Smartfuture
Certifications | Training | Technology solutions

FORMATION & CERTIFICATION • SC-200

Analyste des opérations de sécurité Microsoft

Maîtriser Defender, Sentinel et Copilot for Security pour détecter et répondre aux menaces en environnements hybrides et multi-cloud.

Formation présentielle

Formateurs certifiés Microsoft

Distributeur officiel Certiport

4 jours 28 heures	**Examen** SC-200
Modalité Présentiel — Distanciel	**Niveau** Intermédiaire

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

OBJECTIFS PÉDAGOGIQUES

- Gérer les opérations de sécurité avec Microsoft Defender XDR et Sentinel.
- Configurer connecteurs, ingestion des journaux et stratégies de protection du SI.
- Gérer les alertes et incidents de sécurité avec des playbooks automatisés.
- Utiliser Copilot et KQL pour la détection proactive des menaces.

PUBLIC CIBLE

- Analystes des opérations de sécurité.
- Spécialistes de la sécurité informatique.
- Administrate urs de sécurité.
- Responsables de la sécurité des systèmes d'information (RSSI).

PRÉREQUIS

- Compréhension de base des concepts de sécurité et des technologies de protection.
- Connaissance des principes de surveillance des menaces et de réponse aux incidents.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Gérer un environnement d'opérations de sécurité

- Configurer des paramètres dans Microsoft Defender XDR.
- Configurer une règle et des règles de notification des vulnérabilités.
- Configurer des fonctionnalités avancées de Microsoft Defender for Endpoint.
- Configurer les paramètres des règles des points de terminaison.
- Gérer les fonctionnalités d'enquête et de réponse automatisées dans Microsoft Defender XDR.
- Configurer l'interruption automatique des attaques dans Microsoft Defender XDR.

Gérer les ressources et concevoir Microsoft Sentinel

Gérer des ressources et des environnements

- Configurer et gérer des groupes d'appareils, des autorisations et des niveaux d'automatisation dans Microsoft Defender for Endpoint.
- Identifier les appareils non gérés dans Microsoft Defender for Endpoint.
- Découvrir des ressources non protégées en tirant parti de Defender pour le cloud.
- Identifier et corriger des appareils en utilisant la Gestion des vulnérabilités Microsoft Defender.
- Atténuer les risques à l'aide de la gestion de l'exposition dans Microsoft Defender XDR.

Concevoir et configurer un espace de travail Microsoft Sentinel

- Planifier un espace de travail Microsoft Sentinel.
- Configurer des rôles Microsoft Sentinel et spécifier des rôles RBAC Azure pour la configuration de Microsoft Sentinel.
- Concevoir et configurer le stockage de données Microsoft Sentinel, notamment les types de journaux et la conservation des journaux.

Ingérer et gérer les données dans Microsoft Sentinel

- Identifier les sources de données à ingérer pour Microsoft Sentinel.
- Implémenter et utiliser des solutions de hub de contenu.
- Configurer et utiliser des connecteurs Microsoft pour les ressources Azure, notamment Azure Policy et les paramètres de diagnostic.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Planifier et configurer des collections d'événements Syslog et CEF (Common Event Format).
- Planifier et configurer une collecte d'événements Sécurité Windows en tirant parti de règles de collecte de données, notamment le transfert d'événements Windows (WEF).
- Créer des tables de journaux personnalisées dans l'espace de travail pour stocker les données ingérées.
- Contrôler et optimiser l'ingestion des données.

Configurer des protections et des détections

- Configurer des protections dans les technologies de sécurité Microsoft Defender.
- Configurer des stratégies dans Microsoft Defender pour les applications cloud.
- Configurer des stratégies dans Microsoft Defender pour Office 365.
- Configurer des stratégies de sécurité pour Microsoft Defender for Endpoint, notamment les règles de réduction de la surface d'attaque (ASR).
- Configurer des protections de charge de travail cloud dans Microsoft Defender pour le cloud.
- Configurer les détections dans Microsoft Defender XDR et gérer les règles de détections personnalisées.
- Gérer les alertes, notamment le réglage, la suppression et la corrélation.
- Configurer des règles d'imposture dans Microsoft Defender XDR.
- Configurer des détections dans Microsoft Sentinel, classifier et analyser des données à l'aide d'entités.
- Configurer et gérer les règles d'analyse et interroger des données Microsoft Sentinel en utilisant des analyseurs ASIM.
- Implémenter une analyse comportementale.

Gérer les réponses aux incidents

- Répondre aux alertes et aux incidents dans le portail Microsoft Defender.
- Enquêter et corriger des menaces en utilisant Microsoft Defender pour Office 365.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Enquêter et corriger des incidents de compromission d'e-mails professionnels et de rançongiciel identifiés par une interruption automatique d'attaque.
- Examiner et corriger les entités compromises identifiées par les stratégies de protection contre la perte de données (DLP) Microsoft Purview.
- Enquêter et corriger des menaces identifiées par des stratégies de risque interne Microsoft Purview.
- Enquêter et corriger des alertes et des incidents identifiés par les protections de charge de travail Microsoft Defender pour le cloud.
- Enquêter et corriger des risques de sécurité identifiés par Microsoft Defender pour les applications cloud.
- Enquêter sur les identités compromises identifiées par Microsoft Entra ID et y remédier.
- Enquêter et corriger des alertes de sécurité de Microsoft Defender pour Identity.
- Répondre aux alertes et aux incidents identifiés par Microsoft Defender for Endpoint, examiner les chronologies des appareils et effectuer des actions sur l'appareil.
- Effectuer des enquêtes d'entités et de preuves.
- Examiner les activités de Microsoft 365, enquêter sur des menaces en utilisant le journal d'audit unifié, la Recherche de contenu et les journaux d'activité de Microsoft Graph.
- Répondre aux incidents dans Microsoft Sentinel, investiguer et corriger les incidents.
- Créer et configurer des règles d'automatisation et des playbooks Microsoft Sentinel, y compris sur des ressources locales.

Copilot pour la sécurité et chasse aux menaces

Implémenter et utiliser Copilot pour la sécurité

- Créer et utiliser des livres d'invite.
- Gérer les sources pour Copilot for Security, y compris les plug-ins et les fichiers.
- Intégrer Copilot for Security en implémentant des connecteurs.
- Gérer les autorisations et les rôles dans Copilot pour la sécurité.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Surveiller la capacité et le coût de Copilot pour la sécurité.
- Identifier les menaces et les risques, et examiner les incidents à l'aide de Copilot pour la sécurité.

Gérer les menaces de sécurité et chasser les menaces

- Effectuer un repérage des menaces avec Microsoft Defender XDR.
- Identifier les menaces à l'aide du langage de requête Kusto (KQL) et interpréter les analyses de menaces dans le portail Microsoft Defender.
- Créer des requêtes de repérage personnalisées en tirant parti de KQL.
- Effectuer un repérage des menaces avec Microsoft Sentinel.
- Analyser la couverture de vecteurs d'attaque en utilisant la matrice MITRE ATT&CK.
- Gérer et utiliser des indicateurs de menace, créer et gérer des chasses.
- Créer et surveiller des requêtes de repérage, utiliser des signets de repérage pour les investigations de données.
- Récupérer et gérer les données de journaux archivées, créer et gérer des travaux de recherche.
- Créer et configurer des classeurs Microsoft Sentinel, activer et personnaliser des modèles de classeur.
- Créer des classeurs personnalisés qui incluent KQL et configurer des visualisations.