Analyste des opérations de sécurité Microsoft (SC-200T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

L'analyste des opérations de sécurité de Microsoft collabore avec les parties prenantes de l'organisation pour sécuriser les systèmes de technologie de l'information de l'organisation. Son objectif est de réduire le risque organisationnel en remédiant rapidement aux attaques actives dans l'environnement, en donnant des conseils sur les améliorations à apporter aux pratiques de protection contre les menaces et en signalant les violations des politiques organisationnelles aux parties prenantes appropriées. Les responsabilités comprennent la gestion, la surveillance et la réponse aux menaces en utilisant une variété de solutions de sécurité dans leur environnement. Le rôle consiste principalement à enquêter sur les menaces, à y répondre et à les chasser en utilisant Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender et des produits de sécurité tiers. Puisque l'analyste des opérations de sécurité consomme le résultat opérationnel de ces outils, il est également une partie prenante essentielle dans la configuration et le déploiement de ces technologies.

Objectifs de la formation

- Expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement.
- Créer un environnement Microsoft Defender pour Endpoint.
- Configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10.

Description sommaire

Apprenez à enquêter, répondre et rechercher des menaces en utilisant Microsoft Sentinel, Microsoft Defender XDR et Microsoft Defender pour le Cloud. Dans ce cours, vous apprendrez à atténuer les cybermenaces à l'aide de ces technologies. Plus précisément, vous allez configurer et utiliser Microsoft Sentinel, ainsi qu'exploiter le langage de requête Kusto (KQL) pour effectuer des détections, des analyses et des rapports. Ce cours est conçu pour les professionnels travaillant dans un rôle lié

aux opérations de sécurité et aide les apprenants à se préparer à l'examen SC-200 : Analyste des opérations de sécurité Microsoft.

Contenu du plan de cours

Parcours d'apprentissage 1 : Réduire les menaces avec Microsoft Defender XDR

- Introduction à la protection contre les menaces dans Microsoft 365
- Réduire les incidents à l'aide de Microsoft Defender XDR
- Protéger les identités avec Microsoft Entra ID Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protéger l'environnement avec Microsoft Defender pour l'identité
- Sécuriser les applications et services cloud avec Microsoft Defender pour les applications cloud

Parcours d'apprentissage 2 : Premiers pas avec Microsoft Copilot pour la sécurité

- Fondamentaux de l'IA générative
- Décrire Microsoft Copilot pour la sécurité
- Décrire les fonctionnalités principales de Microsoft Copilot pour la sécurité
- Décrire les expériences intégrées de Microsoft Copilot pour la sécurité

Parcours d'apprentissage 3 : Réduire les menaces avec Microsoft Purview

- Solutions de conformité Microsoft Purview
- Répondre aux alertes de prévention des pertes de données à l'aide de Microsoft Purview
- Gérer les risques internes avec Microsoft Purview
- Enquêter sur les menaces à l'aide de la recherche de contenu dans Microsoft Purview
- Enquêter sur les menaces à l'aide de l'audit Microsoft Purview

Parcours d'apprentissage 4 : Réduire les menaces avec Microsoft Defender pour Endpoint

- Protéger contre les menaces avec Microsoft Defender pour Endpoint
- Déployer l'environnement Microsoft Defender pour Endpoint
- Implémenter des améliorations de sécurité Windows avec Microsoft Defender pour Endpoint

- Effectuer des enquêtes sur les appareils dans Microsoft Defender pour Endpoint
- Effectuer des actions sur un appareil avec Microsoft Defender pour Endpoint
- Effectuer des enquêtes sur des preuves et des entités dans Microsoft Defender pour Endpoint
- Configurer et gérer l'automatisation avec Microsoft Defender pour Endpoint
- Configurer les alertes et détections dans Microsoft Defender pour Endpoint
- Utiliser la gestion des vulnérabilités dans Microsoft Defender pour Endpoint

Parcours d'apprentissage 5 : Réduire les menaces avec Microsoft Defender pour le Cloud

- Planifier la protection des charges de travail cloud avec Microsoft Defender pour le Cloud
- Connecter des ressources Azure à Microsoft Defender pour le Cloud
- Connecter des ressources non-Azure à Microsoft Defender pour le Cloud
- Gérer la posture de sécurité cloud • Expliquer la protection des charges de travail cloud dans Microsoft Defender pour le Cloud
- Remédier aux alertes de sécurité avec Microsoft Defender pour le Cloud

Parcours d'apprentissage 6 : Créer des requêtes pour Microsoft Sentinel à l'aide du langage KQL (Kusto Query Language)

- Construire des instructions KQL pour Microsoft Sentinel
- Analyser les résultats des requêtes à l'aide de KQL
- Créer des instructions multi-tables avec KQL
- Travailler avec des données dans Microsoft Sentinel à l'aide du langage Kusto Query Language

Parcours d'apprentissage 7 : Configurer votre environnement Microsoft Sentinel

- Introduction à Microsoft Sentinel
- Créer et gérer des espaces de travail Microsoft Sentinel
- Interroger les journaux dans Microsoft Sentinel
- Utiliser les listes de surveillance dans Microsoft Sentinel
- Utiliser les renseignements sur les menaces dans Microsoft Sentinel
- Intégrer Microsoft Defender XDR à Microsoft Sentinel

Parcours d'apprentissage 8 : Connecter des journaux à Microsoft Sentinel

- Connecter des données à Microsoft Sentinel à l'aide de connecteurs de données
- Connecter des services Microsoft à Microsoft Sentinel
- Connecter Microsoft Defender XDR à Microsoft Sentinel
- Connecter des hôtes Windows à Microsoft Sentinel
- Connecter des journaux au format Common Event Format à Microsoft Sentinel
- Connecter des sources de données syslog à Microsoft Sentinel
- Connecter des indicateurs de menace à Microsoft Sentinel

Parcours d'apprentissage 9 : Créer des détections et effectuer des enquêtes à l'aide de Microsoft Sentinel

- Détection des menaces avec l'analyse Microsoft Sentinel
- Automatisation dans Microsoft Sentinel
- Réponse aux menaces avec les playbooks Microsoft Sentinel
- Gestion des incidents de sécurité dans Microsoft Sentinel
- Identifier les menaces avec l'analyse comportementale des entités dans Microsoft Sentinel
- Normalisation des données dans Microsoft Sentinel
- Interroger, visualiser et surveiller des données dans Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel

Parcours d'apprentissage 10 : Effectuer des recherches de menaces dans Microsoft Sentinel

- Expliquer les concepts de recherche de menaces dans Microsoft Sentinel

- Recherche de menaces avec Microsoft Sentinel
- Utiliser les tâches de recherche dans Microsoft Sentinel
- Rechercher des menaces à l'aide de notebooks dans Microsoft Sentinel

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés.

Les participants configurent et exploitent progressivement les opérations de sécurité en tant qu'analyste SOC avec Microsoft Sentinel 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 les outils Microsoft de protection et de surveillance.

Animée par un formateur certifié Microsoft, la formation privilégie l'interactivité et le développement de compétences techniques directement transférables pour assurer la surveillance et la réponse aux menaces en contexte professionnel.

Prérequis

- Connaissances de base en sécurité, conformité et identité Microsoft Familiarité avec Microsoft 365 et les services Azure
- Compréhension générale des concepts de cybersécurité (détection, réponse aux incidents)

Recommandations

- Compréhension de base de Microsoft 365
- Compréhension fondamentale des produits Microsoft en matière de sécurité, de conformité et d'identité
- Compréhension intermédiaire de Microsoft Windows
- Familiarité avec les services Azure, spécifiquement Azure SQL Database et Azure Storage
- Familiarité avec les machines virtuelles Azure et les réseaux virtuels
- Compréhension de base des concepts de script