Analyste des opérations de sécurité Microsoft (SC-200)

Description

Développez vos compétences en cybersécurité

Découvrez comment devenir un expert de la cybersécurité en maîtrisant les outils essentiels de Microsoft. La formation Analyste des opérations de sécurité Microsoft (SC-200) vous guide pour détecter, traiter et analyser efficacement les menaces. Grâce à des outils puissants comme Microsoft Sentinel, Microsoft Defender XDR et Microsoft Defender pour le cloud, vous apprendrez à protéger les environnements IT modernes.

Ce cours s'adresse à tous ceux qui souhaitent se spécialiser dans la réponse aux incidents de sécurité et dans la gestion proactive des risques. Vous apprendrez à utiliser le langage Kusto (KQL) pour analyser des incidents, configurer Sentinel et optimiser votre posture de sécurité. Les nombreuses démonstrations pratiques et études de cas vous permettront d'appliquer directement les concepts appris.

Obtenez votre certification SC-200 avec une préparation complète

Ce cours complet vous prépare efficacement à l'examen SC-200, en vous donnant toutes les clés pour réussir. Développez vos capacités d'analyse, améliorez votre réponse aux incidents et devenez un acteur incontournable de la cybersécurité grâce aux solutions Microsoft.

Contenu du cours
Module 1 : Présentation de la protection contre les menaces de Microsoft Defender XDR

- 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

Module 2 : Réduire le nombre d'incidents avec Microsoft Defender

- Utiliser le portail Microsoft Defender
- Gérer les incidents
- Investiguer les incidents
- Gérer et examiner les alertes
- Gérer les enquêtes automatisées
- Utiliser le Centre de notifications
- Explorer la recherche avancée de menaces
- Examiner les journaux de connexion Microsoft Entra
- Comprendre le niveau de sécurité Microsoft
- Analyser les menaces
- Analyser les rapports
- Configurer le portail Microsoft Defender

Module 3 : Corriger les risques avec Microsoft Defender pour Office 365

- Introduction à Microsoft Defender pour Office 365

- Automatiser, investiguer et remédier
- Configurer, protéger et détecter
- Simuler des attaques

Module 4 : Gérer Microsoft Entra Identity Protection

- Passer en revue les principes fondamentaux de Identity Protection
- Implémenter et gérer une stratégie de risque d'utilisateur
- Surveiller, examiner et corriger les utilisateurs à risque
- Implémenter la sécurité pour les identités de charge de travail
- Explorer Microsoft Defender pour Identity

Module 5 : Protéger votre environnement grâce à Microsoft Defender pour Identity

- Présentation de Microsoft Defender pour l'identité
- Configurer les capteurs Microsoft Defender pour l'identité
- Examiner les données ou les comptes compromis
- Intégration avec d'autres outils Microsoft

Module 6 : Sécuriser vos applications et services cloud avec Microsoft Defender pour applications cloud

- Comprendre le cadre de Defender pour les applications Cloud
- Explorer vos applications cloud avec Cloud Discovery
- Protéger vos données et applications avec contrôle d'application par accès conditionnel
- Parcourir la découverte et le contrôle d'accès avec Microsoft Defender for Cloud Apps
- Classifier et protéger les informations sensibles
- Détecter les menaces

Module 7 : Présentation de l'IA générative

- Qu'est-ce que l'IA générative ?
- En quoi consistent les modèles de langage ?
- Utiliser des modèles de langage
- En quoi consistent les copilotes ?
- Microsoft Copilot
- Considérations relatives aux invites Copilot
- Extension et développement de copilotes

Module 8 : Décrire Sécurité Microsoft Copilot

- Familiarisez-vous avec Microsoft Security Copilot
- Décrire la terminologie Microsoft Sécurité Copilot
- Décrire comment Sécurité Microsoft Copilot traite les demandes d'invite
- Décrire les éléments d'une invite efficace
- Décrire comment activer Microsoft Security Copilot

Module 9 : Décrire les fonctionnalités de base de Copilote de sécurité Microsoft

- Décrire les fonctionnalités disponibles dans l'expérience autonome de Microsoft Security Copilot
- Décrire les fonctionnalités disponibles dans une session de l'expérience autonome
- Décrire les espaces de travail
- Décrire les plug-ins Microsoft disponibles dans Microsoft Security Copilot
- Décrire les plug-ins non-Microsoft pris en charge par Microsoft Security Copilot

- Décrire les séquences de prompts personnalisées
- Décrire les connexions de la base de connaissances

Module 10 : Décrire les expériences intégrées de Microsoft Security Copilot

- Décrire Copilot dans Microsoft Defender XDR
- Copilot dans Microsoft Purview
- Copilot dans Microsoft Entra
- Copilot dans Microsoft Intune
- Copilot dans Microsoft Defender pour le cloud (préversion)

Module 11 : Explorer les cas d'usage de Microsoft Security Copilot

- Explorer la première expérience d'exécution
- Explorer l'expérience autonome
- Configurer le plug-in Microsoft Sentinel
- Activer un plug-in personnalisé
- Explorer les chargements de fichiers en tant que base de connaissances
- Créer un guide d'invite personnalisé
- Explorer les fonctionnalités de Copilot dans Microsoft Defender XDR
- Découvrir les fonctionnalités Copilot dans Microsoft Purview

Module 12 : Répondre aux alertes de protection contre la perte de données à l'aide de Microsoft 365

- Décrire les alertes de protection contre la perte de données
- Examiner les alertes de protection contre la perte de données dans Microsoft Purview
- Investiguer les alertes de protection contre la perte de données dans Microsoft Defender for Cloud Apps

Module 13 : Gérer le risque interne dans Microsoft Purview

- Insider risk management overview
- Introduction to managing insider risk policies
- Create and manage insider risk policies
- Investigate insider risk alerts
- Take action on insider risk alerts through cases
- Manage insider risk management forensic evidence
- Create insider risk management notice templates

Module 14 : Rechercher et investiguer avec Microsoft Purview Audit

- Vue d'ensemble d'Audit Microsoft Purview
- Configurer et gérer Microsoft Purview Audit
- Effectuer des recherches avec Audit (Standard)
- Auditer les interactions de Microsoft Copilot pour Microsoft 365
- Examiner les activités avec Audit (Premium)
- Exporter les données du journal d'audit
- Configurer la rétention d'audit avec Audit (Premium)

Module 15 : Investiguer les menaces avec une recherche de contenu dans Microsoft Purview

- Explorer les solutions eDiscovery Microsoft Purview
- Créer une recherche de contenu
- Afficher les résultats et les statistiques de la recherche

- Exporter les résultats et le rapport de recherche
- Configurer le filtrage des autorisations de recherche
- Rechercher et supprimer des e-mails

Module 16 : Se protéger contre les menaces avec Microsoft Defender pour point de terminaison

- Introduction to Microsoft Defender for Endpoint
- Practice security administration
- Hunt threats within your network

Module 17 : Déployer l'environnement Microsoft Defender pour point de terminaison

- Créer votre environnement
- Comprendre la compatibilité et les fonctionnalités des systèmes d'exploitation
- Appareils intégrés
- Gérer l'accès
- Créer et gérer des rôles pour le contrôle d'accès en fonction du rôle
- Configurer des groupes d'appareils
- Configurer des fonctionnalités avancées d'environnement

Module 18 : Implémenter des améliorations de sécurité Windows avec Microsoft Defender pour point de terminaison

- Comprendre la réduction de la surface d'attaque
- Activer les règles de réduction de la surface d'attaque

Module 19 : Enquêter sur les appareils dans Microsoft Defender pour point de terminaison

- Utiliser la liste d'inventaire des appareils
- Examiner l'appareil
- Utiliser le blocage comportemental
- Détecter des appareils avec la découverte d'appareil

Module 20 : Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour point de terminaison

- Expliquer les actions de l'appareil
- Exécuter l'analyse antivirus Microsoft Defender sur les appareils
- Collecter le package d'investigation à partir d'appareils
- Lancer une session de réponse en direct

Module 21 : Effectuer des investigations de preuve et d'entités à l'aide de Microsoft Defender pour point de terminaison

- Examiner un fichier
- Procéder à une investigation sur un compte d'utilisateur
- Examiner une adresse IP
- Examiner un domaine

Module 22 : Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour le point de terminaison

- Configurer les fonctionnalités avancées

- Gérer les paramètres de téléchargement et de dossier de l’automatisation
- Configurer des fonctionnalités d’investigation et de correction automatisées
- Bloquer les appareils à risque

Module 23 : Configurer les alertes et les détections dans Microsoft Defender pour point de terminaison

- Configurer les fonctionnalités avancées
- Configurer des notifications d’alerte
- Gérer la suppression d’alerte
- Gérer les indicateurs

Module 24 : Utiliser la Gestion des vulnérabilités dans Microsoft Defender pour point de terminaison

- Comprendre la gestion des vulnérabilités
- Explorer les vulnérabilités sur vos appareils
- Gérer la correction

Module 25 : Planifier des protections de charge de travail Cloud à l’aide de Microsoft Defender pour le Cloud

- Expliquer Microsoft Defender pour le cloud
- Décrire les protections de charge de travail Microsoft Defender pour cloud
- Activer Microsoft Defender pour le cloud

Module 26 : Connecter des ressources Azure à Microsoft Defender pour le cloud

- Explorer et gérer vos ressources avec l’inventaire des ressources
- Configurer le provisionnement automatique
- Approvisionnement manuel de l’agent Log Analytics

Module 27 : Connecter des ressources non Azure à Microsoft Defender pour le cloud

- Protéger les ressources non Azure
- Connecter des machines non-Azure
- Connecter vos comptes AWS
- Connecter vos comptes GCP

Module 28 : Gérer votre gestion de la posture de sécurité cloud

- Explorer le degré de sécurisation
- Explorer les recommandations
- Mesurer et appliquer la conformité réglementaire
- Comprendre les workbooks

Module 29 : Expliquer les protections de charge de travail cloud dans Microsoft Defender pour le cloud

- Comprendre Microsoft Defender pour les serveurs
- Comprendre Microsoft Defender pour App Service
- Comprendre Microsoft Defender pour le stockage
- Comprendre Microsoft Defender pour SQL
- Comprendre Microsoft Defender pour les bases de données open source
- Comprendre Microsoft Defender pour Key Vault
- Comprendre Microsoft Defender pour Resource Manager

- Comprendre Microsoft Defender pour DNS
- Comprendre le fonctionnement de Microsoft Defender pour les conteneurs
- Comprendre les protections supplémentaires de Microsoft Defender

Module 30 : Corriger les alertes de sécurité à l'aide de Microsoft Defender pour le Cloud

- Comprendre les alertes de sécurité
- Corriger les alertes et automatiser les réponses
- Supprimer les alertes de Defender pour le cloud
- Générer des rapports de renseignement sur les menaces
- Répondre aux alertes à partir de ressources Azure

Module 31 : Construire des instructions KQL pour Microsoft Azure Sentinel

- Comprendre la structure des instructions du langage de requête Kusto
- Utiliser l'opérateur de recherche
- Utiliser l'opérateur where
- Utiliser l'instruction Let
- Utiliser l'opérateur extend
- Utiliser l'ordre par opérateur
- Utiliser les opérateurs de projet

Module 32 : Analyser les résultats d'une requête à l'aide de KQL

- Utiliser l'opérateur de synthèse
- Utiliser l'opérateur de synthèse pour filtrer les résultats
- Utiliser l'opérateur de synthèse pour préparer les données
- Utiliser l'opérateur de rendu pour créer des visualisations

Module 33 : Générer des instructions de tables multiples à l'aide de KQL

- Utiliser l'opérateur d'union
- Utiliser l'opérateur de jointure

Module 34 : 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
- Extraire des données à partir de données de chaîne structurées
- Intégrer des données externes
- Créer des analyseurs avec des fonctions

Module 35 : Présentation de Microsoft Sentinel

- Présentation de Microsoft Sentinel
- Fonctionnement de Microsoft Sentinel
- Quand utiliser Microsoft Sentinel

Module 36 : Créer et gérer des espaces de travail Microsoft Sentinel

- Organisation de l'espace de travail Microsoft Sentinel
- Créer un espace de travail Microsoft Sentinel
- Gérer les espaces de travail parmi les locataires avec Azure Lighthouse
- Présentation des autorisations et des rôles Microsoft Sentinel

- Gestion des paramètres Microsoft Sentinel
- Configurer les journaux

Module 37 : Journaux de requêtes dans Microsoft Azure Sentinel

- Journaux de requête sur la page journaux
- Présentation des tables Microsoft Sentinel
- Comprendre les tables courantes
- Comprendre les tables Microsoft Defender XDR

Module 38 : Utiliser des watchlists dans Microsoft Azure Sentinel

- Planifier des watchlists
- Créer une liste de surveillance
- Gérer des listes Watchlist

Module 39 : Utiliser le renseignement sur les menaces dans Microsoft Azure Sentinel

- Définir le renseignement sur les menaces
- Gérer vos indicateurs de menace
- Afficher vos indicateurs de menace avec KQL

Module 40 : Intégrer Microsoft Defender XDR à Microsoft Sentinel

- Understand the benefits of integrating Microsoft Sentinel with Defender XDR
- Explore the capability differences between Microsoft Defender XDR and Microsoft Sentinel portals
- Onboarding Microsoft Sentinel to Microsoft Defender XDR
- Explore Microsoft Sentinel features in Microsoft Defender XDR

Module 41 : Connecter des données à Microsoft Sentinel à l'aide de connecteurs de données

- Ingérer des données de journal avec des connecteurs de données
- Comprendre les fournisseurs de connecteurs de données
- Afficher les hôtes connectés

Module 42 : Connecter des services Microsoft à Microsoft Sentinel

- Planifier les connecteurs de services Microsoft
- Connecter le connecteur Microsoft 365
- Connecter le connecteur Microsoft Entra
- Connecter le connecteur Microsoft Entra ID Protection
- Se connecter au connecteur Activité Azure

Module 43 : Connecter Microsoft Defender XDR à Microsoft Sentinel

- Planifier les connecteurs Microsoft Defender XDR
- Connecter le connecteur Microsoft Defender XDR
- Connecter le connecteur Microsoft Defender pour le cloud
- Connecter Microsoft Defender pour IoT
- Connecter les connecteurs existants Microsoft Defender

Module 44 : Connecter des hôtes Windows à Microsoft Sentinel

- Planifier le connecteur pour les événements de sécurité des hôtes Windows

- Se connecter en utilisant le connecteur Événements de sécurité Windows via AMA
- Se connecter en utilisant le connecteur Événements de sécurité via l'agent hérité
- Collecter des journaux d'événements Sysmon

Module 45 : Connecter des journaux Common Event Format à Microsoft Sentinel

- Planifier un connecteur Common Event Format
- Connecter votre solution externe en utilisant le connecteur CEF

Module 46 : Connecter des sources de données Syslog à Microsoft Sentinel

- Planifier la collecte des données Syslog
- Collecter des données à partir de sources Linux à l'aide de syslog
- Configurer la règle de collecte de données pour les sources de données Syslog
- Analyser les données syslog avec KQL

Module 47 : Connecter des indicateurs de menace à Microsoft Sentinel

- Planifier les connecteurs de renseignement sur les menaces
- Connecter le connecteur de renseignement sur les menaces TAXII
- Activer le connecteur des plateformes de renseignement sur les menaces
- Afficher vos indicateurs de menace avec KQL

Module 48 : Détection des menaces avec Analytique Microsoft Sentinel

- Qu'est-ce qu'Analytique Microsoft Sentinel ?
- Types de règles analytiques
- Créer une règle analytique à partir de modèles
- Créer une règle analytique à partir de l'Assistant
- Gérer les règles analytiques

Module 49 : Automatisation dans Microsoft Sentinel

- Comprendre les options d'automatisation
- Créer des règles d'automatisation

Module 50 : Réponse aux menaces avec les playbooks Microsoft Sentinel

- Que sont les playbooks Microsoft Sentinel ?
- Déclencher un playbook en temps réel
- Exécuter des playbooks à la demande

Module 51 : Gestion des incidents de sécurité dans Microsoft Sentinel

- Comprendre les incidents
- Preuves et entités d'incidents
- Gestion des incidents

Module 52 : Identifier les menaces avec l'analytique comportementale

- Comprendre l’analytique comportementale
- Explorer les entités
- Afficher les informations sur le comportement des entités
- Utiliser des modèles de règle analytique de détection d’anomalie

Module 53 : Normalisation des données dans Microsoft Sentinel

- Comprendre la normalisation des données
- Utiliser des analyseurs ASIM
- Comprendre les fonctions KQL paramétrables
- Créer un analyseur ASIM
- Configurer des règles de collecte de données Azure Monitor

Module 54 : Interroger, visualiser et monitorer des données dans Microsoft Sentinel

- Superviser et visualiser les données
- Interroger des données en utilisant le langage de requête Kusto
- Utiliser les workbooks Microsoft Sentinel par défaut
- Créer un workbook Microsoft Sentinel

Module 55 : Gérer le contenu dans Microsoft Sentinel

- Utiliser des solutions à partir du hub de contenu
- Utiliser des référentiels pour le déploiement

Module 56 : Expliquer les concepts de chasse des menaces dans Microsoft Sentinel

- Comprendre les repérages de menaces de cybersécurité
- Développer une hypothèse
- Explorer MITRE ATT&CK

Module 57 : Repérage des menaces avec Microsoft Sentinel

- Explorer la création et la gestion des requêtes de chasse aux menaces
- Enregistrer les résultats clés avec des signets
- Observer les menaces dans le temps avec le stream en direct

Module 58 : Utiliser des travaux de recherche dans Microsoft Sentinel

- Repérer avec un travail de recherche
- Restaurer des données historiques

Module 59 : Repérer les menaces à l’aide de notebooks dans Microsoft Sentinel

- Accéder aux données Azure Sentinel avec des outils externes
- Repérer avec les notebooks
- Créer un notebook
- Explorer le code du notebook

Lab / Exercices

- Ce cours vous donne un accès exclusif au laboratoire officiel Microsoft, vous permettant de mettre en pratique vos compétences dans un environnement professionnel.

Documentation

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

Examen

- Ce cours prépare à la certification SC-200 : Microsoft Security Operations Analyst

Profils des participants

- Analystes en cybersécurité
- Techniciens et ingénieurs systèmes
- Consultants en sécurité informatique
- Administrateurs cloud et réseau
- Responsables de la gestion des risques IT

Connaissances Préalables

- Comprendre les concepts fondamentaux de cybersécurité et de gestion des incidents
- Maîtriser les bases de Microsoft Azure et des environnements cloud
- Savoir utiliser des outils d’administration et de monitoring IT

Objectifs

- Configurer et utiliser Microsoft Sentinel pour détecter et traiter les menaces
- Analyser et corriger les incidents avec Microsoft Defender XDR
- Automatiser la réponse aux attaques avec Microsoft Defender pour Office 365
- Gérer et sécuriser les identités avec Microsoft Entra Identity Protection
- Explorer les applications cloud et protéger les données avec Microsoft Defender pour applications cloud
- Utiliser Microsoft Security Copilot pour renforcer la sécurité des opérations
- Déployer et administrer Microsoft Defender pour point de terminaison
- Analyser et corriger les alertes de sécurité avec Microsoft Defender pour le cloud

Description
Analyste des opérations de sécurité Microsoft (SC-200)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
3200
Prix de l'inscription en Virtuel (CHF)
3000
Durée (Nombre de Jours)
4
Reference
SC-200T00