

Durcissement sécurité Linux

5 jours (35 heures)

Expertise

Présentiel ou classe à distance

à partir de

3 475 € 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 :

- Identifier les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent
- Optimiser la sécurisation du système.

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

À qui s'adresse cette formation ?

Responsables sécurité du SI, chefs de projets informatiques, administrateurs systèmes.

Prérequis

Savoir administrer un système d'exploitation Linux. Avoir des connaissances de base en sécurité des systèmes d'information.

Programme

1 Pendant votre formation

Durcissement sécurité Linux

Jour 1 – Matin

Introduction

- Généralités sur Linux
- Menaces et attaques sur l'environnement Linux
- La sécurité de l'environnement Linux (bonnes pratiques)

Exemple de travaux pratiques (à titre indicatif)

- *Audit initial d'un système Linux*

Jour 1 – Après-midi

Les politiques de sécurité

- Caractéristiques d'une PSSI (Politique de Sécurité du Système d'Information)
- Standards de sécurité de l'ANSSI, recommandations BP28

Exemple de travaux pratiques (à titre indicatif)

- *Démonstration d'intégration des recommandations à l'installation*

Guide des bonnes pratiques de déploiement du système Linux

- Démarrage
- Noyau(x)
- Partitionnement
- Gestion des logiciels, MCS

Exemples de travaux pratiques (à titre indicatif)

- *Détournement / appropriation du mot de passe root au démarrage*
- *Sécurisation du démarrage*
- *Suppression des noyaux inutiles*

Jour 2 – Matin

Identification et authentification

- Gestion des comptes utilisateurs
- Gestion des mots de passe
- Les "sudoers"
- PAM (Pluggable Authentication Modules)
 - Les niveaux de sécurité PAM
 - Cloisonnement/ limitations au travers de PAM
 - PAM su
 - Centralisation de la gestion des mots de passe auprès d'Active Directory (SSSD)

Exemples de travaux pratiques (à titre indicatif)

- *Evaluation de la dureté des mots de passe*
- *Durcissement de l'authentification via les modules PAM*
- *Authentification centralisée SSSD*

Jour 2 – Après-midi

Protection des fichiers

- Droits standards des systèmes de fichiers Unix
- Attributs étendus
- ACL (Access Control List)
- Capabilities
- Chiffrement
- Effacement sécurisé

Exemples de travaux pratiques (à titre indicatif)

- *Protection de fichiers avec les attributs étendus*
- *Cloisonnement des accès avec les ACL et les Capabilities*
- *Chiffrement de partitions et fichiers*

Jour 3 – Matin

Les MAC (Mandatory Access Control)

- SELinux

Exemples de travaux pratiques (à titre indicatif)

- *Configuration et modification de politique SELinux*

Jour 3 – Après-midi

La surveillance du système

- Les Host IDS :
 - Surveillance des fichiers (AIDE)
 - Surveillance des processus (Auditd)
- Agents HIDS

Exemples de travaux pratiques (à titre indicatif)

- *Configuration d'un agent HIDS sécurisé*
- *Déploiement Auditd et AIDE*

La sécurité du réseau

- Paramétrage avec Sysctl
- Paramétrage des interfaces réseau

Exemples de travaux pratiques (à titre indicatif)

- *Désactivation d'IPv6*

- Application de filtres ARP

Jour 4 – Matin

L'administration à distance sécurisée

- SSH, bonnes pratiques, key-generation et key-gestion
- Dnssec

Exemples de travaux pratiques (à titre indicatif)

- SSH, key-generation et key-gestion
- Dnssec

Jour 4 – Après-midi

La PKI pour les clients Linux

- Rappel des principes
- Architecture TLS chez les clients

Exemples de travaux pratiques (à titre indicatif)

- Sécurisation d'une architecture "N-tier" avec TLS

Jour 5 – Matin

Evolution du filtrage

- Iptables, l'histoire
- Nftables, le présent
- Firewallld, l'interface

Exemples de travaux pratiques (à titre indicatif)

- Sécurisation d'une architecture simple avec nftables

Jour 5 – Après-midi

Conclusion

- Audit final d'un système Linux
- Ouverture vers les architectures sécurisées

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 30 novembre 2026 au 4 décembre 2026 (5 jours / 35 heures)

À distance

Du 30 novembre 2026 au 4 décembre 2026

À distance

- 30 novembre 2026 9h00 – 15h00
- 1 décembre 2026 9h00 – 15h00
- 2 décembre 2026 9h00 – 15h00
- 3 décembre 2026 9h00 – 15h00
- 4 décembre 2026 9h00 – 15h00