

# CYBERSÉCURITÉ

## SÉCURISER LES DONNÉES, LES SYSTÈMES ET LES USAGES DE L'IA

Déployez l'IA et le numérique en gardant la maîtrise de vos données,  
de vos systèmes et de vos agents.

NIVEAU 2

 **DURÉE**  
**1 jour (7 heures)**

 **FORMAT**  
**Présentiel**

 **EFFECTIF**  
**10 à 16 participants**

 **TARIF**  
**3 500 MAD par participant HT**

UN PROGRAMME DE



EN PARTENARIAT AVEC



**CYB-201**





## PRÉSENTATION

Une journée pour installer, avec les équipes des systèmes d'information, de la qualité, de la production et des métiers, des pratiques de cybersécurité communes. L'intelligence artificielle y est traitée sous deux angles : l'outil qui renforce la défense, et l'usage qui doit lui-même être sécurisé.

## ENJEU DE LA FORMATION

L'intelligence artificielle et la numérisation des sites accélèrent l'innovation des laboratoires. Leur valeur repose sur la confiance dans les données traitées et dans les systèmes pilotés.

La journée installe des pratiques communes aux métiers, à la qualité et à l'informatique. Elle traite les usages de l'IA comme un sujet de sécurité à part entière : données confiées, agents, connecteurs et droits d'accès.



## OBJECTIFS PÉDAGOGIQUES

- 01 Cartographier les actifs critiques d'un laboratoire et les menaces qui les visent
- 02 Appliquer les pratiques de base aux systèmes d'information, qualité et industriels
- 03 Mobiliser l'IA dans la détection et la réponse, sous contrôle humain
- 04 Sécuriser les usages de l'IA : données confiées, agents, connecteurs et droits
- 05 Conduire la réponse à un incident, de la détection à la reprise



## RESSOURCES

- 01 L'autodiagnostic du laboratoire, avec ses priorités
- 02 La revue de sécurité d'un circuit d'agent, avec les droits et points de contrôle retenus
- 03 La fiche réflexe de réponse à incident, adaptée à l'organisation
- 04 La feuille de route à quatre-vingt-dix jours

## RÈGLES D'USAGE DE L'IA

### ASSISTANCE ADMISE

Tri et résumé des alertes. Recherche sur les menaces. Premiers jets de procédures et de rapports d'incident.

### ASSISTANCE SOUS CONTRÔLE

Actions automatisées de réponse, déclenchées par des règles validées et revues. Évaluations de fournisseurs préparées par un agent, validées par l'acheteur et le responsable de la sécurité.

### ACTIONS INTERDITES AUX AGENTS

Modification d'un système qualité ou industriel. Création ou extension de droits d'accès. Suppression de journaux ou de sauvegardes. Envoi de données hors de l'entreprise.

### RESPONSABILITÉ NON DÉLÉGABLE

Déclaration d'un incident. Arrêt et reprise de la production. Libération des lots après incident, par le pharmacien responsable. Communication externe.

### DONNÉES EXCLUES

Données patients et de vigilance nominatives, secrets de fabrication, identifiants et clés, dans tout outil non approuvé par l'entreprise.



## PROGRAMME DE LA FORMATION

MATINÉE · MODULES 1 À 3

01 · 1 H

02 · 1 H 30

03 · 1 H

04 · 1 H 30

05 · 1 H 30

06 · 30 MIN

01

🕒 1h

**CARTOGRAPHIER CE QUE LE LABORATOIRE PROTÈGE**

- Actifs critiques : dossiers réglementaires, données d'essais et de vigilance, procédés
- Systèmes qualité et industriels : LIMS, MES, ERP, automates de production
- Menaces du secteur : rançongiciel, vol de savoir-faire, altération de données
- Chaîne des tiers : sous-traitants, prestataires de recherche, distributeurs

02

🕒 1h30

**INSTALLER LES PRATIQUES DE BASE**

- Identités et accès : double authentification, moindre privilège, comptes à privilèges
- Sauvegardes isolées, restauration testée, intégrité des données restaurées
- Systèmes validés difficiles à mettre à jour : cloisonnement et surveillance
- Exigences de sécurité dans les contrats avec les tiers

**Atelier :** Autodiagnostic du laboratoire sur une grille de vingt pratiques.

03

🕒 1h

**MOBILISER L'IA DANS LA DÉFENSE**

- Détection d'anomalies et tri des alertes par l'IA
- Routines de surveillance, de contrôle des accès et d'évaluation des fournisseurs
- Actions automatisées de réponse : règles, seuils et validation humaine

**Démonstration d'un agent de tri d'alertes, avec ses limites et ses points de contrôle.**

## DÉROULEMENT

**MATINÉE**

Modules 1 à 3, actifs, pratiques de base et IA défensive.

**APRÈS-MIDI**

Modules 4 à 6, usages de l'IA, réponse à incident et gouvernance.



## PROGRAMME DE LA FORMATION

APRÈS-MIDI · MODULES 4 À 6

01 · 1 H

02 · 1 H 30

03 · 1 H

04 · 1 H 30

05 · 1 H 30

06 · 30 MIN

04

🕒 1h30

## SÉCURISER LES USAGES DE L'IA

- Usages non déclarés et données confiées à des outils non approuvés
- Injection d'instructions directe et indirecte : documents, courriels, pages web
- Agents et connecteurs : droits, journalisation, actions soumises à validation
- Fraudes produites par IA : hameçonnage ciblé, voix et vidéo usurpées

**Atelier :** Revue de sécurité d'un circuit d'agent de veille connecté à la messagerie.

05

🕒 1h30

## RÉPONDRE À UN INCIDENT

- Rôles, circuit de décision et registre de crise
- Déclarations : autorité nationale de cybersécurité, CNDP, autorités sanitaires
- Continuité de la production et intégrité des données après la reprise

**Atelier :** Exercice sur table : rançongiciel sur un site de production, doublé d'une fuite par un agent.

06

🕒 30 min

## GOUVERNER

- Responsabilités entre direction, sécurité, qualité et métiers
- Feuille de route à quatre-vingt-dix jours

## MODALITÉS PÉDAGOGIQUES



## MÉTHODES

Exposés courts, démonstrations, ateliers en équipes mixtes, exercice sur table.



## ÉVALUATION

Positionnement en début de journée. En fin de journée, chaque équipe présente sa revue de circuit d'agent et les décisions prises pendant l'exercice.



## SUIVI APRÈS SESSION

Point à quatre-vingt-dix jours sur l'avancement de la feuille de route.



## L'ESSENTIEL

**DURÉE**

1 jour (7 heures)

**FORMAT**

Présentiel, inter ou intra-entreprise

**PUBLIC**

Systèmes d'information, sécurité, qualité, production, porteurs de projets d'IA

**EFFECTIF**

10 à 16 participants

**PRÉREQUIS**

Programme CYB-101 ou SOC-101 recommandé

**LANGUE**

Français

**LIEU**

Casablanca ou Rabat

**TARIF**

Session interentreprises : 3 500 MAD par participant, hors taxes. Intra-entreprise sur devis, selon l'effectif et l'ampleur de la phase de cadrage.



## PROCHAINES SESSIONS

|                  |            |            |
|------------------|------------|------------|
| 19 novembre 2026 | Casablanca | PRÉSENTIEL |
| 10 décembre 2026 | Rabat      | PRÉSENTIEL |

## ORGANISATION

**DÉLAI D'ACCÈS**

Trois à cinq semaines après validation de la proposition, le temps de cadrer le périmètre avec vos équipes.

**ACCESSIBILITÉ**

Les besoins d'aménagement sont examinés au cadrage. Les supports sont fournis dans un format lisible par les technologies d'assistance.

**INTRA OU INTER**

Sessions interentreprises à Casablanca et à Rabat, ou session intra-entreprise. Les ateliers portent sur des scénarios types, sans données réelles.

## VOUS SOUHAITEZ FORMER VOS ÉQUIPES ? PARLONS-EN ENSEMBLE.

Un premier échange nous permet de comprendre les équipes concernées, le format adapté et votre calendrier. Nous vous adressons ensuite une proposition détaillée.

**Sanae Kenini**

Directrice exécutive

✉ [s.kenini@aillifesciences.org](mailto:s.kenini@aillifesciences.org)

☎ +212 661 448 498

**S'inscrire à une session**

Scannez le code pour ouvrir la page de la formation et ses prochaines dates.