

# Microsoft 365 – Durcissement

4 jours (28 heures)

Expertise

Présentiel ou classe à distance

à partir de

**3 140 € 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 :

- Identifier les principaux risques liés à un environnement Microsoft 365 selon une approche Zero Trust
- Prioriser les actions de durcissement à l'aide de Microsoft Secure Score
- Implémenter et gérer les identités, les habilitations et les accès conditionnels avec Microsoft Entra ID
- Mettre en oeuvre la protection des informations avec Microsoft Purview
- Encadrer les usages de l'IA générative dans Microsoft 365, notamment Microsoft 365 Copilot et Copilot Chat
- Implémenter et administrer la protection contre les menaces avec Microsoft Defender XDR
- Surveiller les incidents, les alertes et les journaux d'audit dans les portails Microsoft 365
- Mettre en oeuvre les principales mesures de conformité, de gouvernance, de DLP et de gestion des risques internes.

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

## À qui s'adresse cette formation ?

Administrateurs Microsoft 365 et toute personne impliquée dans la sécurité ou la conformité Microsoft 365.

### Prérequis

Avoir suivi la formation M365-ADM "Microsoft 365 – Administrer la suite complète" ou avoir les connaissances équivalentes.

# Programme

## 1 Pendant votre formation

### Microsoft 365 – Durcissement

Jour 1

#### Introduction aux risques

- Vue d'ensemble des principaux risques
- Introduction aux méthodes de durcissement
- Mettre en oeuvre une méthode adaptée au sein de son entité

#### Le principe du modèle Zero Trust

- Décliner les principes Zero Trust en contrôles Microsoft 365 : authentification forte, accès conditionnel, moindre privilège, supervision et remédiation
- Bonnes pratiques et gouvernance associée

#### Architecture Microsoft 365

- Tour d'horizon de l'architecture Microsoft 365 sous une vision sécurité
- Identifier les risques associés aux différentes parties
- Introduction aux outils de durcissement Microsoft
- Le chiffrement au sein de Microsoft 365
- Découverte de la console Sécurité et du "Secure Score"

#### Protection de l'identité

- Compréhension de l'identité sous Microsoft 365
- Planifier l'identité et l'authentification
- Créer, configurer et gérer des identités et des rôles
- Vue d'ensemble des spécificités liées à l'hybridation
- Implémenter une architecture Microsoft Entra Connect adaptée au contexte de l'organisation
- Identifier les points de défaillance
- Gérer les identités externes, telles que les partenaires ou clients

#### Gestion de l'identité sécurisée

- Mise en oeuvre d'une stratégie d'authentification adaptée
- Introduction à Microsoft Entra
- Configurer les attributs de sécurité
- Mettre en oeuvre les méthodes d'authentification modernes : MFA, passwordless, FIDO2, Windows Hello Entreprise, OATH, accès conditionnel et protection des identités à risque
- Mise en oeuvre
  - Des packages de gouvernance de l'identité

- Des Conditional Access Policies
- Revue des accès utilisateurs
- Compréhension des sécurités par défaut
- Gérer
  - La protection par mot de passe et les seuils de verrouillage
  - L'élévation de l'accès
  - Le contrôle d'application et le contrôle des sessions
- Mettre en oeuvre
  - De l'accès privilégié
  - Microsoft Entra ID Protection

## Jour 2

### Microsoft Defender XDR et protection contre les menaces

- Présenter les principaux composants de Microsoft Defender XDR
- Mise en oeuvre de Defender for Endpoint
- Durcissement des postes clients consommateurs de Microsoft 365 (MDM, MAM)
- Présenter Microsoft Intune et les modèles de durcissement associés
- Exploiter la corrélation des alertes, l'investigation guidée et les actions de remédiation
- Valider les capacités de détection et de réponse au moyen de simulations d'attaque

### Administration de la détection et de la réponse aux menaces

- Administrer les alertes, les incidents et la remédiation dans Microsoft Defender XDR
- Exploiter les capacités d'investigation guidée et de réponse automatisée
- Coordonner les actions de protection sur les identités, postes et applications cloud
- Suivre les recommandations de sécurité opérationnelle issues des portails Microsoft

### Transition vers la protection des données et des usages IA

- Identifier les risques de surexposition des données dans Microsoft 365 et les usages IA

## Jour 3

### Microsoft Purview, protection des données et IA

- Appréhender les différents types de données
- Introduction à Microsoft Purview Information Protection
- Encadrer les usages de Microsoft 365 Copilot, Copilot Chat et des outils d'IA générative par les contrôles de conformité, d'audit et de protection des données
- Utiliser Data Security Posture Management pour identifier et réduire les risques liés aux données sensibles exposées aux scénarios IA
- Implémenter l'empreinte des données
- Gérer les niveaux de confidentialité

- Exploiter les types d'informations sensibles, les classificateurs, les étiquettes de confidentialité et les explorateurs de contenu et d'activité
- Appliquer des protections emails / fichiers basées sur les étiquettes
- Mise en oeuvre
  - De Microsoft Purview et des DLP
  - Des stratégies de protection contre la perte des données
- Gérer la rétention et le cycle de vie des données (DLM) au sein de l'architecture
  - Exchange
  - Teams
  - SharePoint
  - OneDrive...

### Gérer le risque interne

- Comprendre le fonctionnement des politiques, des alertes, des cas et des contrôles de confidentialité associés
  - Alertes
  - Actions
  - Modèles
  - Mises en évidence
- Introduction à Lockbox

Jour 4

### Surveiller l'architecture

- Introduction à :
  - Microsoft Sentinel, introduction à l'architecture SIEM / XDR
  - L'intégration Microsoft Defender XDR / Microsoft Sentinel pour comprendre la corrélation des signaux et les principes d'investigation SOC
  - Microsoft Purview eDiscovery
- Mise en oeuvre des journaux d'audits
- Recherche de contenu

### Les bonnes pratiques de durcissement

- Bonnes pratiques de durcissement au sein de :
  - Microsoft Exchange Online
  - SharePoint Online
  - OneDrive
  - Teams
- Bonnes pratiques de Microsoft 365

*Exemples de travaux pratiques (à titre indicatif)*

- Analyser Microsoft Secure Score afin de prioriser les actions de durcissement
- Mettre en place Microsoft Defender dans le cadre d'un durcissement généralisé
- Mettre en place le JIT JEA
- Durcir Microsoft Entra en respectant les bonnes pratiques
- Créer une stratégie d'accès conditionnel fondée sur le niveau de risque
- Durcir Microsoft Exchange et SharePoint Online en respectant les bonnes pratiques
- Vue d'ensemble de cas d'usages
- Investiguer un incident simulé dans Microsoft Defender XDR
- Contrôler un scénario d'usage IA avec Microsoft Purview : étiquettes de confidentialité, DLP et audit des interactions Copilot
- Surveiller et bloquer une attaque

## 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 2 février 2027 au 5 février 2027 (4 jours / 28 heures)

Paris La Défense

Du 2 février 2027 au 5 février 2027 Paris La Défense

- 2 février 2027 ..... 9h00 – 15h30
- 3 février 2027 ..... 9h00 – 15h30
- 4 février 2027 ..... 9h00 – 15h30
- 5 février 2027 ..... 9h00 – 15h30