Analyste des opérations de sécurité Microsoft

Référence : **MSSC200** Durée : **4 jours** Certification : **SC200**

CONNAISSANCES PREALABLES

• 1-Compréhension de base de Microsoft 365. • 2-Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft. • 3-Compréhension intermédiaire de Windows 10. • 4-Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure. • 5-Connaissance des machines virtuelles Azure et des réseaux virtuels. • 6-Compréhension de base des concepts de script. • 7-Avoir des connaissances de base en langue anglaise car les ateliers seront réalisés sur des VM en anglais.

PROFIL DES STAGIAIRES

• Analystes sécurité. • Ingénieurs sécurité.

OBJECTIFS

• Être capable d'expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement. • Savoir créer un environnement Microsoft Defender pour Endpoint. • Apprendre à configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10. • Comprendre comment effectuer des actions sur un appareil à l'aide de Microsoft Defender pour Endpoint. • Pouvoir examiner les domaines et les adresses IP dans Microsoft Defender pour Endpoint. • Être en mesure d'examiner les comptes d'utilisateurs et configurer les paramètres d'alerte dans Microsoft Defender pour Endpoint. • Comprendre comment effectuer une recherche avancée dans Microsoft 365 Defender. • Savoir gérer les incidents dans Microsoft 365 Defender. • Expliquer comment Microsoft Defender for Identity peut remédier aux risques dans votre environnement. • Pouvoir examiner les alertes DLP dans Microsoft Cloud App Security. • Apprendre à configurer l'approvisionnement automatique dans Azure Defender. • Comprendre comment corriger les alertes dans Azure Defender. • Savoir construire des instructions KQL. • Pouvoir filtrer 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. • Comprendre comment extraire des données de champs de chaîne non structurés à l'aide de KQL. • Savoir gérer un espace de travail Azure Sentinel. • Apprendre à utiliser KQL pour accéder à la liste de surveillance dans Azure Sentinel. • Pouvoir gérer les indicateurs de menace dans Azure Sentinel. • Être capable de connecter les machines virtuelles Azure Windows à Azure Sentinel. • Apprendre à configurer l'agent Log Analytics pour collecter les événements Sysmon. • Savoir créer de nouvelles règles et requêtes d'analyse à l'aide de l'assistant de règle d'analyse. • Pouvoir utiliser des requêtes pour rechercher les menaces.

CERTIFICATION PREPAREE

- Microsoft Security Operations Analyst. La réussite de l'examen permet d'obtenir la Certification Microsoft Certified : Security Operations Analyst Associate

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité Microsoft

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Atténuer les 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 la sécurité de Windows 10 avec Microsoft Defender pour Endpoint
- Gérer les alertes et les incidents dans Microsoft Defender pour Endpoint
- Effectuer des enquêtes sur les appareils dans Microsoft Defender pour Endpoint
- Effectuer des actions sur un appareil 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

Atténuer les menaces à l'aide de Microsoft 3654 Defender

- Introduction à la protection contre les menaces avec Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger les identités avec Azure AD Identity Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protéger son environnement avec Microsoft Defender for Identity
- Sécuriser ses applications et services cloud avec Microsoft Cloud App Security
- Répondre aux alertes de prévention de la perte de données à l'aide de Microsoft 365
- Gérer les risques internes dans Microsoft 365

Atténuer les menaces à l'aide de Microsoft Azure Defender

- Planifier les protections de la 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

Créer des requêtes pour Microsoft Azure Sentinel à l'aide du langage de requête Kusto

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

Configurer votre environnement Microsoft Azure Sentinel

- Introduction à Azure Sentinel
- Créer et gérer des espaces de travail Azure Sentinel
- Requête des journaux dans Azure Sentinel
- Utiliser des listes de surveillance dans Azure Sentinel
- Utiliser l'intelligence des menaces dans Azure Sentinel

Connecter les journaux à Microsoft Azure Sentinel

- Connecter les 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 du format d'événement commun à Azure Sentinel
- Connecter les sources de données Syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel

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

- Détection des menaces avec l'analyse Azure Sentinel
- 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
- Interroger, visualiser et surveiller les données dans Azure Sentinel

Effectuer une recherche de menace dans Microsoft Azure Sentinel

- Chasser les menaces avec Azure Sentinel
- Traquer les menaces à l'aide de blocs-notes dans Azure Sentinel

Certification Microsoft Security Operations Analyst

- Cette formation prépare au passage de la certification Microsoft Security Operations Analyst