Sécurisation des API d'IA et des Endpoints d'Inférence ; Authentification, Rate Limiting et Détection d'Abus

Lien : https://innov-systems.com/formation/securisation-des-api-dia-et-des-endpoints-dinference-authentification-rate-limiting-et-detection-dabus

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI159

CATÉGORIE
Sécurité de l'Intelligence Artificielle

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les risques de sécurité liés aux API d’IA
- Maîtriser les mécanismes d’authentification et d’autorisation
- Mettre en place des stratégies efficaces de contrôle d’accès
- Configurer le rate limiting et la gestion des quotas
- Détecter et prévenir les abus sur les endpoints d’inférence
- Sécuriser les échanges et les données sensibles
- Identifier les attaques spécifiques aux systèmes d’IA
- Mettre en œuvre une surveillance continue des API
- Renforcer la résilience des infrastructures IA
- Développer une approche DevSecOps appliquée à l’IA
- Concevoir des architectures sécurisées pour les services d’inférence
- Étudier des cas concrets de sécurisation d’API IA

POUR QUI ?

- Ingénieurs IA
- Développeurs backend et API
- Architectes logiciels
- DevSecOps engineers
- Ingénieurs cybersécurité
- Responsables sécurité des systèmes d’information (RSSI)
- Architectes cloud
- Machine learning engineers
- Data engineers
- Consultants en cybersécurité
- Chefs de projet techniques
- Toute personne impliquée dans le déploiement et la sécurisation de services IA

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des API d’IA

- Enjeux de sécurité des services d’inférence IA
- Typologie des API d’IA et endpoints exposés
- Menaces spécifiques aux systèmes d’IA

2 / Architecture et surface d’attaque des API d’IA

- Identification des points d’exposition
- Analyse des flux de données
- Cartographie des risques applicatifs

3 / Authentification et contrôle d’accès

- API Keys, OAuth 2.0 et OpenID Connect
- Gestion des identités et des rôles
- Principes du moindre privilège

4 / Autorisation et gouvernance des accès

- Contrôle d’accès basé sur les rôles (RBAC)
- Contrôle d’accès basé sur les attributs (ABAC)
- Segmentation des utilisateurs et services

5 / Rate Limiting et protection contre les abus

- Limitation du nombre de requêtes
- Gestion des quotas et des pics de trafic
- Prévention du déni de service (DoS)

Innov Systems

6 / Détection d’anomalies et surveillance

- Monitoring des endpoints d’inférence
- Détection des comportements suspects
- Analyse des journaux et alertes

7 / Protection contre les attaques ciblant les modèles IA

- Prompt injection et attaques indirectes
- Extraction et vol de modèles
- Attaques d’empoisonnement et d’évasion

8 / Sécurisation des données et des échanges

- Chiffrement des communications (TLS)
- Protection des données sensibles
- Journalisation et traçabilité des accès

9 / Sécurité opérationnelle et réponse aux incidents

- Plan de réponse aux incidents
- Gestion des vulnérabilités
- Audits et tests de sécurité continus

10 / Études de cas et implémentations pratiques

- Sécurisation d’une API d’IA en production
- Mise en place d’une architecture résiliente
- Bonnes pratiques DevSecOps pour l’IA

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

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