Azure Security Engineer Associate

Objectifs pédagogiques

- Créer un environnement Microsoft Defender pour Endpoint
- Configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10
- Rechercher des domaines et des adresses IP Microsoft Defender pour Endpoint
- Enquêter sur les comptes utilisateurs dans Microsoft Defender pour Endpoint
- Configurer les paramètres d'alerte dans Microsoft Defender pour Endpoint
- Gérer les incidents dans Microsoft 365 Defender
- Examiner les alertes DLP dans Microsoft Cloud App Security
- Configurer l'auto-provisioning dans Azure Defender
- Remédier aux alertes dans Azure Defender
- Construire des instructions KQL
- Gérer un espace de travail Azure Sentinel
- Utiliser KQL pour accéder à la liste de surveillance dans Azure Sentinel
- Gérer les indicateurs de menace dans Azure Sentinel
- Configurer l'agent Log Analytics pour collecter les événements Sysmon
- Créer de nouvelles règles et requêtes d'analyse à l'aide de l'assistant de règles d'analyse
- Utiliser des requêtes pour rechercher des menaces

Prérequis

- Connaissances de base de l'environnement Microsoft 365
- Connaissances de base sur les produits de sécurité, de conformité et d'identité de Microsoft
- Connaissance de Windows 10
- Être familiarisé avec certains services Azure, notamment Azure SQL Database et Azure Storage
- Connaissances autour des machines virtuelles Azure et les réseaux virtuels.
- Connaissance de bases sur le Scripting

Programme détaillé

Atténuation des menaces à l'aide de Microsoft Defender pour Endpoint

- Se protéger contre les menaces avec Microsoft Defender pour Endpoint
- Déployer l'environnement Microsoft Defender pour Endpoint
- Mettre en œuvre les améliorations de sécurité de Windows 10 avec Microsoft Defender pour Endpoint
- Gérer les alertes et les incidents dans Microsoft Defender pour Endpoint
- Effectuer des investigations sur les périphériques dans Microsoft Defender pour Endpoint
- Exécuter des actions sur un périphérique à l'aide de Microsoft Defender pour Endpoint
- Effectuer des enquêtes sur les preuves et les entités à l'aide de Microsoft Defender pour Endpoint
- Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour Endpoint
- Configurer les alertes et les détections dans Microsoft Defender pour Endpoint

- Utiliser la gestion des menaces et des vulnérabilités dans Microsoft Defender pour Endpoint
- Travaux pratiques : Atténuer les menaces à l'aide de Microsoft Defender pour Endpoint
    - Déployer Microsoft Defender pour Endpoint
    - Atténuer les attaques à l'aide de Defender for Endpoint

Atténuation des menaces à l'aide de Microsoft 365 Defender

- Introduction à la protection contre les menaces avec Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger vos identités avec Azure AD Identity Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protection de votre environnement avec Microsoft Defender for Identity
- Sécurisez vos applications et services en nuage avec Microsoft Cloud App Security
- Répondre aux alertes de prévention des pertes de données avec Microsoft 365
- Gérez les risques liés aux initiés dans Microsoft 365
- Travaux pratiques : Atténuer les menaces avec Microsoft 365 Defender
    - Atténuer les attaques avec Microsoft 365 Defender

Atténuer les menaces à l'aide de Azure Defender

- Planifier les protections des charges de travail en nuage à l'aide de Azure Defender
- Expliquer les protections des charges de travail en nuage dans Azure Defender.
- Connecter les ressources Azure à Azure Defender
- Connecter les ressources non-Azure à Azure Defender
- Corriger les alertes de sécurité à l'aide de Azure Defender
- Travaux pratiques : Atténuer les menaces à l'aide de Azure Defender
    - Déployer Azure Defender
    - Atténuer les attaques avec Azure Defender

Configuration de votre environnement Azure Sentinel

- Introduction à Azure Sentinel
- Créer et gérer les espaces de travail Azure Sentinel
- Interroger les journaux dans Azure Sentinel
- Utiliser les listes de surveillance dans Azure Sentinel
- Utiliser les renseignements sur les menaces dans Azure Sentinel
- Travaux pratiques : Configurer votre environnement Azure Sentinel
    - Créer un espace de travail Azure Sentinel
    - Créer une liste de surveillance
    - Créer un indicateur de menace

Connecter les journaux à Azure Sentinel

- Connecter des données à Azure Sentinel à l'aide de connecteurs de données
- Connecter les services Microsoft à Azure Sentinel
- Connecter Microsoft 365 Defender à Azure Sentinel
- Connecter les hôtes Windows à Azure Sentinel
- Connecter les journaux Common Event Format à Azure Sentinel

- Connecter des sources de données syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel
- Travaux pratiques : Connecter les journaux à Azure Sentinel
    - Connecter les services Microsoft à Azure Sentinel
    - Connecter les hôtes Windows à Azure Sentinel
    - Connecter les hôtes Linux à Azure Sentinel
    - Connecter les renseignements sur les menaces à Azure Sentinel

Créer des détections et effectuer des investigations à l'aide de Azure Sentinel

- Détection des menaces avec les analyses de Azure Sentinel
- Réponse aux menaces avec les manuels Azure Sentinel
- Gestion des incidents de sécurité dans Azure Sentinel
- Utiliser l'analyse du comportement des entités dans Azure Sentinel
- Interroger, visualiser et surveiller les données dans Azure Sentinel
- Travaux pratiques : Créer des détections et effectuer des enquêtes en utilisant Azure Sentinel
    - Créer des règles analytiques
    - Modéliser les attaques pour définir la logique des règles
    - Atténuer les attaques à l'aide de Azure Sentinel
    - Créer des classeurs dans Azure Sentinel

Effectuer la chasse aux menaces dans Azure Sentinel

- Chasse aux menaces avec Azure Sentinel
- Chasse aux menaces à l'aide de notebooks dans Azure Sentinel
- Travaux pratiques : Chasse aux menaces dans Azure Sentinel
    - Chasse aux menaces dans Azure Sentinel
    - Chasse aux menaces à l'aide de notebooks