Sécurité Offensive et Défensive des Pipelines de Données Massives (Data Poisoning, Model Stealing, Membership Inference)

Lien : https://innov-systems.com/formation/securite-offensive-et-defensive-des-pipelines-de-donnees-massives-data-poisoning-model-stealing-membership-inference

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI161

CATÉGORIE
Sécurité de l'Intelligence Artificielle

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les menaces sur les pipelines de données massives
- Identifier les attaques de type data poisoning, model stealing et membership inference
- Maîtriser les techniques de sécurité offensive et défensive
- Sécuriser les pipelines de données et modèles IA
- Détecter et prévenir les attaques adversariales
- Mettre en place des mécanismes de protection des modèles
- Renforcer la robustesse des systèmes IA
- Surveiller les comportements anormaux dans les pipelines
- Appliquer les bonnes pratiques de cybersécurité IA
- Protéger la confidentialité des données sensibles
- Évaluer les risques de sécurité des systèmes data
- Étudier des cas réels d’attaques et de défense IA

POUR QUI ?

- Ingénieurs cybersécurité
- Data scientists
- Machine learning engineers
- Security engineers
- Architectes data
- DevSecOps engineers
- Consultants en cybersécurité
- Responsables sécurité des systèmes d’information
- Chief information security officers (CISO)
- Chefs de projet IA et data
- Toute personne impliquée dans la sécurité des systèmes IA et data

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des pipelines de données

- Définition des pipelines de données massives
- Enjeux de sécurité en data science et IA
- Panorama des menaces adversariales

2 / Architecture des pipelines de données

- Ingestion, traitement et stockage des données
- Points de vulnérabilité dans les flux data
- Chaîne de confiance des données

3 / Data Poisoning (empoisonnement de données)

- Principe des attaques par corruption de données
- Impacts sur l'entraînement des modèles
- Techniques de détection et mitigation

4 / Model Stealing (vol de modèle)

- Mécanismes d'extraction de modèles IA
- Attaques par requêtes et API
- Protection de la propriété intellectuelle des modèles

5 / Membership Inference Attacks

- Identification de données présentes dans le training set
- Risques pour la confidentialité des données
- Méthodes de prévention et anonymisation

Innov Systems

6 / Sécurité offensive des systèmes IA

- Simulation d’attaques adversariales
- Red teaming des modèles IA
- Évaluation de robustesse des pipelines

7 / Défense des pipelines de données

- Techniques de robustification des modèles
- Filtrage et validation des données
- Sécurisation des accès et API

8 / Monitoring et détection d’anomalies

- Détection de comportements suspects
- Logs et traçabilité des accès
- Systèmes d’alerte en temps réel

9 / Gouvernance et conformité sécurité IA

- Normes de cybersécurité appliquées à l’IA
- Gestion des risques et conformité
- Politiques de sécurité des données

10 / Études de cas et attaques réelles

- Analyse d’incidents de sécurité IA
- Simulation d’attaques sur pipelines
- Bonnes pratiques de défense industrielle

Inov 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

04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca
16 au 20 Août 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