IA au service de la cyberdéfense : détection des menaces et réponse automatisée

Lien : https://innov-systems.com/formation/ia-au-service-de-la-cyberdefense-detection-des-menaces-et-reponse-automatisee

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI201

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 de l'IA appliquée à la cybersécurité
- Détecter les menaces grâce au Machine Learning
- Identifier les comportements anormaux sur les réseaux et systèmes
- Exploiter les solutions SIEM, EDR, XDR et SOAR
- Automatiser les réponses aux incidents de sécurité
- Réduire les délais de détection et de remédiation
- Exploiter l'IA générative pour assister les équipes SOC
- Mettre en œuvre une gouvernance responsable de l'IA en cybersécurité
- Déployer des modèles IA robustes dans un environnement de production
- Améliorer la résilience des infrastructures numériques
- Renforcer les capacités de cyberdéfense des organisations
- Étudier des cas concrets de détection et de réponse automatisée

POUR QUI ?

- Analystes SOC
- Ingénieurs cybersécurité
- RSSI / CISO
- Ingénieurs réseaux et sécurité
- Architectes cybersécurité
- Experts SIEM, EDR, XDR et SOAR
- Data Scientists spécialisés en cybersécurité
- Ingénieurs Machine Learning
- Consultants en cybersécurité
- DevSecOps Engineers
- Responsables de la gestion des risques numériques
- Toute personne impliquée dans la détection, l'analyse et la réponse aux cybermenaces

Innov Systems

Programme détaillé

1 / Fondamentaux de l’IA appliquée à la cyberdéfense

- Concepts de l’intelligence artificielle en cybersécurité
- Évolution des cybermenaces et des mécanismes de défense
- Cas d’usage de l’IA dans les SOC modernes

2 / Collecte et analyse des données de sécurité

- Sources de données (logs, réseaux, endpoints, cloud)
- SIEM et centralisation des événements
- Préparation et enrichissement des données de sécurité

3 / Machine Learning pour la détection des menaces

- Détection d’anomalies comportementales
- Classification des attaques et menaces
- Modèles supervisés, non supervisés et semi-supervisés

4 / Détection des cyberattaques avancées

- Malware, ransomware et APT (Advanced Persistent Threats)
- Détection des attaques Zero-Day
- Analyse comportementale des utilisateurs (UEBA)

5 / IA pour le SOC et la Threat Intelligence

- Corrélation intelligente des événements
- Priorisation des alertes
- Intégration des flux de Cyber Threat Intelligence (CTI)

Innov Systems

6 / Réponse automatisée aux incidents (SOAR)

- Orchestration et automatisation des réponses
- Playbooks de remédiation
- Intégration avec les outils EDR, XDR et SIEM

7 / IA générative au service de la cybersécurité

- Assistance aux analystes SOC
- Génération et analyse de rapports d'incidents
- Automatisation des investigations et de la documentation

8 / Sécurité, gouvernance et IA responsable

- Gestion des faux positifs et faux négatifs
- Explicabilité des modèles IA (Explainable AI)
- Gouvernance, conformité et audit des systèmes IA

9 / Déploiement, supervision et amélioration continue

- Intégration de l'IA dans un SOC opérationnel
- Monitoring des performances des modèles
- MLOps appliqué à la cybersécurité

10 / Cas pratiques et exercices de cyberdéfense

- Détection d'une attaque en temps réel
- Automatisation de la réponse à un incident
- Bonnes pratiques et retours d'expérience

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

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 au 08 Oct. 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