

Renforcer la sécurité des points de terminaison avec Microsoft Intune et Microsoft Copilot for Security

Sécurisez vos endpoints avec l'IA et l'administration centralisée

 A distance



7 h

Prix inter : 950,00 € HT
Forfait intra : 2.850,00 € HT

Réf.: MSMD4011

Ce parcours guide les professionnels IT dans l'**utilisation de Microsoft Intune et Copilot** pour **protéger et sécuriser les points de terminaison**. À travers des modules progressifs, il enseigne comment évaluer la posture de sécurité, configurer des profils de sécurité, appliquer les stratégies de conformité, et analyser les données de sécurité avec Copilot.

Les participants découvrent également comment **automatiser la détection des menaces, répondre aux incidents et améliorer la protection des appareils Windows**. Grâce à l'intégration native de Microsoft Defender for Endpoint et de Copilot dans Intune, ce programme permet d'**optimiser la gestion des risques et la conformité des endpoints** dans un environnement cloud moderne.

A qui s'adresse cette formation ?



Pour qui

- Administrateurs
- Ingénieurs en sécurité
- Analystes des opérations de sécurité



Prérequis

- Connaître les bases des principes de la sécurité informatique
- Être familiarisé avec Microsoft Intune
- Avoir accès à un abonnement Microsoft 365 (BYOS) dans lequel le participant est autorisé à utiliser Microsoft 365 Copilot et Microsoft Intune (afin de réaliser les exercices prévus lors de la formation)
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

Programme

1 - Découvrir les éléments essentiels de Microsoft Intune

- Comprendre le concept de jonction d'appareils à Microsoft Entra ID
- Identifier les prérequis, les limitations et les avantages de la jonction à Microsoft Entra
- Procéder à la jonction d'un appareil à Microsoft Entra ID
- Administrer les appareils enregistrés et joints à Microsoft Entra ID

2 - Déverrouiller des insights avec Microsoft Copilot pour la sécurité

- Découvrir Microsoft Copilot pour la sécurité : fonctionnalités clés, intégration et cas d'usage
- Comprendre l'intégration de Copilot Sécurité dans les écosystèmes Microsoft
- Explorer les différentes expériences : autonomes ou intégrées dans les outils de cybersécurité
- Déployer et configurer Microsoft Copilot pour la sécurité dans votre environnement
- Formuler des requêtes efficaces avec des prompts adaptés à la cybersécurité
- Concevoir et utiliser des séquences d'invites pour automatiser les analyses
- Prendre en main les nouveautés et améliorations de Copilot pour la sécurité (version Mai 2024)

- Adopter une approche éthique avec les principes de l'IA responsable dans Copilot Sécurité

3 - Optimiser Microsoft Intune pour l'intégration de Copilot pour la sécurité

- Utiliser Microsoft Copilot pour la sécurité et Intune pour renforcer la gestion et la protection des terminaux
- Définir et appliquer des conventions de nommage efficaces pour les appareils
- Renommer et administrer les appareils dans Microsoft Intune
- Créer, organiser et gérer des groupes d'appareils et d'utilisateurs dans Intune
- Comprendre les mécanismes d'authentification et de gestion des rôles dans Copilot pour la sécurité
- Intégrer Copilot pour la sécurité avec Microsoft Intune pour des scénarios avancés de protection
- Concevoir et utiliser des prompts personnalisés dans Microsoft Copilot pour la sécurité
- Créer des invites adaptées aux scénarios de gestion d'appareils dans Microsoft Intune



Les objectifs de la formation

- Découvrir Microsoft Intune essentiels : fonctionnalités de gestion des devices, applications et données
- Comprendre le fonctionnement et l'intégration de Microsoft Copilot for Security
- Déployer Microsoft Copilot for Security pour améliorer la sécurité des endpoints
- Utiliser des prompts et promptbooks dans Microsoft Copilot for Security
- Implémenter des conventions de nommage efficaces, renommer des devices et gérer des groupes dans Intune
- Intégrer Microsoft Copilot for Security avec Microsoft Intune via des prompts personnalisés



Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



Les points forts de la formation

- L'apprentissage par la pratique : les apports théoriques sont consolidés par des mises en situation concrètes
- Utilisation d'environnements proches du contexte professionnel
- Le développement de compétences durables pour prévenir et réagir face aux menaces sur les terminaux



Dates 2025 - Référence MSMD4011



Dernières places disponibles



Session garantie

le 8 déc.

- le 8 déc. 9h00 -> 17h00