Protégez-vous contre les cybermenaces avec Microsoft Defender XDR (SC-5004)

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Professionnels de la sécurité informatique
- Analystes SOC (Security Operations Center)
- Administrateurs système et réseau
- Ingénieurs en cybersécurité
- Professionnels des technologies de l'information
- Consultants en sécurité

Objectifs de la formation

- Comprendre Microsoft Defender XDR
- Détection et investigation des menaces
- Configuration et gestion des solutions Defender
- Techniques de réponse aux incidents
- Intégration avec les opérations de sécurité
- Utilisation des fonctionnalités de protection avancée contre les menaces
- Mise en œuvre des meilleures pratiques

Description sommaire

Déployez Microsoft Defender pour Endpoint pour gérer les appareils, enquêter sur les points de terminaison, gérer les incidents avec Defender XDR et utiliser Advanced Hunting avec Kusto Query Language (KQL) pour détecter des menaces spécifiques.

Contenu du plan de cours

- Atténuer les incidents à l'aide de Microsoft Defender
- Déployer l'environnement Microsoft Defender pour Endpoint

- Configurer les alertes et les détections dans Microsoft Defender pour Endpoint
- Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour Endpoint
- Effectuer des investigations sur les appareils dans Microsoft Defender pour Endpoint
- Défendez-vous contre les cybermenaces avec les exercices de laboratoire Microsoft Defender XDR

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés.

Les participants se protègent progressivement contre les cybermenaces avec Microsoft Defender XDR à travers des exercices concrets inspirés de scénarios professionnels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à détecter, analyser et répondre aux incidents de sécurité en utilisant une plateforme unifiée de protection et de réponse étendue.

Animée par un formateur certifié Microsoft, la formation privilégie l’interactivité et le développement de compétences techniques directement transférables pour renforcer la sécurité des environnements en contexte professionnel.

Prérequis

- Expérience d'utilisation du portail Microsoft Defender
- Compréhension de base de Microsoft Defender pour Endpoint
- Compréhension de base de Microsoft Sentinel
- Expérience d'utilisation du langage de requête Kusto (KQL) dans Microsoft Sentinel

Recommandations

Réviser :

- Les bases de la cybersécurité
- Les types de menaces et attaques courantes

Se familiariser avec :

-

L’écosystème Microsoft (Microsoft 365, sécurité)

Identifier vos besoins :

- Détection des menaces
- Protection des utilisateurs et systèmes
- Amélioration de la posture de sécurité