ressources humaines

Programme de sensibilisation à l'IA

- Objectifs et enjeux de la sensibilisation
- Publics cibles : collaborateur, dirigeants, métiers, IT, développeurs
- Messages clés par population
- Risques liés aux usages non maîtrisés (Shadow AI)
- Exemple : le protocole « Think First, Verify Always »
- Dilemmes éthiques concrets

Modalités de sensibilisation

- Formats : e-learning, ateliers, serious games, communications
- Cas pratiques et mises en situation
- Campagnes de sensibilisation aux risques IA (prompt injection, fuites de données)
- Évaluation de l'efficacité des actions

Formation et compétences

- Montée en compétences des équipes sécurité sur l'IA
- Formation des développeurs à la sécurité de l'IA
- Autres besoins de formations

3.B.3 Sécurité de l'IA et relations contractuelles

- Cartographie des prestataires IA
- Clauses contractuelles essentielles
- Transfert et partage de responsabilité
- Gestion de la relation fournisseur
- Points d'attention

3.B.4 Résilience des systèmes d'IA

- Définition de l'« incident grave » au sens de l'AI Act
- Comparaison avec : incident NIS2 / violation de données RGPD / incident DORA
- Articulation des obligations de notification : autorités compétentes / délais / périmètres
- Spécificité du besoin de redondance des systèmes d'IA

Jour 4 - Matin

4.A.1 Cas pratique (global)

4.A.2 Rappel des concepts fondamentaux / Questions / Retex à chaud

Jour 4 – Après-midi

4.B.1 Examen de certification