MFE-IT

Référence : MD-4011

Formation Intune et Security Copilot (MD-4011)

Sécuriser les endpoints avec Intune, Defender et Security Copilot

Durée : 1 jour | Nombre d'heures : 6 h

Distanciel · Sessions garanties dès 1 inscrit · 60 % de travaux pratiques

DESCRIPTION

Cette formation intensive d'une journée vous apprend à renforcer la sécurité des endpoints en combinant Microsoft Intune, Microsoft Defender for Endpoint et Microsoft Security Copilot. Alignée sur le cours officiel Microsoft MD-4011, elle couvre la préparation d'Entra ID et Intune, l'inscription et la configuration des appareils, la conformité, l'Accès conditionnel, le durcissement des postes et la remédiation accélérée par l'IA. Elle prolonge la formation Microsoft Intune pour équipe support IT et s'inscrit dans la continuité de la formation Microsoft 365 MS-102.

Rythmée par une majorité de travaux pratiques, la journée vous conduit d'un tenant prêt pour la gestion des appareils jusqu'à une posture de sécurité surveillée et défendue : profils de configuration, stratégies de conformité, protection des données, bases de référence Defender, règles ASR, puis investigation et recommandations générées par Security Copilot. Les sessions se déroulent en petit groupe de 1 à 3 participants.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, vous serez capable de :

- Préparer Entra ID et Intune (identité, licences, Autopilot, BYOD) pour la gestion des appareils.
- Inscrire, valider et dépanner les appareils dans Microsoft Intune.
- Configurer profils, stratégies de conformité et remédiation automatique via des groupes dynamiques.
- Protéger les données et contrôler l'accès avec les stratégies de protection d'applications et l'Accès conditionnel.
- Renforcer les endpoints avec les bases de référence et Microsoft Defender for Endpoint (règles ASR, posture).
- Accélérer l'investigation et la remédiation avec Microsoft Security Copilot.

PRÉREQUIS

Parce que chaque participant est unique, un entretien préalable ajuste le contenu. Une maîtrise de base de la gestion des appareils et des opérations de sécurité est recommandée pour tirer pleinement parti de la journée.

PUBLIC VISÉ

Cette formation vise les administrateurs d'endpoints, les analystes sécurité (SecOps), les administrateurs Microsoft 365 et les ingénieurs sécurité chargés de la gestion et de la protection des appareils.

PROGRAMME DÉTAILLÉ

La formation alterne apports théoriques et travaux pratiques (environ 60 % du temps). Les modules sont construits autour d'exercices pratiques inspirés de cas d'usage métier concrets.

Module 1 — Préparer Entra ID et Intune pour la gestion des appareils

- Configurer l'identité, les licences et les paramètres du tenant pour l'inscription des appareils.
- Explorer les méthodes d'inscription manuelle.
- Mettre en œuvre Windows Autopilot.
- Prendre en charge les scénarios BYOD (appareils personnels).

Module 2 — Inscrire et valider les appareils avec Intune

- Réaliser l'inscription des appareils dans Microsoft Intune.
- Valider la jonction et l'état de gestion des appareils.
- Configurer les restrictions d'inscription.
- Dépanner les problèmes d'inscription courants.

Module 3 — Configurer et sécuriser les appareils

- Créer et déployer des profils de configuration.
- Mettre en place des stratégies de conformité.
- Cibler les déploiements avec des groupes dynamiques.
- Automatiser la remédiation des appareils non conformes.

Module 4 — Protéger les données et contrôler l'accès

- Protéger les données d'entreprise sur appareils gérés et non gérés (stratégies de protection d'applications).
- Contrôler l'accès aux ressources de l'organisation.
- Appliquer conformité et exigences de sécurité via l'Accès conditionnel Microsoft Entra.

Module 5 — Renforcer les endpoints et surveiller la sécurité

- Déployer les bases de référence de sécurité Microsoft.
- Intégrer les appareils à Microsoft Defender for Endpoint.
- Configurer les règles de réduction de la surface d'attaque (ASR).
- Surveiller la posture de sécurité et répondre aux menaces.

Module 6 — Accélérer la remédiation avec Security Copilot

- Exploiter les capacités d'investigation assistées par IA de Security Copilot.
- Analyser les incidents de sécurité.
- Dépanner les problèmes d'appareils.
- Générer des recommandations de remédiation entre Intune et Defender for Endpoint.

LES PLUS DE LA FORMATION

- Une pédagogie orientée cas réels sur un environnement Microsoft 365.
- La combinaison Intune + Defender + Security Copilot, au cœur de la sécurité moderne des endpoints.
- Un petit groupe (1 à 3 participants) et un accompagnement de 30 jours.

MÉTHODES PÉDAGOGIQUES

Format et déroulement

Formation en distanciel, en groupe de 1 à 3 participants, à raison de 6 h par jour. Le présentiel peut se dérouler directement sur votre site, et le distanciel peut être enregistré à la demande. Environ 60 % du temps est consacré aux travaux pratiques sur un environnement Microsoft 365 de démonstration. Un entretien préalable permet d'adapter le contenu au profil de chaque participant. Les sessions inter-entreprises sont garanties dès 1 seul inscrit (pas de risque de report sauf cas de force majeure).

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants à l'aide de questions à choix multiples, de mises en situation et de travaux pratiques. À l'issue, une attestation de réussite est remise à chaque participant.

Accompagnement post-formation

Pendant un mois après la formation, chaque participant peut contacter les formateurs MFE-IT pour toute question relative à la mise en œuvre des connaissances acquises. Une réponse est apportée par e-mail ou par téléphone sous 48 heures ouvrées.

Accessibilité

MFE-IT s'engage à accueillir les personnes en situation de handicap. Contact : contact@mfe-it.com.

INFORMATIONS PRATIQUES

Ressources du formateur

- Démonstrations structurées alignées sur le programme détaillé
- Énoncés d'exercices et corrigés tout au long de la formation
- Un environnement technique prêt à l'emploi pour les ateliers pratiques
- Validation des acquis par le formateur à la fin de chaque atelier
- Documents de référence au format numérique

Certification et validation

À l'issue de la formation, une attestation est envoyée par e-mail précisant les objectifs, la nature, la durée et les résultats de l'évaluation. Une attestation de fin de formation peut également être fournie sur demande.

Bénéfices pour les participants

- Se former depuis son lieu de travail ou son domicile, sans déplacement
- Bénéficier d'un formateur-consultant expert du sujet
- Profiter d'un format ultra-personnalisé (1 à 3 participants)
- Poursuivre la formation même en cas d'imprévu

Bénéfices pour l'organisation

- Proposer une formation de qualité à tous les collaborateurs, où qu'ils soient
- Limiter les déplacements et leur logistique
- Réduire les temps d'absence liés aux déplacements
- Soutenir la montée en compétences des équipes dans tous les contextes