

SIEM Analytics tactiques

3 jours (21 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

2 625 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

Objectifs

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

- Collecter et normaliser les sources de logs (Windows, Linux, réseau)
- Mettre en place des règles de corrélation pour détecter automatiquement des comportements suspects
- Créer et tester des règles personnalisées adaptées aux risques métier
- Prioriser les incidents sur la base de scénarios de menace et de critères opérationnels
- Développer des tableaux de bord et des workflows d'alerte pour un SOC efficace.

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

À qui s'adresse cette formation ?

Analystes SOC et ingénieurs sécurité, administrateurs et architectes SIEM, responsables Incident Response, consultants en détection de menaces.

Prérequis

Avoir des connaissances de base en Linux / Windows et en protocoles réseau (TCP / IP, DNS), des notions d'administration de serveurs et de scripting (Python ou PowerShell) ainsi qu'une familiarité avec un outil de gestion de logs (Syslog, Winlogbeat...).

Programme

1 Pendant votre formation

SIEM Analytics tactiques

Jour 1 – Matin

Présentation de l'architecture SIEM

- Collecte
- Parsing
- Normalisation

Configuration des agents de collecte

- Windows Event Collector
- Beats

Exemple de travaux pratiques (à titre indicatif)

- Ingestion de logs Windows et Linux dans la plateforme

Jour 1 – Après-midi

Introduction à la corrélation de logs

- Principes
- Types de corrélations (statique, temporelle, multi-sources)

Exemple de travaux pratiques (à titre indicatif)

- Mise en place d'une règle de corrélation simple (détection de bruteforce réseau)

Jour 2 – Matin

Création de règles personnalisées

- Syntaxe
- Variables
- Fonctions avancées (regex, agrégations)

Exemple de travaux pratiques (à titre indicatif)

- Rédaction et ajustement de 2 règles métier (accès administrateur tardif, exfiltration via protocole non standard)

Jour 2 – Après-midi

Tests et tuning des règles

- Simulation d'événements
- Optimisation des seuils
- Réduction des faux positifs

Exemple de travaux pratiques (à titre indicatif)

- Mise en place d'un environnement de test automatisé pour valider les règles à grande échelle

Jour 3 – Matin

Priorisation des incidents

- Scoring des alertes
- Mapping sur la Cyber Threat Intelligence

Workflow d'alerte et gestion d'incident

- Assignation
- SLA
- Escalade automatisée

Exemple de travaux pratiques (à titre indicatif)

- Création d'un playbook d'escalade via API ou Webhooks

Jour 3 – Après-midi

Tableaux de bord et reporting opérationnel

- KPIs clés (MTTD, MTTR, volume d'alertes)

Exemple de travaux pratiques (à titre indicatif)

- Détection et priorisation d'une série d'incidents simulés, de la corrélation à l'escalade

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 12 janvier 2027 au 14 janvier 2027 (3 jours / 21 heures)

Paris La Défense

Du 12 janvier 2027 au 14 janvier 2027 Paris La Défense

- 12 janvier 2027 9h00 – 16h00
- 13 janvier 2027 9h00 – 16h00
- 14 janvier 2027 9h00 – 16h00