

Nouveauté

Ref. IA-SOC

Intégration de l'Intelligence Artificielle (IA) au sein d'un SOC

3 jours (21 heures)

Expertise

Présentiel ou classe à distance

à partir de

2 925 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 08/10/2026.

Objectifs

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

- Décrire comment l'Intelligence Artificielle (IA) transforme les opérations d'un Security Operations Center (SOC), ses apports, ses limites et ses enjeux opérationnels
- Mettre en oeuvre des outils d'IA (LLM, agents autonomes, hyper-automation) pour assister les tâches d'un SOC : triage d'alerte, corrélation, enquête, réponse
- Concevoir et exécuter un scénario de SOC "augmenté" par l'IA : de la détection à la réponse, en intégrant la collaboration humain-IA
- Analyser et interpréter les résultats produits par l'IA, gérer les faux-positifs, calibrer la confiance et la gouvernance autour des agents IA
- Appliquer les bonnes pratiques éthiques, réglementaires, de gouvernance et de supervision humaine liées à l'usage d'IA dans un SOC.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Analystes SOC, responsables SOC, ingénieurs "Detection and Response", consultants sécurité, responsables opérations Cyber, architectes sécurité.

Prérequis

Avoir des connaissances de base en opérations SOC : traitement d'alertes, SIEM, SOAR, cas d'incidents.

Avoir connaissance des outils classiques de sécurité (SIEM, EDR, réseau) et des flux SOC. Avoir une compréhension élémentaire des principes d'IA / ML / agents autonomes.

Programme

1 Pendant votre formation

Intégration de l'Intelligence Artificielle (IA) au sein d'un SOC

Jour 1 – Matin

Panorama de l'IA dans le SOC et mise en place des outils

- Introduction à l'évolution des SOC et le besoin d'IA : défis actuels (volume d'alertes, fatigue analyste, complexité des menaces)
- Etat de l'art de l'IA dans le SOC : triage automatique, agents multi-outils, co-pilotes IA, hyper-automation
- Cas d'usage concrets : corrélation comportementale, réponse automatisée, documentation et reporting IA

Exemple de travaux pratiques (à titre indicatif)

- Mise en place d'un environnement SOC simulé, installation initiale des outils IA (LLM, agent de triage, workflow SOAR)

Jour 1 – Après-midi

Panorama de l'IA dans le SOC et mise en place des outils – Suite

- Construction d'un pipeline IA d'alerte SOC : ingestion d'événements, enrichissement contextuel, priorisation via IA
- Débrief et retour d'expérience : limites, biais, calibrage initial

Exemple de travaux pratiques (à titre indicatif)

- Capture d'un flux d'alertes, automatisation de triage et enrichissement par IA, démonstration de réduction de faux-positifs

Jour 2 – Matin

Détection, investigation et réponse augmentées par l'IA

- Utilisation de l'IA dans la détection d'anomalies, la corrélation multi-source, la détection comportementale
- Agents IA et workflow SOC : comment intégrer des agents autonomes dans les playbooks SOC existants

Exemple de travaux pratiques (à titre indicatif)

- Simulation d'un incident (ex : phishing et mouvement latéral), utilisation de l'IA pour investigation, extraction de contexte, génération de rapport d'investigation

Jour 2 – Après-midi

Détection, investigation et réponse augmentées par l'IA – Suite

- Réponse automatisée ou semi-automatisée : intégration entre SOAR, IA et intervention humaine

Exemples de travaux pratiques (à titre indicatif)

- Mise en oeuvre d'un scénario complet : alerte générée, IA triage, IA agent propose remédiation, analyste valide / affine, documentation automatique
- Discussion : comment garder la supervision humaine, calibrer niveaux d'autonomie IA, gestion des erreurs et des risques

Jour 3 – Matin

Gouvernance, reporting et limites éthiques de l'IA dans le SOC

- Analyse critique de l'IA dans le SOC : hallucinations, biais, défi de la confiance, supervision humain-IA
- Automatisation du reporting et documentation par IA : génération de rapports exécutifs, tableaux de bord dynamiques, traçabilité

Exemple de travaux pratiques (à titre indicatif)

- Génération automatique d'un rapport de sécurité SOC à partir d'un incident traité, adaptation au niveau de management et au niveau technique

Jour 3 – Après-midi

Gouvernance, reporting et limites éthiques de l'IA dans le SOC – Suite

- Cadre légal, réglementaire et éthique : RGPD, AI Act, responsabilités, transfert de décisions, preuve
- Intégration stratégique de l'IA dans le SOC : roadmap, KPI, maturité, mesure d'impact

Exemple de travaux pratiques (à titre indicatif)

- Chaque participant réalise un mini-cas SOC "augmenté IA" (de la détection à la restitution), restitution

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 5 janvier 2027 au 7 janvier 2027 (3 jours / 21 heures)

À distance

Du 5 janvier 2027 au 7 janvier 2027

À distance

- 5 janvier 2027 ----- 9h00 – 16h00
- 6 janvier 2027 ----- 9h00 – 16h00
- 7 janvier 2027 ----- 9h00 – 16h00