

Nouveauté

Ref. SEC-DEF

Cybersécurité défensive

10 jours (70 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

6 000 € 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 :

- Analyser le paysage des menaces et structurer une posture de défense en profondeur
- Durcir les systèmes et les architectures réseau (CIS, ANSSI)
- Organiser un SOC, déployer un SIEM et concevoir des règles de détection
- Surveiller les terminaux (EDR / XDR), mener des chasses aux menaces et exploiter la CTI
- Conduire une réponse à incident et des investigations numériques (forensic)
- Gérer les vulnérabilités et inscrire la défense dans la gouvernance (EBIOS RM, ISO 27001, NIS2)
- Piloter l'amélioration continue de la détection et de la réponse.

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

À qui s'adresse cette formation ?

Administrateurs systèmes et réseaux, techniciens et ingénieurs sécurité, futurs analystes SOC et analystes cyberdéfense, consultants en sécurité et RSSI.

Prérequis

Disposer de connaissances pratiques des systèmes d'exploitation (Windows et Linux), maîtriser les fondamentaux des réseaux (TCP/IP, services courants), connaître les concepts de base de la cybersécurité et être à l'aise avec la ligne de commande.

Programme

1 Pendant votre formation

Cybersécurité défensive

Jour 1 – Matin

Analyser le paysage des menaces et la posture défensive

- Panorama des menaces (APT, rançongiciels, phishing, supply chain)
- Chaîne d'attaque (kill chain) et référentiel MITRE ATT&CK
- Principes de défense en profondeur et de moindre privilège
- Organisation de la cyberdéfense : SOC, CERT, CSIRT, CTI

Exemple de travaux pratiques (à titre indicatif)

- Modélisation d'un scénario d'attaque avec ATT&CK Navigator

Jour 1 – Après-midi

Cartographier le SI et organiser la surveillance

- Inventaire des actifs et identification des surfaces d'exposition
- Sources de données à monitorer : Windows, réseau, EDR, DNS, DHCP, messagerie
- Stratégie de journalisation et de centralisation des logs
- Mise en place de Sysmon et de la télémétrie

Exemple de travaux pratiques (à titre indicatif)

- Configuration de Sysmon et première collecte de journaux

Jour 2 – Matin

Durcir les systèmes (hardening)

- Lignes de base de sécurité Windows et Linux
- Référentiels CIS Benchmarks et guides ANSSI
- Gestion des comptes, des privilèges et des secrets
- Contrôle et vérification de conformité du durcissement

Exemple de travaux pratiques (à titre indicatif)

- Application d'un durcissement CIS / ANSSI sur un système

Jour 2 – Après-midi

Sécuriser l'architecture réseau

- Segmentation, cloisonnement et principes du zero trust
- Pare-feu, IDS / IPS et passerelles de sécurité
- Sécurisation des services exposés (WAF, DNS, messagerie)
- Détection des flux anormaux et des mouvements latéraux

Exemple de travaux pratiques (à titre indicatif)

- Mise en place d'une règle IDS et analyse de flux réseau

Jour 3 – Matin

Comprendre et organiser un SOC

- Etat de l'art du SOC : missions, services, modèles de gouvernance
- Métier d'analyste : triage, niveaux 1 / 2 / 3, playbooks
- Articulation SOC, CERT et CSIRT
- Indicateurs et métriques d'un SOC

Exemple de travaux pratiques (à titre indicatif)

- Rédaction d'un playbook de traitement d'alerte

Jour 3 – Après-midi

Déployer et exploiter un SIEM

- Principes du SIEM : collecte, normalisation, corrélation
- Panorama des solutions (Elastic / ELK, Splunk, Microsoft Sentinel)
- Mise en oeuvre de la suite Elastic (Beats, Logstash, Elasticsearch, Kibana)
- Construction de tableaux de bord de supervision

Exemple de travaux pratiques (à titre indicatif)

- Déploiement d'ELK et remontée des premiers événements

Jour 4 – Matin

Concevoir des règles de détection (detection engineering)

- Cas d'usage de détection alignés sur ATT&CK
- Règles Sigma et corrélation d'événements
- Réduction des faux positifs et réglage des seuils
- Apport de l'analyse comportementale (UEBA) et de l'IA à la détection

Exemple de travaux pratiques (à titre indicatif)

- Création de règles de détection Sigma et d'alertes

Jour 4 – Après-midi

Surveiller les postes et serveurs (EDR / XDR)

- Rôle de l'EDR, du XDR et de la protection des terminaux (EPP)
- Télémétrie endpoint et détection comportementale
- Investigation et réponse depuis la console EDR
- Articulation EDR / SIEM

Exemple de travaux pratiques (à titre indicatif)

- Analyse d'une détection endpoint et qualification

Jour 5 – Matin

Mener une chasse aux menaces (threat hunting)

- Démarche : hypothèses, IoC et IoA
- Techniques de chasse proactive alignées sur ATT&CK
- Requêtes et pivots dans le SIEM et l'EDR
- Documentation et capitalisation des chasses

Exemple de travaux pratiques (à titre indicatif)

- Campagne de threat hunting sur un jeu de données

Jour 5 – Après-midi

Exploiter la Cyber Threat Intelligence (CTI)

- Niveaux de CTI : stratégique, tactique, opérationnel
- Plateformes et formats : MISP, STIX / TAXII, ATT&CK
- Enrichissement des alertes et des indicateurs
- Intégration de la CTI dans la détection

Exemple de travaux pratiques (à titre indicatif)

- Enrichissement d'indicateurs via MISP

Jour 6 – Matin

Structurer la réponse à incident

- Cadres de référence : NIST SP 800-61 et démarche SANS (PICERL)
- Organisation de crise et rôles des intervenants
- Chaîne d'alerte et procédures d'escalade
- Communication et coordination (SOC, CERT, juridique, direction)

Exemple de travaux pratiques (à titre indicatif)

- Construction d'un plan de réponse à incident

Jour 6 – Après-midi

Qualifier et trier les incidents

- Analyse et qualification des alertes
- Priorisation selon l'impact et la gravité
- Décisions d'escalade et de confinement initial
- Traçabilité et documentation de l'incident

Exemple de travaux pratiques (à titre indicatif)

- Triage d'une série d'alertes et qualification d'un incident

Jour 7 – Matin

Conduire une investigation numérique (forensic)

- Principes du forensic et chaîne de preuve
- Acquisition des données à chaud et à froid
- Analyse des artefacts disque et système (Windows, Linux)
- Outils d'investigation (Autopsy, FTK Imager)

Exemple de travaux pratiques (à titre indicatif)

- Acquisition et analyse d'artefacts sur une image disque

Jour 7 – Après-midi

Analyser la mémoire et le réseau

- Analyse de mémoire vive avec Volatility
- Analyse de captures réseau (Wireshark, Zeek)
- Reconstitution de la chronologie (timeline)
- Identification des indicateurs de compromission

Exemple de travaux pratiques (à titre indicatif)

- Analyse mémoire et réseau d'un poste compromis

Jour 8 – Matin

Analyser un code malveillant

- Analyse statique de base d'un échantillon
- Analyse dynamique en environnement isolé (sandbox)
- Extraction d'indicateurs et de signatures (YARA)
- Limites et précautions de manipulation

Exemple de travaux pratiques (à titre indicatif)

- Analyse en bac à sable d'un échantillon et extraction d'IOC

Jour 8 – Après-midi

Confiner, éradiquer et rétablir

- Stratégies de confinement et d'éradication
- Rétablissement des services et vérification d'intégrité

- Mesures correctives et durcissement post-incident
- Retour d'expérience (post-mortem) et capitalisation

Exemple de travaux pratiques (à titre indicatif)

- *Elaboration d'un plan de confinement et de rétablissement*

Jour 9 – Matin

Gérer les vulnérabilités

- Cycle de gestion des vulnérabilités
- Scan, identification et qualification (CVSS, EPSS)
- Priorisation de la remédiation et patch management
- Suivi et métriques de réduction du risque

Exemple de travaux pratiques (à titre indicatif)

- *Analyse d'un rapport de scan et plan de remédiation*

Jour 9 – Après-midi

Inscrire la défense dans la gouvernance et la conformité

- Analyse de risque (EBIOS RM) et référentiel ISO / IEC 27001
- Obligations réglementaires : NIS2, RGPD
- Politiques de sécurité et plans de continuité
- Usage responsable de l'IA dans la défense

Exemple de travaux pratiques (à titre indicatif)

- *Ebauche d'une analyse de risque sur un périmètre donné*

Jour 10 – Matin

Réaliser un exercice défensif de bout en bout (capstone)

- Mise en situation : détection, qualification, réponse et reporting
- Travail en équipe sur un scénario d'attaque réaliste
- Rédaction d'un rapport d'incident et de recommandations
- Restitution et revue par les pairs

Exemple de travaux pratiques (à titre indicatif)

- *Exercice blue team intégrateur et rapport d'incident*

Jour 10 – Après-midi

Ancrer une démarche d'amélioration continue

- Purple teaming et tests de détection
- Métriques de performance du SOC (MTTD, MTTR)
- Organisation de la veille et de l'entraînement
- Bilan, évaluation des acquis et plan de montée en compétence

Exemple de travaux pratiques (à titre indicatif)

- Construction d'un tableau de bord de pilotage défensif

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

Sessions

À distance

Du 18 novembre 2026 au 1 décembre 2026

Du 4 janvier 2027 au 15 janvier 2027

Paris La Défense

Du 12 novembre 2026 au 25 novembre 2026

Du 11 janvier 2027 au 22 janvier 2027