Microsoft Security Operations Analyst – Formation intensive («SC200»)

Cette formation de niveau intermédiaire vous apprend à reconnaître les cybermenaces, à les analyser et à y réagir adéquatement grâce à Microsoft Sentinel, Microsoft Defender XDR et Microsoft Purview. Ce cours permet de se préparer à l'examen SC-200.

Durée: 4 jours
Prix : 3'400.– excl. 8.1% TVA
Documents : Support numérique officiel Microsoft et accès Microsoft Learn
Code officiel: SC-200

Contenu

Le contenu de cette formation intensive est basé sur le contenu de l'examen « SC-200: Microsoft Security Operations Analyst ». Commencez à vous préparer dès maintenant à votre formation sur Microsoft Learn. Lors des sessions journalières intensives avec nos experts, vous travaillerez avec les supports de formation officiels Microsoft (plus d'informations à la rubrique « méthodologie et didactique »).
Ce cours est une formation intensive (bloc de sessions journalières), si vous préférez suivre cette formation au format flexible (6 à 8 sessions virtuelles de 3 heures sur max. 4 semaines), cliquez ici.

Cette formation vous permet d'apprendre à contrer des cybermenaces à l'aide des technologies Microsoft. Vous apprendrez en particulier à configurer et utiliser Azure Sentinel ainsi que le langage Kusto Query Language (KQL) pour reconnaître et analyser des menaces ainsi que pour générer des rapports. Cette formation s'adresse aux personnes qui occupent un rôle professionnel dans la sécurité des opérations et permet de se préparer de manière optimale à l'examen.

Module 1 : Atténuer les menaces avec Microsoft Defender XDR
Analysez les données de menace dans l'ensemble des domaines et atténuez rapidement les menaces avec l'orchestration et l'automatisation intégrées dans Microsoft Defender XDR (Microsoft 365 Defender).
Chapitres

- Introduction à la protection contre les menaces avec Microsoft 365
- Réduire les incidents avec Microsoft Defender XDR
- Protéger vos identités avec Azure AD Identity Protection
- Corriger les risques avec Microsoft Defender pour Office 365
- Protéger votre environnement grâce à Microsoft Defender pour Identity
- Sécuriser vos applications et services cloud avec Microsoft Defender pour applications cloud
- Répondre aux alertes de protection contre la perte de données à l'aide de Microsoft 365
- Gérer le risque interne dans Microsoft Purview
- Investiguer les menaces à l'aide des fonctionnalités d'audit de Microsoft Defender XDR et Microsoft Purview Standard

Module 2 : Atténuer les menaces avec Microsoft Purview
Ce module se concentre sur les solutions de gestion des risques et de conformité de Microsoft Purview qui permettent aux analystes des opérations de sécurité de détecter les menaces des organisations et d'identifier, de classer et de protéger les données sensibles, ainsi que de superviser la conformité en créant des rapports.
Chapitres

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

- Gérer le risque interne dans Microsoft Purview
- Investiguer les menaces à l'aide des fonctionnalités d'audit de Microsoft Defender XDR et Microsoft Purview Standard
- Investiguer les menaces en utilisant l'audit dans Microsoft Defender XDR et Microsoft Purview Premium
- Investiguer les menaces avec une recherche de contenu dans Microsoft Purview

Module 3 : Atténuer les menaces avec Microsoft Defender pour point de terminaison
Implémentez la plateforme Microsoft Defender pour point de terminaison pour détecter, investiguer et répondre aux menaces avancées.
Chapitres

- Se protéger contre les menaces avec Microsoft Defender pour point de terminaison
- Déployer l'environnement Microsoft Defender pour point de terminaison
- Implémenter des améliorations de sécurité Windows avec Microsoft Defender pour point de terminaison
- Enquêter sur les appareils dans Microsoft Defender pour point de terminaison
- Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour point de terminaison
- Effectuer des investigations de preuve et d'identités à l'aide de Microsoft Defender pour point de terminaison
- Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour point de terminaison
- Configurer les alertes et les détections dans Microsoft Defender pour point de terminaison
- Utiliser la gestion des vulnérabilités dans Microsoft Defender pour point de terminaison

Module 4 : Atténuer les menaces avec Microsoft Defender pour le cloud
Utilisez Microsoft Defender pour protéger et sécuriser les charges de travail dans Azure, dans le cloud hybride et au niveau local.
Chapitres

- Planifier les protections des charges de travail du cloud à l'aide de Microsoft Defender pour le Cloud
- Connecter des ressources Azure à Microsoft Defender pour le cloud
- Connecter des ressources non Azure à Microsoft Defender pour le cloud
- Gérer la 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 pour le cloud

Module 5 : Créer des requêtes pour Microsoft Sentinel en utilisant Kusto Query Language (KQL)
Écrivez des instructions avec le langage de requête Kusto (KQL) pour interroger les données de journal afin d'exécuter des détections, des analyses et des rapports dans Microsoft Sentinel. Ce parcours d'apprentissage se concentre sur les opérateurs les plus utilisés. Les exemples d'instructions KQL montrent des requêtes de table relatives à la sécurité.
Chapitres

- Construire des instructions KQL pour Microsoft Azure Sentinel
- Analyser les résultats des requêtes à 'aide de KQL
- Construire des instructions de tables multiples à l'aide de KQL
- Utiliser des données dans Microsoft Azure Sentinel à l'aide de Kusto Query Language.

Module 6 : Configuration de votre environnement Microsoft Sentinel
Configurez correctement l'espace de travail Microsoft Sentinel pour bien démarrer avec Microsoft Sentinel.
Chapitres

- Introduction à Microsoft Sentinel

- Créer et gérer les espaces de travail Microsoft Sentinel
- Journaux de requêtes dans Microsoft Azure Sentinel
- Utiliser les watchlists dans Microsoft Azure Sentinel
- Utiliser les renseignements sur les menaces dans Microsoft Azure Sentinel

Module 7 : Connecter des journaux à Microsoft Sentinel
Connectez des données à l'échelle du cloud sur l'ensemble des utilisateurs, des appareils, des applications et des infrastructures, localement et dans plusieurs clouds, à Microsoft Sentinel.
Chapitres

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

Module 8 : Créer des détections et effectuer des investigations à l'aide de Microsoft Sentinel
Détectez des menaces non découvertes précédemment et remédiez rapidement aux menaces grâce à l'orchestration et à l'automatisation intégrées dans Microsoft Sentinel.
Chapitres

- Détection des menaces avec Analytique Microsoft Sentinel
- 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'analytique comportementale
- Normalisation des données dans Microsoft Sentinel
- Interroger, visualiser et surveiller les données dans Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel

Module 9 : Effectuer un repérage des menaces dans Microsoft Sentinel
Effectuez une chasse proactive aux menaces de sécurité en utilisant les puissants outils de chasse aux menaces de Microsoft Sentinel.
Chapitres

- Expliquer les concepts de chasse des menaces dans Microsoft Sentinel
- Repérage des menaces avec Microsoft Sentinel
- Utiliser des travaux de recherche dans Microsoft Sentinel
- Repérage des menaces à l'aide de notebooks dans Microsoft Sentinel

Objectifs

- Contrer les menaces avec Microsoft Defender XDR (Microsoft 365 Defender)
- Contrer les menaces avec Azure Defender
- Contrer les menaces avec Azure Sentinel
- Contrer les menaces avec Microsoft Purview

Méthodologie & Didactique

Ce cours est une formation intensive (bloc de sessions journalières), si vous préférez suivre cette formation au format flexible (6 à 8 sessions virtuelles de 3 heures sur max. 4 semaines), cliquez ici.

Formule d'apprentissage mixte de Digicomp :

- **Pre-study :** dès l'inscription à la formation, vous recevez un accès à Microsoft Learn et vous pouvez dès lors commencer individuellement à vous familiariser avec la matière. Nous vous conseillons de passer en revue toute la matière au moins une fois avant le cours et de vous concentrer plus en détail sur les passages où vous manquez le plus de connaissances.
- **After-study :** après la formation, vous continuez à avoir accès à Microsoft Learn. Vous pouvez ainsi continuer à apprendre et à vous exercer selon vos besoins afin de permettre un apprentissage plus durable et de vous préparer idéalement à l'examen de certification.

Public cible

Les analystes des opérations de sécurité de Microsoft collaborent avec les parties prenantes d'une organisation pour sécuriser les systèmes de technologie de l'information. Leur objectif est de réduire les risques organisationnels en remédiant rapidement aux attaques actives dans l'environnement, en donnant des conseils sur les améliorations à apporter aux pratiques de protection contre les menaces et en signalant les violations des politiques organisationnelles aux parties prenantes appropriées. Leurs responsabilités comprennent la gestion, la surveillance et la réponse aux menaces en utilisant une variété de solutions de sécurité dans leur environnement. Leur rôle consiste principalement à enquêter sur les menaces, à y répondre et à les repérer en utilisant Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender et des produits de sécurité tiers. Puisque les analystes des opérations de sécurité utilisent le résultat opérationnel de ces outils, ils sont également des parties prenantes essentielles dans la configuration et le déploiement de ces technologies.

Prérequis

- Connaissances fondamentales de Microsoft 365
- Connaissances fondamentales des produits de sécurité, de conformité et d'identité de Microsoft.
- Connaissances intermédiaires de Windows 10
- Familiarité avec les services Azure, notamment Azure SQL Database et Azure Storage
- Familiarité avec les machines virtuelles Azure et les réseaux virtuels
- Connaissances fondamentales des concepts de scripting

Nous recommandons de suivre le cours suivant au préalable ou de vous assurer de posséder des connaissances équivalentes :

Microsoft Security, Compliance, and Identity Fundamentals («SC900»)

- Microsoft Security, Compliance, and Identity Fundamentals – Formation intensive («SC900»)
- Microsoft Security, Compliance, and Identity Fundamentals – Formation flexible («SC900V»)

Certification

Cette formation marque la première étape de préparation à l'**examen** :

« SC-200: Microsoft Security Operations Analyst »

La réussite de cet examen permet de décrocher la **certification** :

ATTENTION : L'examen ne se déroule pas dans le cadre de la formation, vous devrez vous y inscrire séparément. Pratiquer vos nouvelles connaissances en situation réelle augmente considérablement vos chances de réussite à l'examen, c'est pourquoi nous vous conseillons de ne pas passer l'examen tout de suite après votre formation, mais de prendre votre temps et de vous y inscrire lorsque vous serez prêt.

Inscription à l'examen

Vous avez la possibilité de vous inscrire à un examen que vous passerez soit dans un de nos centres de formation Digicomp, agréés centre de test Pearson Vue, à Lausanne ou Genève, soit depuis chez vous.

Chez Digicomp : Inscrivez-vous à l'examen directement sur le site de Pearson VUE et sélectionnez l'un de nos centres de formation Digicomp (Lausanne ou Genève). Vous pourrez ensuite choisir parmi les créneaux d'examen proposés dans nos centres.

Chez vous : Pour passer un examen depuis chez vous, vous devez vous inscrire en passant par ce lien.

Le prix de l'examen est de CHF 216.- (sous réserve de modification par l'éditeur).

Formations complémentaires

- Microsoft Cybersecurity Architect – Formation intensive («SC100»)

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-digital-transformation-technologies/cloud/cloud-security/cours-microsoft-security-operations-analyst-formation-intensive-sc-200