Analyse de sécurité avec Microsoft (SC-200)

Date et durée

Code formation : SC-200
Durée : 4 jours
Nombre d'heures : 28 heures

Description

La formation **Analyse de sécurité avec Microsoft (SC-200)** est conçue pour les professionnels de la sécurité souhaitant acquérir les compétences pour détecter, répondre et résoudre efficacement les menaces de sécurité avec les outils Microsoft. Grâce à des solutions comme Microsoft Sentinel, Microsoft 365 Defender et Azure Defender, cette formation permet aux participants de maîtriser l'analyse des menaces et la mise en œuvre de stratégies de réponse pour renforcer la posture de sécurité de leur organisation.

Objectifs

- **Détecter** et analyser les menaces de sécurité avec Microsoft Sentinel.
- **Utiliser Microsoft 365 Defender** pour identifier et remédier aux incidents de sécurité sur les endpoints.
- **Maîtriser Azure Defender** pour la protection des ressources cloud et hybrides.
- **Automatiser les réponses** aux incidents pour une efficacité accrue dans la gestion des menaces.

Points forts

Formation certifiante, animée par des experts Microsoft, avec un programme officiel en français incluant des labs pour une maîtrise pratique des outils Sentinel et Defender.

Certification

Cette formation prépare au passage de l'examen SC-200, permettant d'obtenir la certification **Microsoft Certified: Security Operations Analyst Associate**. Cette certification atteste de votre expertise en gestion et réponse aux incidents de sécurité avec les solutions Microsoft, un atout pour renforcer votre profil de professionnel de la sécurité.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

- Connaissance de base des concepts de sécurité informatique, notamment sur la détection des menaces et la réponse aux incidents.
- Expérience pratique avec les environnements Microsoft et les services de sécurité cloud.

Public

- Professionnels de la sécurité informatique cherchant à optimiser leurs compétences en détection et gestion des menaces.
- Analystes de sécurité et ingénieurs responsables de la protection des environnements Microsoft.
- Administrateurs souhaitant se spécialiser dans l'analyse de la sécurité avec Microsoft Sentinel, Microsoft 365 Defender et Azure Defender.

Programme

Module 1 : Introduction à Microsoft Sentinel pour la détection des menaces

- Configuration de Microsoft Sentinel et création de workspaces dédiés.
- Intégration des connecteurs de données pour collecter des logs de sources diverses.
- Création de requêtes KQL (Kusto Query Language) pour rechercher des menaces dans les logs.
- Construction de playbooks automatisés pour gérer les incidents.
- **Lab :** Configuration de Sentinel, connexion de sources de données et détection de menaces avec KQL.

Module 2 : Gestion des incidents et investigation avec Microsoft 365 Defender

- Introduction aux fonctionnalités de Microsoft 365 Defender pour la détection des menaces.
- Gestion des alertes de sécurité et investigation des incidents dans le centre de sécurité.
- Analyse des menaces et corrélation des signaux pour détecter des attaques sophistiquées.
- Implémentation des stratégies de réponse et des automatisations pour les incidents.
- **Lab :** Investigation d'incidents, configuration d'alertes et automatisation des réponses avec Microsoft 365 Defender.

Module 3 : Protection avancée avec Azure Defender

- Présentation d'Azure Defender et de ses fonctionnalités de protection pour les environnements cloud et hybrides.
- Configuration des alertes de sécurité et détection des vulnérabilités sur les ressources Azure.
- Détection des menaces sur les réseaux, bases de données et conteneurs avec Azure Defender.
- **Lab :** Protection d'un environnement hybride avec Azure Defender et gestion des alertes de sécurité.

Module 4 : Optimisation et automatisation de la réponse aux incidents

- Introduction aux workflows d'automatisation pour la réponse aux incidents.
- Création de playbooks avancés avec Logic Apps pour automatiser les réponses aux menaces.
- Optimisation des stratégies de sécurité et gestion centralisée des incidents avec Microsoft Sentinel.
- Exploitation des données de surveillance pour améliorer la détection de nouvelles menaces.
- **Lab :** Création de playbooks automatisés et optimisation de la gestion des incidents.