Red Teaming augmenté par l'IA : techniques offensives de nouvelle génération

Lien : https://innov-systems.com/formation/red-teaming-augmente-par-lia-techniques-offensives-de-nouvelle-generation

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI203

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 du Red Teaming moderne et le rôle de l'IA
- Planifier et structurer des exercices de sécurité offensifs dans un cadre autorisé
- Utiliser l'IA pour améliorer l'analyse, la priorisation et la simulation de scénarios
- Évaluer la sécurité des applications et systèmes intégrant l'IA
- Concevoir des scénarios d'évaluation réalistes et mesurables
- Renforcer la collaboration entre Red Team, Blue Team et Purple Team
- Intégrer les exercices de sécurité dans une démarche DevSecOps
- Produire des rapports exploitables et des recommandations de remédiation
- Aligner les exercices sur les référentiels de cybersécurité reconnus
- Développer une démarche d'amélioration continue de la posture de sécurité
- Mesurer l'efficacité des contrôles de sécurité existants
- Réaliser des exercices pratiques dans un environnement contrôlé et autorisé

POUR QUI ?

- Ingénieurs cybersécurité
- Red Teamers
- Purple Teamers
- Blue Teamers
- Analystes SOC
- Pentesters
- Architectes sécurité
- Consultants en cybersécurité
- Responsables RSSI / CISO
- Auditeurs en sécurité des systèmes d’information
- Ingénieurs DevSecOps
- Toute personne impliquée dans l’évaluation de la sécurité des systèmes d’information dans un cadre autorisé

Innov Systems

Programme détaillé

1 / Fondamentaux du Red Teaming et de l'IA

- Principes, objectifs et méthodologie du Red Teaming
- Évolution des opérations offensives avec l'intelligence artificielle
- Cadre légal, éthique et règles d'engagement (Rules of Engagement)

2 / Cycle d'une opération de Red Team

- Planification et définition des objectifs
- Collecte d'informations (OSINT) et cartographie de la surface d'attaque
- Gestion des risques et coordination avec la Blue Team

3 / Intelligence artificielle au service des opérations offensives

- Analyse et corrélation de données à grande échelle
- Automatisation des tâches de reconnaissance et de priorisation
- Assistance à la génération de scénarios d'attaque réalistes

4 / Évaluation de la sécurité des systèmes basés sur l'IA

- Identification des risques propres aux applications d'IA
- Analyse des surfaces d'exposition des modèles et pipelines
- Évaluation des mécanismes de sécurité et de gouvernance

5 / Simulation d'attaques avancées

- Élaboration de scénarios réalistes multi-étapes
- Exercices Purple Team et validation des capacités de détection
- Évaluation de la résilience organisationnelle

Innov Systems

6 / Automatisation des campagnes de sécurité

- Orchestration des exercices de Red Team
- Intégration avec les plateformes de gestion de la sécurité
- Analyse automatisée des résultats et indicateurs

7 / Détection, réponse et amélioration continue

- Analyse des journaux et événements de sécurité
- Mesure de l’efficacité des contrôles défensifs
- Recommandations de remédiation et retour d’expérience

8 / Gouvernance, conformité et gestion des risques

- Cadres de référence (NIST, ISO/IEC 27001, MITRE ATT&CK)
- Documentation et reporting des exercices
- Gestion des risques cyber à l’échelle de l’entreprise

9 / Intégration du Red Teaming dans le DevSecOps

- Validation continue de la sécurité
- Collaboration entre Red Team, Blue Team et Purple Team
- Sécurisation du cycle de développement

10 / Cas pratiques et exercices de Red Team

- Conception d’un exercice Red Team encadré
- Analyse des résultats et plan d’amélioration
- Bonnes pratiques pour les programmes de sécurité offensifs

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

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
13 au 17 Sep. 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