

Systèmes de prévention (IPS) et détection (IDS) d'intrusion

3 jours (21 heures)

Initiation

Présentiel ou classe à distance

à partir de

2 205 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 05/10/2026.

Objectifs

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

- Déployer et maintenir différents outils de prévention et de détection d'intrusion
- Paramétrer et fine-tuner des systèmes de détection et d'alerte
- Organiser et centraliser les alertes pour un SIEM
- Identifier les raisons de déclenchement d'une règle ou d'un faux positif.

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

À qui s'adresse cette formation ?

Pentesters, administrateurs système et réseau, analystes SOC, responsables de la sécurité des systèmes d'information (RSSI), consultants en cybersécurité et étudiants en sécurité informatique.

Prérequis

Avoir des connaissances générales en système, réseau et développement.

Programme

1 Pendant votre formation

Systèmes de prévention (IPS) et détection (IDS) d'intrusion

Jour 1 – Matin

Introduction aux IPS et IDS

- Les principaux dispositifs de sécurité dans le système d'information
- Le rôle des IPS et des IDS
- Le positionnement des IPS et des IDS
- Les différents types d'IPS et d'IDS
- Les différentes technologies clés
 - Signature
 - Comportementale
 - Heuristique...
- Les produits communautaires et commerciaux

Jour 1 – Après-midi

Composants et architecture

- Les composants clés
 - Capteurs
 - Gestionnaires
 - Consoles
 - Bases de données...
- Le déploiement dans l'architecture réseau et placement stratégique des capteurs
- Les interactions avec d'autres systèmes de sécurité
 - Firewalls
 - Systèmes de gestion des logs
 - SIEM...
- Les IPS et IDS dans le Cloud

Types de détections

- La détection basée sur :
 - Les signatures
 - L'anomalie
 - L'état
- Les avantages et limites de chaque méthode

Exemples de travaux pratiques (à titre indicatif)

- Installation et découverte des paramètres d'un H-IPS
- Installation et découverte des paramètres d'un N-IDS

Jour 2 – Matin

Configuration, gestion et analyse des alertes

- Les paramètres de base d'un IPS et d'un IDS
- Les principales règles d'un IPS
- Les principales règles d'un IDS
- Les règles par défaut
- Le paramétrage avancé
 - Les règles compilées
 - Les préprocesseurs
 - Les dissecteurs et analyseurs
- La personnalisation des règles
 - Le format des règles
 - L'historisation des alertes
- L'analyse des alertes
 - Tri
 - Hiérarchisation
 - Réponse
- L'intégration avec les systèmes de ticketing et les procédures de réponse aux incidents

Jour 2 – Après-midi

Exemples de travaux pratiques (à titre indicatif)

- *Création de règles de surveillance pour le système d'exploitation*
- *Création de règles de surveillance pour les protocoles d'infrastructure*
- *Création de règles de surveillance pour un serveur applicatif*
- *Création d'une politique d'historisation et de remontée des alertes*
- *Déploiement d'une solution IDS pour les domaines Microsoft*
- *Création d'une politique d'audit et d'historisation des événements d'importance*

Maintenance et mise à jour

- Processus de mise à jour des signatures et des algorithmes
- Surveillance de la performance et du bon fonctionnement
- Techniques de troubleshooting

Exemple de travaux pratiques (à titre indicatif)

- *Création d'une "update policy" et d'une "patch management policy" pour les IPS et IDS déployés*

Jour 3 – Matin

Techniques avancées de détection

- Les principales techniques d'évasion

- La détection de l'évasion et les techniques anti-évasion
- L'intégration de l'Intelligence Artificielle (IA) et de l'apprentissage automatique
- L'analyse comportementale approfondie
- Le EndPoint Protection

Exemples de travaux pratiques (à titre indicatif)

- *Création de paquets avec signature d'attaque et évasion d'un IDS*
- *Création d'un pont MITM pour SSL/TLS*
- *Modification de la politique de surveillance des IPS et des IDS pour échapper aux "protocols violations"*
- *Installation et paramétrage d'une solution EDR / XDR*

Jour 3 – Après-midi

Personnalisation et optimisation

- Développement de signatures personnalisées
- Optimisation des règles pour réduire les faux positifs
- Adaptation des systèmes IDS / IPS à des environnements spécifiques
 - Gouvernement
 - Finance...

Exemples de travaux pratiques (à titre indicatif)

- *Création de règles spécifiques pour bloquer les paquets d'évasion du module précédent*
- *Création d'une politique de sécurité pour un environnement virtuel ou conteneurisé*
- *Création d'une règle pour bloquer un malware créé par le formateur*

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 18 novembre 2026 au 20 novembre 2026 (3 jours / 21 heures)

Nancy

Du 18 novembre 2026 au 20 novembre 2026

Nancy

- 18 novembre 2026 9h00 – 16h00
- 19 novembre 2026 9h00 – 16h00
- 20 novembre 2026 9h00 – 16h00