Se défendre contre les cybermenaces avec Microsoft Defender XDR (SC-5004)

Description

Protégez votre organisation contre les cybermenaces

Les cyberattaques sont de plus en plus sophistiquées et peuvent compromettre la sécurité de votre entreprise en quelques instants. La maîtrise des outils de détection et de réponse aux incidents est essentielle pour garantir une protection efficace. Avec la formation SC-5004, vous apprendrez à utiliser Microsoft Defender XDR pour surveiller, analyser et neutraliser les menaces en temps réel.

Maîtrisez Microsoft Defender XDR et améliorez votre sécurité

Cette formation vous permet de déployer et configurer Microsoft Defender for Endpoint, d'investiguer les alertes et d'automatiser la réponse aux incidents. Vous découvrirez comment gérer les appareils, analyser les journaux et utiliser le langage de requête Kusto (KQL) pour identifier les attaques ciblées. Grâce à un apprentissage structuré et des exercices pratiques, vous développerez des compétences opérationnelles en cybersécurité.

Destinée aux analystes en sécurité, cette formation approfondie vous donnera les clés pour exploiter pleinement Microsoft Defender et renforcer la résilience de votre organisation face aux cybermenaces.

Niveau
Intermédiaire
Contenu du cours
Module 1 : Réduire le nombre d'incidents avec Microsoft Defender

- Utiliser le portail Microsoft Defender
- Gérer les incidents et examiner les alertes
- Investiguer les incidents avec Microsoft Defender XDR
- Gérer les enquêtes automatisées
- Explorer la recherche avancée de menaces
- Examiner les journaux de connexion Microsoft Entra
- Comprendre le niveau de sécurité Microsoft
- Analyser les menaces et les rapports
- Configurer le portail Microsoft Defender

Module 2 : Déployer l'environnement Microsoft Defender pour point de terminaison

- Créer et configurer l'environnement de sécurité
- Comprendre la compatibilité des systèmes d'exploitation
- Intégrer et gérer les appareils
- Gérer les accès et les rôles
- Configurer les groupes d'appareils et les fonctionnalités avancées

Module 3 : Configurer les alertes et les détections

- Configurer les fonctionnalités avancées

- Gérer les notifications d’alerte
- Administrer la suppression d’alerte
- Activer et gérer les indicateurs de détection

Module 4 : Automatiser la réponse aux incidents

- Configurer l’automatisation dans Microsoft Defender
- Gérer les paramètres de téléchargement et d’investigation
- Bloquer les appareils à risque

Module 5 : Enquêter sur les appareils avec Microsoft Defender

- Utiliser la liste d’inventaire des appareils
- Examiner les appareils et bloquer les comportements suspects
- Détecter les appareils via la découverte automatique

Module 6 : Se défendre contre les cybermenaces avec Microsoft Defender XDR

- Configurer l’environnement Microsoft Defender XDR
- Déployer Microsoft Defender for Endpoint
- Atténuer les attaques avec Microsoft Defender

Lab / Exercices

- Ce cours vous donne un accès exclusif au laboratoire officiel Microsoft, vous permettant de mettre en pratique vos compétences dans un environnement professionnel.

Documentation

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

Profils des participants

- Analystes des opérations de sécurité
- Experts en cybersécurité
- Administrateurs systèmes et réseaux
- Responsables de la gestion des incidents

Connaissances Préalables

- Expérience avec le portail Microsoft Defender
- Notions de base sur Microsoft Defender for Endpoint
- Compréhension élémentaire de Microsoft Sentinel

Objectifs

- Utiliser le portail Microsoft Defender pour gérer les incidents
- Déployer et configurer Microsoft Defender for Endpoint
- Configurer les alertes et les détections de menaces
- Automatiser la gestion des incidents et des appareils
- Analyser les menaces et exploiter les journaux de connexion
- Utiliser le langage de requête Kusto (KQL) pour investiguer les attaques

Description

Se défendre contre les cybermenaces avec Microsoft Defender XDR (SC-5004)
Prix de l'inscription en Présentiel (CHF)
900
Prix de l'inscription en Virtuel (CHF)
850
Durée (Nombre de Jours)
1
Reference
SC-5004