Microsoft Security Operations Analyst (Microsoft SC-200)

Cours officiel SC-200, préparation à l'examen

Cours Pratique de 4 jours - 28h
Réf : MCJ - Prix 2024 : 2 790€ HT

Avec cette formation, vous apprendrez à enquêter, répondre et rechercher les menaces en utilisant Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender. Vous saurez ainsi comment atténuer les cybermenaces à l'aide de ces technologies. Vous configurerez et utiliserez Azure Sentinel et le Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la création de rapports.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

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

Exécuter des actions sur un périphérique à l'aide de Microsoft Defender pour Endpoint

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

Remédier aux alertes dans Azure Defender

Mener une chasse avancée dans Microsoft 365 Defender

Expliquer comment Microsoft Defender for Identity peut remédier aux risques dans votre environnement

Examiner les alertes de prévention des pertes de données (DLP) dans Microsoft Cloud App Security

Expliquer les types d'actions que vous pouvez entreprendre dans un dossier de gestion des risques internes

Configurer l'auto-provisioning dans Azure Defender

Expliquer comment le paysage des menaces évolue

Gérer les incidents dans Microsoft 365 Defender

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

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

PARTICIPANTS

Analystes sécurité, ingénieurs sécurité.

PRÉREQUIS

Connaissances de base : Microsoft 365. Bonnes connaissances de Windows 10, des services Azure (Azure SQL, stockage Azure), des machines virtuelles Azure et des réseaux virtuels, etc.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 01/2024

1) 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 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.

Travaux pratiques : Déployer Microsoft Defender pour Endpoint. Atténuer les attaques à l'aide de Defender for Endpoint.

2) Atténuer les 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.
- Protéger votre environnement avec Microsoft Defender for Identity.
- Sécuriser vos applications et services cloud avec Microsoft Cloud App Security.
- Répondre aux alertes de prévention des pertes de données (DLP) avec Microsoft 365.
- Gérer les risques liés aux initiés dans Microsoft 365.

Travaux pratiques : Mise en application : atténuer les menaces avec Microsoft 365 Defender.

3) Atténuer les menaces à l'aide d'Azure Defender

- Planifier les protections des charges de travail cloud à l'aide d'Azure Defender.
- Expliquer les protections des charges de travail cloud 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 d'Azure Defender.

Travaux pratiques : Déployer Azure Defender. Atténuer les attaques avec Azure Defender.

4) Créer des requêtes pour Azure Sentinel avec le Kusto Query Language

- Construire des instructions Kusto Query Language (KQL) pour Azure Sentinel.
- Analyser les résultats des requêtes en utilisant Kusto Query Language (KQL).
- Construire des instructions multi-tables à l'aide de Kusto Query Language (KQL).
- Travailler avec des données dans Azure Sentinel en utilisant Kusto Query Language (KQL).

Travaux pratiques : Construire des instructions KQL de base. Analyser les résultats des requêtes à l'aide de KQL. Construire des requêtes multi-tables en utilisant KQL. Travailler avec des données de type chaîne à l'aide d'instructions KQL.

5) Configurer 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 : Créer un espace de travail Azure Sentinel. Créer une liste de surveillance. Créer un indicateur de menace.

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.
- Connecter Microsoft 365 Defender à Azure Sentinel.
- Connecter les hôtes Windows à Azure Sentinel.
- Connecter les journaux Common Event Format (CEF) à Azure Sentinel.
- Connecter des sources de données syslog à Azure Sentinel.
- Connecter les indicateurs de menace à Azure Sentinel.

Travaux pratiques : 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.

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

- Détecter des menaces avec les analyses d'Azure Sentinel.
- Répondre aux menaces avec les manuels Azure Sentinel.
- Gérer les 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 règles analytiques. Modéliser les attaques pour définir la logique des règles. Atténuer les attaques à l'aide d'Azure Sentinel. Créer des classeurs dans Azure Sentinel.

8) 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 à l'aide de notebooks.

LES DATES

CLASSE À DISTANCE
2024 : 27 mai, 16 juil., 05 nov.

PARIS
2024 : 09 juil., 22 oct.