

Sécurité de l'Active Directory

3 jours (21 heures)

Expertise

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 02/10/2026.

Objectifs

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

- Décrire les mécanismes internes Active Directory
- Identifier les fonctionnalités de sécurité
- Concevoir une architecture robuste
- Identifier les attaques et principales exploitations dans un système existant
- Mettre en oeuvre les contre-mesures.

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

À qui s'adresse cette formation ?

Architectes et administrateurs systèmes, ingénieurs sécurité.

Prérequis

Avoir de bonnes connaissances dans l'administration Windows Server 2012 R2 / 2016 / 2019 ainsi que dans les rôles Active Directory.

Programme

1 Pendant votre formation

Sécurité de l'Active Directory

Jour 1 – Matin

Les fondamentaux en sécurité

- Comprendre une architecture Active Directory typique
- Revue de l'authentification / autorisation
- Tour d'horizon des différents protocoles
- Comprendre les recommandations et bonnes pratiques associées
- Mettre en oeuvre une stratégie de sécurité
- Comprendre la notion de Cloche de la cybersécurité

Comprendre les risques et les attaques

- Vue d'ensemble des méthodes de gestion des risques SI
- Comprendre les différentes étapes d'une attaque
- Simuler des attaques et analyser les contre-mesures
- Détecter les failles de sécurité
- Comprendre les notions de Pass-the-Hack, Golden Ticket...
- Vue d'ensemble des outils associés

Jour 1 – Après-midi

Durcissement de l'infrastructure AD

- Concevoir un plan de durcissement
- Déployer les directives associées
- Savoir auditer une infrastructure
- Collecter les événements au niveau de l'entreprise
- Mettre en oeuvre :
 - Les directives préconisées
 - Les nouveautés de durcissement (PAM, JIT / JEA...), les comptes protégés...

Jour 2 – Matin

Comprendre les modèles d'administration

- Connaître les différents modèles d'administration (EAM, Tier)
- Intérêt et limites du concept de forêt d'administration
- Mise en oeuvre d'une forêt d'administration
- Vue d'ensemble des bonnes pratiques et état de l'art quant au durcissement et la sécurisation AD

L'identité dans le Cloud

- Vue d'ensemble de la sécurisation via les outils Cloud
- Concevoir une architecture hybride
- Vue d'ensemble des outils :
 - Azure Entra Security
 - Secure Score
 - Defender for Identity

Jour 2 – Après-midi

Mise en oeuvre d'un durcissement complémentaire Active Directory

- Déployer une infrastructure PKI afin de porter les fonctionnalités de durcissement
- Introduction au durcissement on-premise de la fédération avec AD FS
- Configuration avancée Azure Entra Connect

Jour 3 – Matin

Mise en oeuvre d'un PCA / PRA

- Concevoir une architecture PCA / PRA sur le socle Authentification
- Planifier des tests de PCA / PRA
- Comprendre les outils et méthodes pour tester un PCA / PRA
- Mettre en oeuvre la sauvegarde et restauration

Surveiller et auditer

- Vue d'ensemble des niveaux d'audit
- Gestion du cycle de vie des audits
- Identifier les failles de sécurité par les logs
- Centralisation des logs
- Bonnes pratiques et indicateurs

Jour 3 – Après-midi

Les dernières nouveautés

- Mettre en oeuvre le top 10 du durcissement de l'identité

Exemples de travaux pratiques (à titre indicatif)

- Mettre en place une architecture ESAE dans le cadre du durcissement
- Durcir l'AD en respectant les bonnes pratiques du moment
- Identifier une attaque et contre mesure

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 14 octobre 2026 au 16 octobre 2026 (3 jours / 21 heures)

Paris La Défense

Du 14 octobre 2026 au 16 octobre 2026

Paris La Défense

- 14 octobre 2026 9h00 - 16h00
- 15 octobre 2026 9h00 - 16h00
- 16 octobre 2026 9h00 - 16h00