Programme de formation
SC-200 : Microsoft Security Operations Analyst

(Préparation certification Microsoft SC-200)
(Mis à jour le 02/01/2024)

DESCRIPTION DE LA FORMATION :

Cette formation vous permettra d'enquêter, de répondre et de rechercher les menaces et les atténuer à l'aide de Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender. Lors de cette formation, vous serez amenés à configurer et utiliser Azure Sentinel et à utiliser Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la création de rapports.

OBJECTIFS PEDAGOGIQUES :

A l'issue de cette formation, les participants seront en capacité de :

- Atténuer les menaces avec Microsoft Defender XDR
- Atténuer les menaces avec Microsoft Purview
- Atténuer les menaces avec Microsoft Defender pour point de terminaison
- Atténuer les menaces avec Microsoft Defender pour le cloud
- Créer des requêtes pour Microsoft Sentinel avec le langage de requête Kusto (KQL)
- Configurer votre environnement Microsoft Sentinel
- Connecter des journaux à Microsoft Sentinel
- Créer des détections et effectuer des investigations avec Microsoft Sentinel
- Effectuer la chasse aux menaces dans Microsoft Sentinel

MÉTHODES & MODALITÉS PÉDAGOGIQUES :

- Cette formation sera principalement constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.
- Support : un support de cours officiel Microsoft sera remis aux participants au format électronique.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Prérequis évalués avant la formation, questions régulières, travaux pratiques, QCM ou autres méthodes).
- Formateur : le tout animé par un formateur expérimenté et accrédité Microsoft Certified Trainer.
- Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations.
- Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
- Cette formation peut être dispensée en format inter-entreprises ou intra-entreprise sur demande et en mode présentiel comme en distanciel.

PROGRAMME DE FORMATION :

Découvrir la protection contre les menaces avec Microsoft 365

- Explorer les cas d'utilisation de la réponse XDR (Extended Detection and Response).
- Comprendre Microsoft Defender XDR dans un centre des opérations de sécurité (SOC).
- Explorer Microsoft Security Graph.
- Examiner les incidents de sécurité dans Microsoft Defender XDR.

Réduire les incidents avec Microsoft Defender XDR

- Gérer les incidents dans Microsoft Defender XDR.
- Examiner les incidents dans Microsoft Defender XDR.
- Effectuer un repérage avancé dans Microsoft Defender XDR.

Protéger vos identités avec Microsoft Entra ID Protection

- Découvrir les fonctionnalités de Microsoft Entra ID Protection.
- Découvrir les fonctionnalités d'investigation et de correction de Microsoft Entra ID Protection.

Corriger les risques avec Microsoft Defender pour Office 365

- Définir les fonctionnalités de Microsoft Defender pour Office 365.
- Simuler des attaques au sein de votre réseau.
- Remédier aux risques dans votre environnement avec Microsoft Defender pour Office 365.

Protéger votre environnement avec Microsoft Defender pour l'identité

- Définir les fonctionnalités de Microsoft Defender pour l'identité.
- Configurer des capteurs Microsoft Defender pour l'identité.
- Corriger des risques dans votre environnement avec Microsoft Defender pour l'identité.

Sécuriser vos applications et services cloud avec Microsoft Defender for Cloud Apps

- Définir l'infrastructure Defender for Cloud Apps.
- Expliquer comment Cloud Discovery vous aide à voir ce qui se passe dans votre organisation.
- Utiliser des stratégies de contrôle d'application par accès conditionnel pour contrôler l'accès aux applications de votre organisation.

Répondre aux alertes de protection contre la perte de données à l'aide de Microsoft 365

- Décrire les composants de protection contre la perte de données (DLP) dans Microsoft 365.
- Examiner les alertes DLP dans le portail de conformité Microsoft Purview.
- Investiguer les alertes DLP dans Microsoft Defender for Cloud Apps.

Gérer les risques internes dans Microsoft Purview

- Prévenir, détecter et contenir les risques internes dans une organisation avec Microsoft Purview Insider Risk Management.
- Décrire les types de modèles de stratégie intégrés et prédéfinis.
- Répertorier les conditions préalables à remplir avant de créer des stratégies de risque interne.
- Expliquer les types d'actions à entreprendre dans un cas de gestion des risques internes.

Examiner les menaces à l'aide des fonctionnalités d'audit de Microsoft Defender XDR et Microsoft Purview Standard

- Décrire les différences entre la solution Audit (Standard) et la solution Audit (Premium).
- Démarrer l'enregistrement des activités des utilisateurs et des administrateurs dans le journal d'audit unifié (UAL).
- Identifier les fonctionnalités principales de la solution Audit (Standard).
- Configurer et implémenter la recherche dans les journaux d'audit à l'aide de la solution Audit (Standard).
- Exporter, configurer et visualiser les enregistrements des journaux d'audit.
- Utiliser la recherche dans les journaux d'audit pour résoudre les problèmes de support courants.

Investiguer les menaces en utilisant l'audit dans Microsoft Defender XDR et Microsoft Purview (Premium)

- Configurer et implémenter Microsoft Purview Audit (Premium).
- Créer des stratégies de conservation des journaux d'audit.
- Effectuer des enquêtes à propos des comptes d'utilisateurs compromis.

Investiguer les menaces avec une recherche de contenu dans Microsoft Purview

- Utiliser une recherche de contenu dans le portail de conformité Microsoft Purview.
- Concevoir et créer une recherche de contenu.
- Prévisualiser les résultats de la recherche.
- Afficher les statistiques de la recherche.
- Exporter les résultats et le rapport de la recherche.
- Configurer le filtrage des autorisations de recherche.

Protéger des menaces avec Microsoft Defender for Endpoint

- Définir les fonctionnalités de Microsoft Defender pour Endpoint.
- Traquer les menaces au sein de votre réseau.
- Remédier aux risques dans votre environnement avec Microsoft Defender for Endpoint.

Déployer l'environnement Microsoft Defender pour point de terminaison

- Créer un environnement Microsoft Defender pour point de terminaison.
- Intégrer des périphériques devant être analysés par Microsoft Defender pour point de terminaison.
- Configurer les paramètres de Microsoft Defender pour point de terminaison.

Implémenter des améliorations de sécurité Windows avec Microsoft Defender pour point de terminaison

- Expliquer la réduction de la surface d'attaque dans Windows.
- Activer les règles de réduction de la surface d'attaque sur les appareils sous Windows 10.
- Configurer les règles de réduction de la surface d'attaque sur les appareils sous Windows 10.

Enquêter sur les appareils dans Microsoft Defender pour point de terminaison

- Utiliser la page de l'appareil dans Microsoft Defender pour point de terminaison.
- Décrire les informations forensiques sur les appareils collectées par Microsoft Defender pour point de terminaison.
- Décrire le blocage comportemental par Microsoft Defender pour point de terminaison.

Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour point de terminaison

- Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour point de terminaison.
- Exécuter une collecte de données d'investigation à l'aide de Microsoft Defender for Endpoint.
- Accéder à distance à des appareils à l'aide de Microsoft Defender pour point de terminaison.

Effectuer des investigations de preuve et d'entités à l'aide de Microsoft Defender pour point de terminaison

- Examiner les fichiers dans Microsoft Defender pour point de terminaison.
- Examiner les domaines et les adresses IP dans Microsoft Defender pour point de terminaison.
- Examiner les comptes d'utilisateur dans Microsoft Defender pour point de terminaison.

Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour le point de terminaison

- Configurer des fonctionnalités avancées de Microsoft Defender pour le point de terminaison.
- Gérer les paramètres d'automatisation dans Microsoft Defender pour le point de terminaison.

Configurer les alertes et les détections dans Microsoft Defender pour point de terminaison

- Configurer les paramètres d'alerte dans Microsoft Defender pour point de terminaison.
- Gérer les indicateurs dans Microsoft Defender pour point de terminaison.

Utiliser la Gestion des vulnérabilités dans Microsoft Defender pour point de terminaison

- Gérer des menaces et des vulnérabilités dans Microsoft Defender pour point de terminaison.
- Identifier les vulnérabilités sur les appareils avec Microsoft Defender pour point de terminaison.
- Suivre les menaces émergentes dans Microsoft Defender pour point de terminaison.

Planifier des protections de charge de travail Cloud à l'aide de Microsoft Defender pour le Cloud

- Décrire les fonctionnalités de Microsoft Defender pour le Cloud.
- Expliquer les protections de charge de travail dans Microsoft Defender pour le Cloud.
- Activer Microsoft Defender pour le cloud.

Connecter des ressources Azure à Microsoft Defender pour le cloud

- Explorer les ressources Azure.
- Configurer l'approvisionnement automatique dans Microsoft Defender pour le cloud.
- Décrire l'approvisionnement manuel dans Microsoft Defender pour le cloud.

Connecter des ressources non Azure à Microsoft Defender pour le cloud

- Connecter des ordinateurs non Azure à Microsoft Defender pour le cloud.
- Connecter des comptes AWS à Microsoft Defender pour le cloud.
- Connecter des comptes GCP à Microsoft Defender pour le cloud.

Gérer votre gestion de la posture de sécurité cloud

- Décrire les fonctionnalités de Microsoft Defender pour le cloud.
- Expliquer les protections de gestion de la posture de sécurité Microsoft Defender pour le cloud pour vos ressources.

Expliquer les protections de charge de travail cloud dans Microsoft Defender pour le cloud

- Expliquer quelles sont les charges de travail protégées par Microsoft Defender pour le cloud.
- Décrire les avantages des protections offertes par Microsoft Defender pour le cloud.
- Expliquer comment la protection de Microsoft Defender pour le cloud fonctionne.

Corriger les alertes de sécurité à l'aide de Microsoft Defender pour le Cloud

- Décrire les alertes dans Microsoft Defender pour le Cloud.
- Corriger les alertes dans Microsoft Defender pour le Cloud.
- Automatiser les réponses dans Microsoft Defender pour le Cloud.

Construire des instructions KQL pour Microsoft Azure Sentinel

- Construire des instructions KQL.
- Rechercher des événements de sécurité dans les fichiers journaux à l'aide de KQL.
- 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.

Analyser les résultats d'une requête à l'aide de KQL

- Synthétiser des données à l'aide d'instructions KQL.
- Afficher des visualisations à l'aide d'instructions KQL.

Générer des instructions de tables multiples à l'aide de KQL

- Créer des requêtes à l'aide d'unions pour afficher les résultats sur plusieurs tables à l'aide de KQL.
- Fusionner deux tables avec l'opérateur de jointure à l'aide de KQL.

Utiliser des données dans Microsoft Azure Sentinel à l'aide du langage de requête Kusto

- Extraire des données à partir de champs de chaîne non structurés à l'aide de KQL.
- Extraire des données à partir de données de chaîne structurées à l'aide de KQL.
- Créer des fonctions à l'aide de KQL.

Découvrir Microsoft Sentinel

- Identifier les différents composants et fonctionnalités de Microsoft Sentinel.
- Identifier les cas d'usage où Microsoft Sentinel constitue une bonne solution.

Créer et gérer des espaces de travail Microsoft Sentinel

- Décrire l'architecture de l'espace de travail Microsoft Sentinel.
- Installer l'espace de travail Microsoft Sentinel.
- Gérer un espace de travail Microsoft Sentinel.

Utiliser les journaux de requêtes dans Microsoft Azure Sentinel

- Utiliser la page Journaux pour afficher les tables de données dans Microsoft Azure Sentinel.
- Interroger les tables les plus utilisées à l'aide de Microsoft Azure Sentinel.

Utiliser des watchlists dans Microsoft Azure Sentinel

- Créer un watchlist dans Microsoft Azure Sentinel.
- Utiliser KQL pour accéder à la watchlist dans Microsoft Azure Sentinel.

Utiliser le renseignement sur les menaces dans Microsoft Azure Sentinel

- Gérer les indicateurs de menace dans Microsoft Azure Sentinel.
- Utiliser KQL pour accéder aux indicateurs de menace dans Microsoft Azure Sentinel.

Connecter des données à Microsoft Sentinel à l'aide de connecteurs de données

- Installer des solutions de hub de contenu pour provisionner des connecteurs de données Microsoft Sentinel.
- Utiliser des connecteurs de données dans Microsoft Sentinel.
- Décrire les fournisseurs de connecteurs de données Microsoft Sentinel.
- Expliquer les différences entre Common Event Format et le connecteur Syslog dans Microsoft Sentinel.

Connecter des services Microsoft à Microsoft Sentinel

- Connecter les connecteurs de service Microsoft.
- Expliquer comment les connecteurs créent automatiquement des incidents dans Microsoft Sentinel.

Connecter Microsoft Defender XDR à Microsoft Sentinel

- Activer le connecteur Microsoft Defender XDR dans Microsoft Sentinel.
- Activer le connecteur Microsoft Defender pour le cloud dans Microsoft Azure Sentinel.
- Activer le connecteur Microsoft Defender pour IoT dans Microsoft Sentinel.

Connecter des hôtes Windows à Microsoft Sentinel

- Connecter les machines virtuelles Windows Azure à Microsoft Sentinel.
- Connecter des hôtes Windows non Azure à Microsoft Sentinel.
- Configurer l'agent Log Analytics pour collecter les événements Sysmon.

Connecter des journaux Common Event Format à Microsoft Sentinel

- Déployer le connecteur Common Event Format dans Microsoft Sentinel.
- Exécuter le script de déploiement pour le connecteur Common Event Format.

Connecter des sources de données Syslog à Microsoft Sentinel

- Décrire la règle de collecte de données de l'agent Azure Monitor pour Syslog.
- Installer et configurer l'extension Agent Linux Azure Monitor avec la règle de collecte de données Syslog.
- Exécuter les scripts de déploiement et de connexion d'Azure Arc Linux.
- Vérifier que les données de journal Syslog sont disponibles dans Microsoft Sentinel.
- Créer un analyseur en utilisant KQL dans Microsoft Sentinel.

Connecter des indicateurs de menace à Microsoft Sentinel

- Configurer le connecteur TAXII dans Microsoft Sentinel
- Configurer le connecteur de la plateforme de renseignement sur les menaces dans Microsoft Sentinel
- Afficher les indicateurs de menace dans Microsoft Sentinel

Détecter des menaces avec Analytique Microsoft Sentinel

- Expliquer l'importance d'Analytique Microsoft Sentinel.
- Expliquer les différents types de règles analytiques.
- Créer des règles à partir de modèles.
- Créer de nouvelles règles et requêtes analytiques à l'aide de l'Assistant Règle analytique.
- Gérer les règles avec les modifications.

Automatiser dans Microsoft Sentinel

- Expliquer les options d'automatisation dans Microsoft Sentinel.
- Créer des règles d'automatisation dans Microsoft Sentinel.

Répondre aux menaces avec les playbooks Microsoft Sentinel
- Expliquer les fonctionnalités SOAR de Microsoft Sentinel.
- Explorer le connecteur Logic Apps Microsoft Sentinel.
- Créer un playbook pour automatiser une réponse aux incidents.
- Exécuter un playbook à la demande en réponse à un incident.

Gérer des incidents de sécurité dans Microsoft Sentinel
- Découvrir les incidents de sécurité et la gestion des incidents Microsoft Sentinel.
- Explorer les preuves et les entités d'incidents Microsoft Sentinel.
- Utiliser Microsoft Sentinel pour investiguer les incidents de sécurité et gérer la résolution des incidents.

Identifier les menaces avec l'analytique comportementale
- Expliquer l'analyse du comportement des utilisateurs et des entités dans Azure Sentinel.
- Explorer les entités dans Microsoft Azure Sentinel.

Normaliser des données dans Microsoft Sentinel
- Utiliser des analyseurs ASIM.
- Créer un analyseur ASIM.
- Créer des fonctions KQL paramétrables.

Interroger, visualiser et monitorer des données dans Microsoft Sentinel
- Visualiser les données de sécurité en utilisant des workbooks Microsoft Sentinel.
- Comprendre le fonctionnement des requêtes.
- Explorer les fonctionnalités des workbooks.
- Créer un workbook Microsoft Sentinel.

Gérer le contenu dans Microsoft Sentinel
- Installer une solution de hub de contenu dans Microsoft Sentinel.
- Connecter un dépôt GitHub à Microsoft Sentinel.

Expliquer les concepts de chasse des menaces dans Microsoft Sentinel
- Décrire les concepts de chasse des menaces à utiliser avec Microsoft Sentinel.
- Définir une hypothèse de chasse des menaces à utiliser dans Microsoft Sentinel.

Expliquer les concepts de chasse des menaces dans Microsoft Sentinel
- Décrire les concepts de chasse des menaces à utiliser avec Microsoft Sentinel.
- Définir une hypothèse de chasse des menaces à utiliser dans Microsoft Sentinel.

Repérer des menaces avec Microsoft Sentinel
- Utiliser des requêtes pour chasser les menaces.
- Enregistrer les résultats clés avec des signets.
- Observer les menaces dans le temps avec le stream en direct.

Utiliser des travaux de recherche dans Microsoft Sentinel

- Utiliser des travaux de recherche dans Microsoft Sentinel.
- Restaurer des journaux d'archivage dans Microsoft Sentinel.

Repérer les menaces à l'aide de notebooks dans Microsoft Sentinel

- Explorer les bibliothèques d'API pour le repérage avancé des menaces dans Microsoft Sentinel.
- Décrire les notebooks dans Microsoft Sentinel.
- Créer et utiliser des notebooks dans Microsoft Sentinel.

PRÉREQUIS :

Pour participer à cette formation, Il faut avoir préalablement suivi la formation « SC-900 : Microsoft Security, Compliance, and Identity Fundamentals »

Un niveau d'anglais B1 est recommandé, retrouvez les niveaux sur ce lien : Classification des niveaux de langue

PRE-CERTIFCIATION :

Cette formation prépare à l'examen de certification Microsoft SC-200 « Microsoft Security Operations Analyst »

DUREE : 4 jours (28 heures)

INTERLOCUTEURS : Opérateurs de sécurité

NIVEAU : Intermédiaire