Confidential Computing pour l'IA : Enclaves Sécurisées, Chiffrement Homomorphe et Calcul Multipartite

Lien : https://innov-systems.com/formation/confidential-computing-pour-lia-enclaves-securisees-chiffrement-homomorphe-et-calcul-multipartite

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI155

CATÉGORIE
Sécurité de l'Intelligence Artificielle

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes du confidential computing appliqué à l’IA
- Maîtriser les enclaves sécurisées (TEE) et leur fonctionnement
- Exploiter le chiffrement homomorphe pour le calcul sur données sensibles
- Concevoir des systèmes IA utilisant le calcul multipartite sécurisé (MPC)
- Renforcer la sécurité des pipelines de machine learning
- Déployer des modèles IA dans des environnements isolés et sécurisés
- Réduire les risques de fuite de données en exécution
- Intégrer les technologies de confidential computing dans le cloud
- Optimiser les performances des systèmes sécurisés
- Assurer la conformité réglementaire des solutions IA
- Développer des architectures IA hautement sécurisées
- Étudier des cas concrets d’implémentation industrielle

POUR QUI ?

- Ingénieurs IA
- Data scientists
- Machine learning engineers
- Architectes cloud
- Cybersecurity engineers
- Cryptographes appliqués
- DevSecOps engineers
- Consultants en sécurité des données
- Responsables conformité (DPO, RSSI)
- Chercheurs en IA et sécurité
- Développeurs backend avancés
- Toute personne impliquée dans la conception de systèmes IA sécurisés

Innov Systems

Programme détaillé

1 / Introduction au Confidential Computing pour l'IA

- Définition du confidential computing
- Enjeux de sécurité des données en exécution
- Cas d'usage en IA sensible (finance, santé, défense)

2 / Fondements cryptographiques et sécurisation du calcul

- Principes du chiffrement des données au repos, en transit et en usage
- Limites des approches classiques de sécurité
- Introduction aux modèles de calcul sécurisé

3 / Enclaves sécurisées (Trusted Execution Environments - TEE)

- Fonctionnement des enclaves matérielles
- Intel SGX, AMD SEV et alternatives cloud
- Isolation des processus et protection mémoire

4 / Chiffrement homomorphe

- Principe du calcul sur données chiffrées
- Types de chiffrement homomorphe (partiel, total)
- Cas d'usage et limites de performance

5 / Calcul multipartite sécurisé (MPC)

- Principe du secret partagé
- Protocoles de calcul distribué sécurisé
- Applications collaboratives inter-organisations

Innov Systems

6 / Architectures IA basées sur le confidential computing

- Intégration dans les pipelines machine learning
- IA distribuée sécurisée
- Orchestration des environnements sécurisés

7 / Outils et plateformes cloud de confidential computing

- Services cloud sécurisés (AWS, Azure, GCP)
- SDKs et frameworks spécialisés
- Déploiement d’applications IA sécurisées

8 / Performance et contraintes techniques

- Latence et overhead de chiffrement
- Optimisation des calculs sécurisés
- Compromis sécurité vs performance

9 / Gouvernance, conformité et risques

- Réglementations sur la protection des données
- Auditabilité des environnements sécurisés
- Gestion des menaces avancées

10 / Études de cas et implémentations pratiques

- IA sécurisée en environnement bancaire et médical
- Implémentation d’un pipeline confidentiel end-to-end
- Bonnes pratiques industrielles

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 11 Déc. 2026	Distanciel
25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés