

Mis à jour le 26/10/2026

S'inscrire

Formation Certification ISO/IEC 27090 Lead Implementer

5 jours (35 heures)

Présentation

ISO/IEC 27090:2026 fournit des recommandations pour identifier, détecter et atténuer les menaces propres aux systèmes d'intelligence artificielle. De la collecte des données au réentraînement des modèles, ce référentiel accompagne la protection du cycle de vie de l'IA et complète les pratiques de cybersécurité existantes. (iso.org)

Notre Formation Certification ISO/IEC 27090 Lead Implementer vous prépare à la certification officielle AI Security (ISO/IEC 27090:2026) Lead Implementer (ITC-230) délivrée par ITCERTS, qui valide des connaissances avancées en sécurité de l'IA. (itcerts.ca)

Vous apprendrez à analyser les scénarios de compromission, à protéger les données et les modèles, puis à sélectionner des mesures de détection et de protection adaptées aux architectures étudiées.

À l'issue de la formation, vous serez en mesure de construire un plan de sécurisation opérationnel, de justifier vos arbitrages et de vérifier les protections déployées grâce à des ateliers et des évaluations ciblées.

La préparation associe études de cas, révisions et examen blanc. Elle distingue la certification individuelle des recommandations de la norme, qui ne constituent pas des exigences de certification organisationnelle. (iso.org)

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Analyser les menaces et les surfaces d'attaque sur l'ensemble du cycle de vie de l'IA
- Évaluer les scénarios de compromission des données et des modèles
- Mettre en œuvre des protections multicouches adaptées aux risques identifiés
- Vérifier l'efficacité des mesures et leurs interactions à partir de tests documentés
- Organiser la surveillance et la réponse aux incidents propres aux systèmes IA
- Préparer l'examen à partir de cas pratiques et de questions d'entraînement

Public visé

- Architecte cybersécurité
- Responsable de la sécurité des systèmes d'information
- Ingénieur Machine Learning
- Ingénieur MLOps
- Consultant en sécurité de l'IA

Pré-requis

- Expérience en cybersécurité, analyse de risques ou sécurisation des applications
- Compréhension des principes du Machine Learning et des étapes d'entraînement et d'inférence
- Connaissance des contrôles d'accès, de la journalisation et de la protection des données
- Capacité à interpréter une architecture technique et des résultats de tests de sécurité
- Compréhension de l'anglais technique pour exploiter les ressources de préparation

Pré-requis techniques

- Ordinateur équipé de Windows 11 ou Ubuntu 24.04 LTS avec processeur quatre cœurs et 8 Go de mémoire vive minimum
- Navigateur Firefox ou Chrome à jour et lecteur de documents PDF
- Connexion Internet stable autorisant l'accès à la plateforme pédagogique et aux laboratoires distants
- Accès nominatif aux environnements de laboratoire préparés pour les ateliers, sans carte graphique dédiée ni compte cloud personnel requis
- Webcam, microphone et espace calme à prévoir pour le passage de l'examen télésurveillé, sous réserve de validation des exigences du prestataire

Programme de notre formation ISO/IEC 27090 Lead Implementer

[Jour 1 - Matin]

Référentiel et périmètre de sécurisation

- Positionnement de la Formation Certification ISO/IEC 27090 Lead Implementer et organisation de la préparation

- Lecture du périmètre ISO/IEC 27090:2026 et distinction entre recommandations, exigences et certification individuelle
- Terminologie des systèmes IA, des données, des modèles et des processus d'apprentissage
- Décomposition du cycle de vie, de la conception au retrait du service
- Atelier pratique : Cartographier un système IA fil rouge, ses actifs critiques et les responsabilités associées à chaque phase.

[Jour 1 - Après-midi]

Gouvernance et modélisation des menaces

- Articulation de la gouvernance IA avec la sécurité de l'information et la gestion des risques
- Identification des adversaires, capacités d'accès et frontières de confiance
- Construction de scénarios de compromission et appréciation des impacts métier
- Application des principes Zero Trust et de défense en profondeur aux architectures IA
- Priorisation des risques et préparation de questions d'entraînement contextualisées
- Atelier pratique : Produire un modèle de menaces et hiérarchiser les protections du système fil rouge.

[Jour 2 - Matin]

Protection des données et de l'apprentissage

- Analyse de la provenance des données, des transformations et des droits d'accès
- Scénarios d'empoisonnement des données et introduction de portes dérobées
- Contrôles d'intégrité, validation des sources et séparation des jeux de données
- Détection d'anomalies et qualification des signaux de contamination
- Protection des données collectées en production avant leur réutilisation pour le réentraînement
- Atelier pratique : Analyser un jeu de données altéré et configurer une chaîne de contrôles avant entraînement.

[Jour 2 - Après-midi]

Intégrité des modèles et chaîne d'approvisionnement

- Analyse de l'empoisonnement direct des modèles et des modifications non autorisées des paramètres
- Évaluation des modèles tiers, dépendances et composants de la chaîne d'approvisionnement
- Durcissement des environnements de développement et des pipelines de livraison
- Gestion des secrets, séparation des privilèges et protection du registre de modèles
- Vérification de provenance, traçabilité des versions et critères d'acceptation des artefacts
- Atelier pratique : Sécuriser la promotion d'un modèle et bloquer un artefact dont l'intégrité ne peut pas être établie.

[Jour 3 - Matin]

Évasion et confidentialité des modèles

- Analyse des attaques par évasion et des perturbations des entrées à l'inférence
- Scénarios d'exfiltration de modèle et d'extraction par interrogation
- Distinction entre inférence d'appartenance et inversion de modèle
- Réduction de l'exposition des sorties, contrôle des requêtes et détection des usages abusifs
- Évaluation des compromis entre confidentialité, robustesse, précision et disponibilité
- Atelier pratique : Tester une interface d'inférence isolée et comparer les protections contre l'évasion et les requêtes d'extraction.

[Jour 3 - Après-midi]

Sécurité des interfaces génératives

- Analyse des injections de prompt directes et indirectes dans les flux applicatifs
- Protection des données sensibles et maîtrise des sorties du modèle
- Traitement des sorties contenant des instructions ou des charges d'injection
- Séparation entre instructions et contenus non fiables dans les architectures RAG
- Restriction des outils, validation des actions et limitation des privilèges des agents
- Atelier pratique : Exploiter une injection indirecte dans un assistant de laboratoire puis déployer et retester des protections applicatives.

[Jour 4 - Matin]

Validation des protections et interactions

- Construction d'une matrice menaces, détections et mesures de protection
- Analyse des complémentarités, conflits et angles morts entre mesures
- Définition d'un protocole de red teaming autorisé et reproductible
- Mesure de l'efficacité des protections et qualification des faux positifs et faux négatifs
- Évaluation du risque résiduel et justification des arbitrages de mise en production
- Atelier pratique : Exécuter une campagne de tests adversariaux et documenter les interactions entre trois protections.

[Jour 4 - Après-midi]

Surveillance et réponse aux incidents IA

- Conception de la journalisation des accès, versions, entrées et événements sensibles
- Détection des comportements malveillants et distinction avec la dérive ou une dégradation ordinaire
- Définition des alertes, seuils et procédures de qualification des incidents
- Confinement, conservation des preuves et retour à une version maîtrisée
- Réévaluation des protections lors des mises à jour, réentraînements et opérations de retrait

- Atelier pratique : Traiter un incident de compromission, isoler les éléments affectés et préparer une reprise sécurisée.

[Jour 5 - Matin]

Cas intégrateur et préparation ciblée

- Consolidation du plan de sécurisation sur l'ensemble du cycle de vie
- Formalisation des responsabilités, preuves de contrôle et critères de réévaluation
- Révision du périmètre, de la terminologie et de l'application de la sécurité de l'information
- Entraînement à la qualification des compromissions et au choix des mesures adaptées
- Analyse des distracteurs et justification des réponses dans des questions scénarisées
- Atelier pratique : Présenter un dossier de sécurisation complet et défendre les choix de protection devant un comité simulé.

[Jour 5 - Après-midi]

Examen blanc et préparation au passage

- Synthèse des points critiques et révision des confusions terminologiques
- Méthode de lecture des questions et gestion du temps
- Préparation administrative et technique au passage de l'examen officiel
- Construction d'un plan de révision individuel et organisation du passage proposé
- Atelier pratique : Réaliser un examen blanc chronométré, analyser les réponses et définir les actions de remédiation avant l'examen officiel.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.