Programme de cours
Microsoft Security Operations Analyst

Durée :	4 jours soit 28 heures	Référence :	SC-200T00

Public visé :

Cette formation est destinée aux informaticiens qui doivent découvrir, rechercher et répondre aux menaces à l'aide de Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender.
Ce cours est destiné au futur Analyste des opérations de sécurité Microsoft, qui devra sécuriser les systèmes informatiques de son entreprise, de son organisation.
Ce cours est destiné aux informaticiens qui souhaitent se préparer et passer la certification SC-200T00.

Pré-requis :

Pour suivre cette formation, les apprenants doivent :

- Avoir une compréhension de base de Microsoft 365.
- Avoir suivi le cours SC-900T00 "Les principes fondamentaux de la sécurité, de la conformité et de l'identité Microsoft" ou avoir les connaissances équivalentes.
- Maitriser Windows 10.
- Etre familiarisés avec les services Azure, en particulier Azure SQL Database et Azure Storage.
- Etre familiarisés avec les machines virtuelles Azure et les réseaux virtuels.
- Avoir une compréhension de base des concepts de script.

Objectifs pédagogiques :

A l'issue de la formation, les apprenants auront acquis les compétences suivantes :

- Expliquez comment Microsoft Defender for Endpoint peut remédier aux risques dans votre environnement
- Créer un environnement Microsoft Defender for Endpoint
- Configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10
- Effectuer des actions sur un appareil à l'aide de Microsoft Defender for Endpoint
- Enquêter sur les domaines et les adresses IP dans Microsoft Defender for Endpoint
- Enquêter sur les comptes d'utilisateurs dans Microsoft Defender for Endpoint
- Configurer les paramètres d'alerte dans Microsoft Defender for Endpoint
- Expliquer comment le paysage des menaces évolue
- Mener une chasse avancée dans Microsoft 365 Defender
- Gérer les incidents dans Microsoft 365 Defender
- Expliquez comment Microsoft Defender for Identity peut remédier aux risques dans votre environnement.
- Enquêter sur les alertes DLP dans Microsoft Cloud App Security
- Expliquez les types d'actions que vous pouvez entreprendre dans un cas de gestion des risques d'initiés.
- Configurer le provisionnement automatique dans Azure Defender
- Corriger les alertes dans Azure Defender
- Construire des instructions KQL
- Filtrez les recherches en fonction de l'heure de l'événement, de la gravité, du domaine et d'autres données pertinentes à l'aide de KQL
- Extraire des données de champs de chaîne non structurés à l'aide de 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
- Expliquer les différences entre le format d'événement commun et le connecteur Syslog dans Azure Sentinel
- Connecter les machines virtuelles Azure Windows à 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 règle d'analyse
- Créer un playbook pour automatiser une réponse à un incident
- Utilisez des requêtes pour rechercher les menaces
- Observez les menaces au fil du temps avec la diffusion en direct

Compétences acquises à l'issue de la formation :

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc

- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Programme de cours
Microsoft Security Operations Analyst

Description / Contenu

Module 1 : Protection contre les menaces à l'aide de Microsoft Defender for Endpoint

- Protégez-vous contre les menaces avec Microsoft Defender for Endpoint
- Déployer l'environnement Microsoft Defender for Endpoint
- Implémentez les améliorations de sécurité de Windows 10 avec Microsoft Defender for Endpoint
- Gérer les alertes et les incidents dans Microsoft Defender for Endpoint
- Effectuer des enquêtes sur les appareils dans Microsoft Defender for Endpoint
- Effectuer des actions sur un appareil à l'aide de Microsoft Defender for Endpoint
- Effectuer des enquêtes sur les preuves et les entités à l'aide de Microsoft Defender for Endpoint
- Configurer et gérer l'automatisation à l'aide de Microsoft Defender for Endpoint
- Configurer les alertes et les détections dans Microsoft Defender for Endpoint
- Utiliser la gestion des menaces et des vulnérabilités dans Microsoft Defender for Endpoint

Module 2 : Protection contre les menaces à l'aide de Microsoft 365 Defender

- Introduction à la protection contre les menaces avec Microsoft 365
- Atténuez les incidents à l'aide de Microsoft 365 Defender
- Protégez vos identités avec Azure AD Identity Protection
- Corrigez les risques avec Microsoft Defender pour Office 365
- Protégez votre environnement avec Microsoft Defender for Identity
- Sécurisez vos applications et services cloud avec Microsoft Cloud App Security
- Répondez aux alertes de prévention des pertes de données à l'aide de Microsoft 365
- Gérer le risque d'initié dans Microsoft 365

Module 3 : Protection contre les menaces à l'aide d'Azure Defender

- Planifier des protections de charge de travail cloud à l'aide d'Azure Defender
- Expliquer les protections des charges de travail cloud dans Azure Defender
- Connecter les actifs Azure à Azure Defender
- Connecter des ressources non Azure à Azure Defender
- Corriger les alertes de sécurité à l'aide d'Azure Defender

Module 4 : créer des requêtes pour Azure Sentinel à l'aide du langage de requête Kusto (KQL)

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

Module 5 : Configurer votre environnement Azure Sentinel

- Présentation d'Azure Sentinel
- Créer et gérer des espaces de travail Azure Sentinel
- Journaux de requête dans Azure Sentinel
- Utiliser les listes de surveillance dans Azure Sentinel
- Utiliser les renseignements sur les menaces dans Azure Sentinel

Module 6 : 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
- Connectez Microsoft 365 Defender à Azure Sentinel
- Connecter des hôtes Windows à Azure Sentinel
- Connecter les journaux Common Event Format à Azure Sentinel
- Connecter les sources de données Syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel

Module 7 : Créer des détections et effectuer des enquêtes à l'aide d'Azure Sentinel

- Détection des menaces avec Azure Sentinel Analytics
- Réponse aux menaces avec les playbooks Azure Sentinel
- Gestion des incidents de sécurité dans Azure Sentinel
- Utiliser l'analyse du comportement des entités dans Azure Sentinel
- Interrogez, visualisez et surveillez les données dans Azure Sentinel

Module 8 : Effectuer une chasse aux menaces dans Azure Sentinel

- Chasse aux menaces avec Azure Sentinel
- Rechercher les menaces à l'aide de blocs-notes dans Azure Sentinel