Sécuriser Copilot et les Agents IA en Entreprise

Lien : https://innov-systems.com/formation/securiser-copilot-et-les-agents-ia-en-entreprise

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI194

CATÉGORIE
Sécurité de l'Intelligence Artificielle

OBJECTIFS DE LA FORMATION

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

- Comprendre les risques de sécurité liés aux copilots et agents IA
- Mettre en place une architecture sécurisée pour les agents IA
- Protéger les données sensibles utilisées par les systèmes IA
- Sécuriser les interactions utilisateurs et les prompts
- Gérer les identités et accès des agents IA
- Contrôler les connecteurs et intégrations externes
- Mettre en œuvre des politiques de gouvernance IA
- Détecter et prévenir les attaques sur les systèmes IA
- Assurer la conformité réglementaire des solutions IA
- Superviser les comportements des agents en production
- Réduire les risques liés à l'IA générative en entreprise
- Étudier des cas concrets de sécurisation de copilots IA

Innov Systems

POUR QUI ?

- Security Engineers
- DevSecOps Engineers
- Cloud Security Architects
- AI Engineers
- Machine Learning Engineers
- MLOps Engineers
- DevOps Engineers
- Software Engineers
- SRE (Site Reliability Engineers)
- RSSI / CISO
- Consultants cybersécurité
- Architectes SI
- Toute personne impliquée dans la sécurité des systèmes IA en entreprise

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des copilots et agents IA

- Enjeux de sécurité des systèmes d'IA générative en entreprise
- Différence entre copilots, agents IA et applications LLM
- Surface d'attaque spécifique aux systèmes IA

2 / Architecture sécurisée des agents IA

- Composants d'un agent IA en production
- Orchestration des modèles et outils connectés
- Isolation des environnements d'exécution

3 / Gestion des identités et des accès (IAM)

- Authentification et autorisation des agents IA
- Microsoft Entra ID et RBAC
- Principe du moindre privilège

4 / Protection des données et confidentialité

- Classification des données sensibles
- Prévention des fuites de données (DLP)
- Chiffrement des données au repos et en transit

5 / Sécurisation des prompts et des interactions

- Prompt injection et attaques adversariales
- Filtrage et validation des entrées utilisateurs
- Guardrails et politiques de sécurité IA

Innov Systems

6 / Sécurité des outils et connecteurs

- Contrôle des accès aux APIs et plugins
- Gestion des secrets et tokens
- Sécurisation des intégrations tierces

7 / Gouvernance des agents IA en entreprise

- Cycle de vie des agents IA
- Validation et approbation des agents
- Politiques d’utilisation et conformité

8 / Monitoring et détection des comportements anormaux

- Observabilité des agents IA
- Logging des interactions et audit
- Détection des abus et dérives

9 / Conformité et cadre réglementaire

- RGPD et IA Act (Europe)
- Exigences de conformité pour les systèmes IA
- Traçabilité et explicabilité des décisions

10 / Cas pratiques et mise en œuvre sécurisée

- Sécurisation d’un copilote en environnement enterprise
- Mise en place de guardrails IA
- Bonnes pratiques de production

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

30 Nov. au 04 Déc. 2026	Distanciel
01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 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