EduGroupe
Accompagner pour réussir

Analyste des opérations de sécurité Microsoft

Référence : **MSSC200** Durée : **4 jours (28 heures)** Certification : **SC200**

Connaissances préalables

- 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
- 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 préparée

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

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité Microsoft

Méthodes d'évaluation des acquis

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

Contenu du cours

1. Atténuer les menaces à l'aide de Microsoft 365 Defender

- Présentation de la protection contre les menaces Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger les identités avec Azure AD Identity Protection
- Corriger les risques avec Microsoft Defender pour Office 365
- Protéger un environnement avec Microsoft Defender pour Identity
- Sécuriser les applications et services cloud avec Microsoft Defender pour les applications cloud
- Répondre aux alertes de prévention des pertes de données à l'aide de Microsoft 365
- Gérer les risques internes dans Microsoft 365

2. Atténuer les menaces à l'aide de Microsoft Defender for Endpoint

- Se protéger contre les menaces avec Microsoft Defender for Endpoint
- Déployer l'environnement Microsoft Defender pour Endpoint
- Implémenter les améliorations de sécurité de Windows
- Effectuer des enquêtes sur les appareils
- Effectuer des actions sur un appareil
- Effectuer des enquêtes sur les preuves et les entités
- Configurer et gérer l'automatisation
- Configurer les alertes et les détections
- Utiliser la gestion des vulnérabilités

3. Atténuer les menaces à l'aide de Microsoft Defender pour le cloud

- Planifier les protections des charges de travail cloud à l'aide de Microsoft Defender pour le cloud
- Connecter les actifs Azure à Microsoft Defender pour le Cloud
- Connecter des ressources non Azure à Microsoft Defender pour le cloud
- Gérer la gestion de votre posture de sécurité cloud
- Expliquer les protections de charge de travail cloud dans Microsoft Defender pour le cloud
- Corriger les alertes de sécurité à l'aide de Microsoft Defender for Cloud

4. Créer des requêtes pour Microsoft Sentinel à l'aide du langage de requête Kusto (KQL)

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

5. Configurer votre environnement Microsoft Sentinel

- Présentation de Microsoft Sentinel
- Créer et gérer des espaces de travail Microsoft Sentinel
- Interroger les journaux dans Microsoft Sentinel
- Utiliser des listes de surveillance dans Microsoft Sentinel
- Utiliser les renseignements sur les menaces dans Microsoft Sentinel

6. Connecter les journaux à Microsoft Sentinel

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

7. Créer des détections et effectuer des enquêtes à l'aide de Microsoft Sentinel

- Détection des menaces avec Microsoft Sentinel Analytics
- 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 du comportement des entités dans Microsoft Sentinel
- Normalisation des données dans Microsoft Sentinel
- Interroger, visualiser et surveiller les données dans Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel

8. Effectuer une recherche de menace dans Microsoft Sentinel

- Expliquer les concepts de chasse aux menaces dans Microsoft Sentinel
- Chasse aux menaces avec Microsoft Sentinel
- Utiliser la recherche d'emplois dans Microsoft Sentinel
- Chasse aux menaces à l'aide de blocs-notes dans Microsoft Sentinel

9. Certification Microsoft Security Operations Analyst

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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.