

Cybersécurité Augmentée par l'IA — Détection des Menaces, SOC Intelligent et Réponse Automatisée

Lien : https://innov-maroc.com/formation/cybersecurite-augmentee-par-lia-detection-des-menaces-soc-intelligent-et-reponse-automatisee

DURÉE
8 jours (56h)

RÉFÉRENCE
IEEI52

CATÉGORIE
Cybersécurité Augmentée par l'IA et SOC Intelligent

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- Maîtriser les fondamentaux de l’intelligence artificielle appliquée à la cybersécurité.
- Identifier les principaux cas d’usage de l’IA dans les SOC, SIEM, EDR, XDR et plateformes de sécurité.
- Exploiter intelligemment les logs et événements de sécurité pour améliorer la détection des menaces.
- Mettre en œuvre des techniques d’Anomaly Detection pour identifier les comportements suspects.
- Concevoir les principes d’un SOC augmenté par IA et améliorer l’efficacité des analystes de sécurité.
- Exploiter l’IA pour enrichir et analyser les informations de Cyber Threat Intelligence.
- Utiliser l’UEBA pour détecter les comportements anormaux et les compromissions de comptes.
- Appliquer l’IA à la détection des malwares, ransomwares et attaques avancées.
- Automatiser certaines étapes de l’Incident Response grâce à l’IA et aux mécanismes SOAR.
- Utiliser l’IA générative et les LLM pour assister les analystes SOC dans leurs investigations.
- Développer des capacités prédictives permettant d’anticiper les cybermenaces et événements de sécurité.
- Mettre en place une gouvernance robuste et une stratégie d’industrialisation d’un SOC augmenté par IA.

INNOV MAROC

POUR QUI ?

- Directeurs cybersécurité, Chief Information Security Officers (CISO) et responsables de la sécurité des systèmes d’information.
- SOC Managers, responsables Security Operations et responsables de la supervision de sécurité.
- SOC Analysts, Security Analysts et Cybersecurity Analysts.
- Ingénieurs cybersécurité, Network Security Engineers et Security Engineers.
- Threat Intelligence Analysts et spécialistes de la détection des menaces.
- Incident Response Managers et spécialistes de la réponse aux incidents.
- Administrateurs et ingénieurs SIEM, SOAR, EDR, XDR et plateformes de sécurité.
- Data Scientists, Machine Learning Engineers et AI Engineers spécialisés en cybersécurité.
- Responsables IT, infrastructures, réseaux, Cloud et sécurité opérationnelle.
- Consultants, auditeurs et experts en cybersécurité, gestion des risques et transformation numérique.
- Responsables gouvernance, Risk & Compliance et responsables de la résilience numérique.
- Dirigeants et managers souhaitant renforcer leur dispositif de cybersécurité grâce à l’intelligence artificielle.

INNOV MAROC



Programme détaillé

1 / FONDAMENTAUX DE L'IA APPLIQUÉE À LA CYBERSÉCURITÉ

- Comprendre les principes de l'intelligence artificielle et du Machine Learning appliqués à la détection et à la prévention des cybermenaces.
- Identifier les cas d'usage de l'IA dans les environnements SOC, SIEM, EDR, XDR et Security Operations.
- Évaluer les apports, limites et risques de l'IA dans la protection des infrastructures numériques.

2 / COLLECTE ET CORRÉLATION INTELLIGENTE DES DONNÉES DE SÉCURITÉ

- Exploiter les logs, événements réseau, données endpoint, identités et informations issues des applications.
- Mettre en place des mécanismes de normalisation, corrélation et enrichissement des données de sécurité.
- Utiliser l'IA pour identifier des relations et signaux faibles difficilement détectables par des règles statiques.

3 / DÉTECTION DES ANOMALIES ET COMPORTEMENTS SUSPECTS

- Utiliser les techniques d'Anomaly Detection pour identifier les comportements inhabituels sur les systèmes et réseaux.
- Détecter les écarts par rapport aux comportements normaux des utilisateurs, équipements et applications.
- Réduire les faux positifs grâce à la contextualisation et à la priorisation intelligente des alertes.

4 / SOC INTELLIGENT ET AI-DRIVEN SECURITY OPERATIONS

- Transformer un SOC traditionnel en centre de supervision augmenté par l'intelligence artificielle.

INNOV MAROC

- Utiliser l’IA pour trier, corréler, enrichir et prioriser automatiquement les alertes de sécurité.
- Assister les analystes SOC dans l’investigation, la qualification et la réponse aux incidents.

5 / THREAT INTELLIGENCE AUGMENTÉE PAR IA

- Exploiter les techniques d’IA pour analyser les indicateurs de compromission, tactiques et techniques des attaquants.
- Corréler les informations issues des Threat Intelligence Feeds avec les événements observés dans l’organisation.
- Identifier les nouvelles tendances de menace et produire des évaluations de risque exploitables.

6 / USER AND ENTITY BEHAVIOR ANALYTICS — UEBA

- Analyser les comportements des utilisateurs, comptes, applications et équipements afin d’identifier les activités anormales.
- Détecter les compromissions de comptes, mouvements latéraux et comportements internes à risque.
- Construire des profils comportementaux dynamiques et adapter les niveaux de risque en fonction du contexte.

7 / IA POUR LA DÉTECTION DES MALWARES, RANSOMWARE ET ATTAQUES AVANCÉES

- Utiliser le Machine Learning et les techniques comportementales pour identifier les activités malveillantes.
- Détecter les comportements caractéristiques des ransomwares, malwares et attaques persistantes avancées.
- Combiner analyse statique, analyse comportementale et signaux réseau pour renforcer la détection.

8 / AUTOMATISATION DE L’INCIDENT RESPONSE ET SOAR

- Utiliser l’IA pour accélérer la qualification et l’investigation des incidents de cybersécurité.
- Automatiser certaines actions de réponse à travers des mécanismes SOAR et des playbooks de sécurité.
- Définir des niveaux d’automatisation garantissant une supervision humaine pour les décisions critiques.

9 / IA GÉNÉRATIVE POUR LES ANALYSTES SOC ET LA CYBERSÉCURITÉ

INNOV MAROC

- Utiliser les LLM pour résumer les incidents, analyser les logs et accélérer la recherche d’informations.
- Générer des synthèses d’incidents, rapports techniques, chronologies et recommandations d’investigation.
- Concevoir des assistants IA capables d’accompagner les analystes dans leurs opérations quotidiennes.

10 / DÉTECTION PRÉDICTIVE ET ANTICIPATION DES CYBERMENACES

- Exploiter les données historiques pour identifier les tendances et facteurs annonciateurs d’incidents.
- Construire des modèles permettant d’estimer la probabilité et la criticité de certains événements de sécurité.
- Développer une approche proactive permettant de renforcer la prévention avant la matérialisation des menaces.

11 / GOUVERNANCE, EXPLICABILITÉ ET RISQUE DE MODÈLE

- Identifier les risques liés aux biais, erreurs, hallucinations et mauvaises interprétations des modèles d’IA.
- Mettre en place des mécanismes d’explicabilité, validation, traçabilité et supervision humaine des décisions assistées par IA.
- Définir des règles de gouvernance garantissant une utilisation sécurisée, éthique et maîtrisée de l’IA.

12 / INDUSTRIALISATION DU SOC AUGMENTÉ PAR IA

- Définir une architecture intégrant SIEM, SOAR, EDR/XDR, Threat Intelligence, UEBA et modèles d’IA.
- Mesurer les performances du dispositif à travers des KPI tels que MTTD, MTTR, taux de faux positifs et volume d’alertes traitées.
- Construire une feuille de route d’industrialisation permettant de déployer progressivement l’IA dans les opérations de cybersécurité.

INOV MAROC

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

08 au 17 Fév. 2027	Présentiel - Casablanca
05 au 14 Avr. 2027	Présentiel - Casablanca
31 Mai au 09 Juin 2027	Présentiel - Casablanca
26 Juil. au 04 Août 2027	Présentiel - Casablanca
20 au 29 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-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés