

Microsoft Defender – Sécuriser vos ressources

2 jours (14 heures)

Expertise

Présentiel ou classe à distance

à partir de

1 470 € 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 :

- Expliquer le rôle de Microsoft Defender dans une stratégie de sécurité moderne
- Identifier les usages des principaux services Microsoft Defender
- Préparer le déploiement : prérequis, licences, rôles et périmètre de protection
- Configurer les protections de base et les recommandations prioritaires
- Analyser les incidents, alertes et vulnérabilités dans le portail Microsoft Defender
- Mettre en oeuvre les principales actions d'investigation et de remédiation
- Suivre l'évolution de la posture de sécurité à l'aide des tableaux de bord et rapports.

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

À qui s'adresse cette formation ?

Administrateurs Microsoft 365, administrateurs sécurité, ingénieurs système, administrateurs postes de travail et analystes SOC chargés de déployer, superviser ou améliorer la sécurité d'un environnement Microsoft.

Prérequis

Avoir suivi la formation M365-ADM "Microsoft 365 – Administrer la suite complète" ou disposer de connaissances équivalentes sur Microsoft 365, Microsoft Entra ID, Windows 10/11, les principes de sécurité réseau et l'administration des postes de travail. Une première expérience de l'administration Microsoft 365 ou de la sécurité opérationnelle est recommandée.

Programme

1 Pendant votre formation

Microsoft Defender – Sécuriser vos ressources

Jour 1 – Comprendre l'écosystème Microsoft Defender

- Comprendre les principaux risques : phishing, compromission d'identités, ransomwares, Shadow IT, postes non conformes et environnements hybrides
- Situer Microsoft Defender XDR dans une démarche Zero Trust et de supervision sécurité
- Identifier les périmètres couverts : endpoints, messagerie, identités, applications SaaS, workloads cloud et signaux XDR
- Découvrir le portail Microsoft Defender : incidents, alertes, Secure Score et recommandations
- Identifier les prérequis, rôles, licences et responsabilités avant déploiement

Identifier les services Microsoft Defender

- Comprendre le rôle de Microsoft Defender XDR comme point de corrélation et de réponse
- Defender for Endpoint : protection et supervision des postes et serveurs
- Defender for Office 365 : protection de la messagerie et des outils collaboratifs
- Defender for Identity : détection des risques liés aux identités hybrides
- Defender for Cloud Apps : gouvernance SaaS, Shadow IT et applications à risque
- Defender for Cloud : protection des workloads cloud et environnements hybrides
- Positionner Defender Antivirus et Defender for IoT selon les contextes rencontrés

Préparer et déployer les protections de base

- Préparer le déploiement : gouvernance, rôles, licences, connecteurs et périmètre de protection
- Configurer les paramètres initiaux et les politiques de protection de base
- Onboarder les endpoints et vérifier l'état de santé de l'environnement
- Lire les recommandations prioritaires et les indicateurs de posture

Exemples de travaux pratiques (à titre indicatif)

- Explorer le portail Microsoft Defender et identifier les services activés
- Vérifier les prérequis de déploiement et l'état de santé global
- Simuler l'onboarding d'un endpoint et contrôler sa remontée dans Defender
- Consulter le Secure Score et identifier les recommandations prioritaires

Jour 2 – Exploiter Microsoft Defender au quotidien

- Analyser les incidents et alertes corrélés dans Microsoft Defender
- Lire la chronologie d'un incident, les entités impactées, les preuves et les recommandations
- Mettre en oeuvre les actions de réponse : isolation, collecte d'investigation, analyse, quarantaine et remédiation automatisée
- Exploiter les recommandations de vulnérabilité pour prioriser les corrections

- Superviser les règles de réduction de surface d'attaque, la protection réseau, la protection web et l'accès contrôlé aux dossiers
- Utiliser la chasse avancée, en mode guidé ou avec KQL, pour rechercher des indicateurs de compromission
- Documenter les actions menées et enrichir les incidents à partir des résultats d'analyse
- Exploiter les tableaux de bord, rapports et automatisations pour suivre la posture de sécurité

Exemples de travaux pratiques (à titre indicatif)

- Qualifier un incident Defender XDR
- Appliquer une action de remédiation sur un endpoint
- Tester une règle de réduction de surface d'attaque en mode audit puis blocage
- Construire une requête de chasse avancée simple

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 5 octobre 2026 au 6 octobre 2026 (2 jours / 14 heures)

Blois

Du 5 octobre 2026 au 6 octobre 2026

Blois

- 5 octobre 2026 9h00 – 16h30
- 6 octobre 2026 9h00 – 16h30