Auditer un système IA générative sur le plan technique et réglementaire

Référence: AUD-IA-501

Tarif:
1700 € Net de taxes par bénéficiaire

Durée :
2 jours (14h) en présentiel / distanciel

Effectif:
4 à 8 participants

Niveau et public:
La formation et la certification s'adressent aux architectes IA, consultants en transformation digitale, auditeurs IT, responsables conformité, experts cybersécurité et cabinets de conseil souhaitant utiliser l'Intelligence Artificielle pour analyser, sécuriser et optimiser les systèmes d'information, afin de renforcer la conformité, maîtriser les risques et accélérer la transformation digitale.

Pré-requis :
·Maîtriser les bases d'architecture LLM et RAG
·Comprendre les systèmes multi-agents
·Connaître les principes du AI Act
·Avoir une expérience en architecture ou audit IT

Modalités :
Formation en présentiel ou à distance, théorie et travaux pratiques.

Délais d'accès:
Inscription jusqu'à 7 jours avant la session (selon la disponibilité).

Accessibilité:
Adaptation possible pour les personnes en situation de handicap.

Contact:
iazen@iazenconsulting.onmicrosoft.com
+33 6 23 37 13 91

Programme 2026, mis à jour le 25/02/2026

Objectif général:

➢ Former des experts capables de réaliser un audit complet d'un système d'intelligence artificielle générative, en évaluant sa robustesse technique, sa sécurité, sa gouvernance et sa conformité au AI Act, afin de produire un rapport structuré, exploitable et professionnel.

Objectifs pédagogiques:

À l'issue de la formation, le participant sera capable de :

➢ Cartographier un système IA générative complexe
➢ Analyser une architecture LLM / RAG / multi-agents
➢ Analyser une architecture LLM / RAG / multi-agents
➢ Évaluer les risques d'hallucination, dérive et biais
➢ Vérifier la conformité au AI Act
➢ Analyser la documentation et la traçabilité
➢ Évaluer les mécanismes de supervision humaine
➢ Rédiger un rapport d'audit structuré et argumenté

Compétences visées :

- Audit d'architecture IA
- Analyse de robustesse LLM et RAG
- Évaluation de systèmes agentiques
- Audit de conformité réglementaire IA
- Analyse multi-dimensionnelle des risques
- Rédaction de rapport d'audit professionnel

Programme détaillé:

Jour 1 – Audit technique approfondi d'un système IA

1. Cartographier un système IA générative

- Identifier les composants clés :
  → Modèle LLM
  → Pipeline RAG
  → Base vectorielle
  → Agents et outils
- Analyser les flux de données
- Identifier les dépendances fournisseurs
- Cartographier les interactions avec le SI
- Structurer une vue d'architecture audit exploitable

Cas pratique : Rédaction d'un plan d'intégration et d'une feuille de route tenant compte des contraintes organisationnelles et techniques de l'entreprise.

Auditer un système IA générative sur le plan technique et réglementaire

Formateur :

Amel Mhamdi est Data Scientist Senior et Architecte en IA, spécialisée dans les systèmes multi-agents et les modèles de langage (LLM). Elle possède plus de 10 ans d'expérience dans la conception de solutions d'intelligence artificielle, les architectures distribuées et le déploiement de projets data à fort impact. Experte en LangChain, en RAG, en IA générative et en orchestration d'agents, elle accompagne également des missions de conseil et de formation.

Modalités d'évaluation :

·Évaluation continue via ateliers
·Validation du plan de gouvernance conçu
·Questionnaire de validation des acquis
·Attestation de fin de formation délivrée

Processus de candidature :

Analyse du dossier de candidature, entretien de positionnement et validation des prérequis.

Moyens pédagogiques et techniques :

Supports pédagogiques, démonstrations, cas pratiques et environnement de développement (Python, LLM, LangChain).

Indicateurs de résultat :

Taux de satisfaction et de réussite, avec évaluation des compétences acquises en fin de formation.

2. Évaluer la robustesse du système

- Tester la cohérence des réponses générées
- Identifier les risques d'hallucination
- Analyser la gestion des erreurs
- Tester la stabilité sur requêtes répétées
- Évaluer la qualité des sorties structurées

3. Identifier les vulnérabilités techniques

- Prompt injection
- Jailbreak et contournements
- Escalade d'outils agentiques
- Data leakage
- Risques liés aux embeddings et bases vectorielles
- Mauvaise isolation des outils

4. Examiner la gestion des données

- Origine des données
- Politique de conservation
- Données sensibles injectées dans les prompts
- Journalisation des requêtes
- Journalisation des requêtes

Atelier 1 – Diagnostic technique structuré

Étude de cas réaliste :

- ·Analyse d'une architecture fournie
- ·Identification des failles
- ·Priorisation des risques
- ·Construction d'une grille d'évaluation

Restitution collective avec posture d'auditeur.

Jour 2 – Audit réglementaire & production du rapport

5. Vérifier la conformité au AI Act

- Qualification du niveau de risque
- Identification des obligations applicables
- Vérification de la documentation technique
- Examen du registre IA
- Évaluation des exigences de transparence

Auditer un système IA générative sur le plan technique et réglementaire

7. Analyser la gouvernance IA

- Rôles et responsabilités définis
- Existence d'un comité IA
- Procédures internes formalisées
- Mécanismes de mise à jour du système
- Gestion des incidents IA

8. Évaluer l'explicabilité et la traçabilité

- Présence de logs exploitables
- Capacité de justification d'une décision
- Documentation des modèles utilisés
- Transparence vis-à-vis des utilisateurs
- Archivage des preuves

9. Structurer un rapport d'audit professionnel

- Rédiger une synthèse exécutive
- Formaliser les constats techniques
- Classer les non-conformités
- Structurer une matrice de criticité
- Proposer un plan d'actions priorisé
- Présenter des recommandations argumentées

Projet final – Audit simulé complet

Les participants réalisent :

- Cartographie du système
- Analyse technique
- Analyse conformité AI Act
- Matrice de risques
- Rapport d'audit structuré

Présentation finale avec posture cabinet conseil.

Méthodes pédagogiques

- Alternance théorie / pratique (40 % / 60 %)
- Études de cas réalistes
- Simulation d'audit
- Travail en sous-groupes
- Revue critique collective
- Coaching sur posture d'auditeur

Livrables remis aux participants

Les participants conçoivent :

- Support complet AI Act structuré
- Modèle de registre IA prêt à utiliser
- Modèle de fiche de classification
- Matrice de cartographie des risques IA
- Template de dossier de conformité
- Checklist supervision humaine
- Modèle de plan de gouvernance IA