

SOC (Security Operation Center) – First Responder et traitement des incidents

2 jours (14 heures)

Initiation

Présentiel ou classe à distance

à partir de

1950 € 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 :

- Accomplir les opérations SOC suivantes : reporting, tri des alertes et premières actions de réponse
- Expliquer l'organisation d'un SOC et les missions d'un first responder
- Utiliser un SIEM pour collecter et prioriser les alertes de sécurité
- Analyser des logs afin d'identifier et qualifier un incident de sécurité
- Mettre en place des actions de containment de premier niveau (isolation d'hôtes, blocage d'IP)
- Rédiger un ticket d'incident complet et coordonner le transfert vers les équipes N2 / N3
- Participer à un exercice opérationnel de détection, containment et reporting d'un incident.

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

À qui s'adresse cette formation ?

Débutants en SOC et sécurité opérationnelle, techniciens et ingénieurs support IT, membres d'équipes NOC souhaitant basculer vers un rôle SOC, toute personne devant assurer la première ligne de réponse aux incidents.

Prérequis

Avoir des connaissances de base en réseau (TCP / IP, DNS) ainsi que des notions d'administration Windows et Linux et avoir une aisance avec un shell et un éditeur de texte.

Programme

1 Pendant votre formation

SOC (Security Operation Center) – First Responder et traitement des incidents

Jour 1 – Matin

Introduction au SOC et au rôle de first responder

- Périmètre, responsabilités, niveau d'escalade

Architecture et composants clés

- Collecte de logs (SIEM), alerting, tableaux de bord

Exemple de travaux pratiques (à titre indicatif)

- Prise en main de la console SIEM et tri des premières alertes

Jour 1 – Après-midi

Investigation initiale

- Analyse de logs pour identifier la nature et la portée d'un incident

Reporting opérationnel

- Rédaction d'un ticket d'incident structuré (qui, quoi, où, quand, comment)

Exemple de travaux pratiques (à titre indicatif)

- Gestion d'un incident simulé et passage de relais à l'équipe d'investigation

Jour 2 – Matin

Containment et remédiation de premier niveau

- Isolement d'hôtes, blocage d'adresses IP

Utilisation d'outils de réponse rapide

- Scripts PowerShell / Linux, playbooks automatisés

Exemple de travaux pratiques (à titre indicatif)

- Exécution d'un playbook pour stopper une attaque en cours

Jour 2 – Après-midi

Communication et coordination avec les équipes N2 / N3

- Transfert d'informations clés et suivi

Retour d'expérience et post-mortem

- Elaboration d'un mini-rapport et recommandations de durcissement

Exemple de travaux pratiques (à titre indicatif)

- *Exercice SOC : détection, tri, containment et reporting d'un incident de bout en bout*

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 9 novembre 2026 au 10 novembre 2026 (2 jours / 14 heures)

Toulouse

Du 9 novembre 2026 au 10 novembre 2026 **Toulouse**

- 9 novembre 2026 9h00 – 16h30
- 10 novembre 2026 9h00 – 16h30