

Sessions garanties disponibles

Formation IA et sécurité en entreprise : enjeux, risques et bonnes pratiques

Réf. SF34433

Maîtrisez les risques de l'IA et des LLM pour protéger vos données, vos modèles et votre organisation !

2 j Durée	2 100 € HT Inter / participant	4 000 € HT Intra (≤12 pers.)	13 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Identifier les risques et scénarios d'attaque pertinents pour un cas d'usage IA/LLM de l'entreprise
- ✓ Concevoir une charte d'usage de l'IA générative pour son organisation
- ✓ Analyser l'architecture d'une application IA pour cartographier la surface d'attaque et localiser les points de contrôle de sécurité critiques
- ✓ Élaborer un mini-plan de gestion des risques IA pour un projet donné, aligné sur les exigences RGPD et IA Act
- ✓ Appliquer des mesures de security-by-design à un cas pratique de projet IA ou d'IA générative

Public visé & prérequis

Public visé Chefs de projet, Directeurs de projet, DSI, Product Owners, Responsables de la sécurité des systèmes d'information (RSSI), Responsables métier

Prérequis Connaissances générales des systèmes d'information (réseaux, applications, API, cloud...) et des principes de base de la cybersécurité. Notions fondamentales en data / IA.

Programme détaillé

Panorama de l'IA en entreprise et enjeux de sécurité

Rappels sur l'IA, le machine learning, les LLM et les architectures types d'applications IA
Cartographie des actifs et dépendances d'un système IA : données, modèles, services cloud, outils MLOps
Enjeux business, éthiques et réglementaires (RGPD, IA Act, NIS2, ISO 42001) pour l'adoption de l'IA
Introduction aux principaux cadres de risques IA et aux bonnes pratiques de l'écosystème (OWASP, MITRE, NIST, ENISA)
Méthodes pédagogiques : exposés interactifs, quiz de positionnement, échanges sur les cas des participants

Activités pratiques :

Cartographie rapide d'un cas d'usage IA réel des participants en identifiant actifs, parties prenantes et dépendances
Mini diagnostic collectif des enjeux de sécurité et de conformité associés à ces cas d'usage

Menaces, vulnérabilités et scénarios d'attaque sur les systèmes IA et LLM

Typologie des menaces sur l'IA : prompt injection, data poisoning, model stealing, membership inference, biais exploités
Attaques sur les chaînes de traitement : ingestion de données, entraînement, déploiement, monitoring
Exemples concrets de mésusages et incidents publics impliquant l'IA générative
Lecture guidée des référentiels OWASP Top 10 LLM, MITRE ATLAS, NIST Adversarial ML
Méthodes pédagogiques : décryptage de cas réels, jeu de menaces, travail en sous-groupes

Activités pratiques :

Atelier de construction d'une fiche scénario d'attaque IA à partir d'un cas d'usage métier (acteurs, vecteurs, impacts)
Exercice de classification de scénarios dans les taxonomies OWASP et MITRE et priorisation des risques associés

Sécuriser l'architecture IA : security by design, MLOps et LLMOps

Patrons d'architecture sécurisée pour applications IA et IA générative (front, API, modèles, data lake, outils MLOps)
Principes de security by design appliqués à l'IA : moindre privilège, cloisonnement, journalisation, supervision
Sécurité des données et des modèles : anonymisation, chiffrement, gestion de secrets, watermarking, segmentation des jeux de données
Sécurisation des pipelines MLOps et LLMOps : intégrité des modèles, gestion des versions, contrôles d'accès, surveillance des dérives
Protection des endpoints IA : filtrage d'entrées, validation de prompts, détection d'abus et de comportements anormaux
Méthodes pédagogiques : walkthrough d'architectures de référence, discussions techniques guidées, matrices de contrôles

Activités pratiques :

Atelier de revue d'architecture : analyse d'un schéma d'application IA, identification de la surface d'attaque et des points de contrôle
Construction d'une check-list de mesures security by design à appliquer à un projet IA de l'entreprise
Simulation de périmètre de monitoring et de journaux nécessaires pour investiguer un incident lié à un modèle ou un LLM

Gouvernance, conformité et charte d'usage de l'IA générative

Rappels RGPD, IA Act, NIS2 et normes ISO applicables aux systèmes IA et LLM
Principes d'IA responsable : transparence, explicabilité, gestion des biais, contrôle humain
Éléments indispensables d'une charte d'usage de l'IA générative : cas d'usage autorisés, contenus interdits, données sensibles, validation humaine
Organisation de la gouvernance IA : rôles CAIO, RSSI, DPO, métiers, comités IA
Indicateurs et tableaux de bord pour suivre les usages IA, les incidents et la conformité
Méthodes pédagogiques : canevas de charte, retours d'expérience, débats argumentés

Activités pratiques :

Co-construction en sous-groupes d'une première version de charte IA générative à partir d'un modèle fourni
Cartographie des rôles et responsabilités autour d'un cas d'usage IA et définition des points de contrôle humain (human in the loop)
Exercice d'analyse d'un cas d'usage limite pour décider s'il est acceptable, conditionnel ou interdit et justifier la décision

Plan de gestion des risques IA et feuille de route de sécurisation

Étapes clés d'une analyse de risques IA : contexte, événements redoutés, scénarios, mesures existantes, plan d'actions
Utilisation pragmatique des cadres NIST AI RMF, EBIOS RM, ISO 42001 pour les projets IA
Typologie de mesures : techniques (contrôles, monitoring, red teaming) et organisationnelles (politiques, formation, audits)
Construction d'une feuille de route IA sécurisée et réaliste pour l'entreprise
Méthodes pédagogiques : atelier guidé, travail en équipes, restitution collective

Activités pratiques :

Atelier de mini analyse de risques IA sur un cas d'usage apporté par les participants ou fourni par le formateur
Élaboration en groupe d'un plan de traitement des risques avec priorisation, responsables et indicateurs de succès
Synthèse individuelle : rédaction d'une courte feuille de route de sécurisation IA à ramener dans son organisation

Prochaines sessions

DATE	LIEU	STATUT
09/11/2026	à distance	Sur confirmation
20/01/2027	Lyon	Sur confirmation
20/01/2027	Aix-en-Provence	Sur confirmation
20/01/2027	Grenoble	Sur confirmation
20/01/2027	à distance	Sur confirmation
04/05/2027	Paris	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 7 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Camilo R. — Formateur IA générative & Intelligence artificielle

Camilo intervient sur des formations portant sur l'IA appliquée aux métiers et sa gouvernance. Les sujets abordés incluent notamment l'intelligence artificielle. Son activité de formation a débuté en 2024.

Ils nous font confiance

Cette année notre filière Gouvernance, Risques & Conformité (GRC) a accompagné plus de 21 entreprises dont :

AVEM MÉTROPOLE DE LYON ADISTA ALSTOM ASTEK FRANCE AXA ASSISTANCE FRANCE ECONOCOM SERVICES & SOLUTION EGIS ENSSIB EURIDICE DEVELOPPEMENT +11 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com