# Améliorer la sécurité des points de terminaison avec Microsoft Intune et Microsoft Security Copilot (MD4011)

Durée: 1 jour
Public cible: Professionnel TI

## À qui s'adresse cette formation ?

Ce cours s’adresse aux administrateurs de points de terminaison et aux analystes en sécurité qui maîtrisent les opérations de base en gestion des appareils et en sécurité.

## Objectifs de la formation

À

la fin de ce cours, les participants seront en mesure de :

- Configurer les rôles Microsoft Entra ID, les licences et les paramètres du locataire pour la gestion des appareils
- Enregistrer et valider des appareils Windows, iOS, iPadOS et Android
- Créer et déployer des profils de configuration et des stratégies de conformité avec Microsoft Intune
- Mettre en œuvre des stratégies de protection des applications et de l’accès conditionnel pour prévenir la perte de données
- Déployer des configurations de sécurité de base et intégrer les appareils à Microsoft Defender pour Endpoint
- Configurer les règles de réduction de la surface d’attaque et surveiller la posture de sécurité
- Exploiter Microsoft Security Copilot pour l’enquête sur les incidents et le dépannage des appareils grâce à l’IA

## Description sommaire

Ce cours permet aux professionnels TI et aux analystes en sécurité d’acquérir l’expertise nécessaire pour utiliser efficacement Microsoft Intune et Microsoft Security Copilot dans les opérations de gestion des appareils et de sécurité.

Il guide les apprenants vers l’optimisation d’Intune pour renforcer la sécurité et l’intégration de Security Copilot afin d’améliorer la posture de sécurité de leur organisation.

## Contenu du plan de cours

**Parcours d’apprentissage 1 : Renforcer la sécurité des points de terminaison avec Microsoft Intune et Microsoft Security Copilot**

- Module 1 : Préparer Microsoft Entra ID et Intune pour la gestion des appareils
- Module 2 : Enregistrer et valider les appareils avec Microsoft Intune
- Module 3 : Configurer et sécuriser les appareils avec les stratégies Intune
- Module 4 : Protéger les données et contrôler l’accès avec Microsoft Intune et l’accès conditionnel
- Module 5 : Durcir les points de terminaison et surveiller la sécurité avec Microsoft Intune et Defender for Endpoint
- Module 6 : Accélérer la remédiation et la réponse aux incidents avec Microsoft Security Copilot

## Approche et méthode pédagogique

Approche pratique et structurée combinant une théorie ciblée et des ateliers guidés orientés vers la sécurité. Les participants développent progressivement leur expertise en protection des points de terminaison en appliquant Microsoft Intune et Microsoft Security Copilot à des scénarios opérationnels inspirés de situations réelles.

À travers des exercices concrets, ils apprennent à optimiser les configurations de sécurité des appareils, analyser les signaux de sécurité pertinents et intégrer Copilot dans les processus d’enquête sur les incidents afin d’améliorer l’efficacité de la réponse.

Animée par un formateur certifié Microsoft (MCT), la formation met l’accent sur l’interactivité, les démonstrations pratiques et le développement de compétences immédiatement transférables aux opérations modernes de sécurité des points de terminaison.

## Prérequis

Les participants devraient posséder les connaissances et l’expérience suivantes avant de suivre ce cours :

- Familiarité avec les services et l’administration Microsoft 365
- Compréhension de base de Microsoft Entra ID (anciennement Azure Active Directory)
- Expérience avec les concepts de gestion des appareils Windows 10/11
- Compréhension des concepts de sécurité, incluant l’authentification, l’autorisation et le chiffrement

## Recommandations

- Compréhension de base des principes de sécurité informatique.
- Familiarité avec Microsoft Intune.
- Expérience de la gestion des appareils dans un environnement d''entreprise.
- Connaissance de Microsoft Entra ID.
- Accès aux outils Microsoft Intune et Copilot pour la sécurité pour des exercices pratiques