Sécuriser et monitorer un écosystème MCP en production

Lien :
https://innov-systems.com/formation/securiser-et-monitorer-un-ecosysteme-mcp-en-production

DURÉE
4 jours (28h)

RÉFÉRENCE
BDI107

CATÉGORIE
IA Agentique et Systèmes Multi-Agents

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre l’architecture d’un écosystème MCP en production
- Sécuriser les communications et les flux de contexte
- Mettre en place une authentification et un contrôle d’accès robustes
- Assurer la traçabilité des actions dans un système MCP
- Surveiller les performances et la santé des systèmes IA
- Détecter les comportements anormaux ou malveillants
- Gérer efficacement les incidents de sécurité
- Implémenter des solutions de monitoring avancées
- Garantir la conformité et la gouvernance des systèmes MCP
- Réduire les risques liés aux systèmes multi-agents
- Optimiser la résilience des architectures MCP
- Étudier des cas concrets de production MCP

POUR QUI ?

- Ingénieurs IA
- Architectes systèmes
- DevOps engineers
- Security engineers
- Data engineers
- Machine learning engineers
- Administrateurs systèmes cloud
- SRE (Site Reliability Engineers)
- Consultants en cybersécurité
- Product managers techniques
- CTO et responsables IT
- Toute personne impliquée dans la production d’écosystèmes MCP

Innov Systems

Programme détaillé

1 / Introduction aux écosystèmes MCP en production

- Rôle du Model Context Protocol (MCP) dans les architectures IA
- Enjeux de production et de scalabilité
- Surface d’exposition des systèmes MCP

2 / Architecture d’un écosystème MCP sécurisé

- Composants d’un système MCP en production
- Flux de données et points critiques
- Design sécurisé by design

3 / Authentification et contrôle d’accès

- Gestion des identités et des permissions
- Authentification forte (API keys, OAuth, tokens)
- Segmentation des accès entre services MCP

4 / Sécurisation des échanges de contexte

- Chiffrement des communications
- Protection des données sensibles dans le contexte
- Validation et filtrage des entrées MCP

5 / Journalisation et traçabilité

- Logging des interactions MCP
- Audit des actions des agents et services
- Conservation et exploitation des logs

Innov Systems

6 / Monitoring des performances et de la santé du système

- Métriques clés (latence, erreurs, throughput)
- Observabilité des flux MCP
- Alerting et détection d’anomalies

7 / Détection des menaces et comportements anormaux

- Identification des accès suspects
- Analyse comportementale des agents
- Systèmes de détection d’intrusion

8 / Gestion des incidents et réponse opérationnelle

- Procédures de réponse aux incidents
- Isolation des composants compromis
- Plan de reprise et continuité de service

9 / Gouvernance et conformité des systèmes MCP

- Respect des standards de sécurité
- Politiques internes de gouvernance IA
- Conformité réglementaire et audit

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

01 au 04 Déc. 2026	Distanciel
09 au 12 Fév. 2027	Présentiel - Casablanca
06 au 09 Avr. 2027	Présentiel - Casablanca
01 au 04 Juin 2027	Présentiel - Casablanca
27 au 30 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

Innov Systems