Microsoft Security Operations Analyst (SC-200T00)

ID SC-200T00 **Prix** CHF 3 380,– (Hors Taxe) **Durée** 4 jours

A qui s'adresse cette formation

- Analystes sécurité
- Ingénieurs sécurité

Cette formation prépare à la/aux certifications

Microsoft Certified: Security Operations Analyst Associate (MCSOAA)

Pré-requis

- Compréhension de base de Microsoft 365
- Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft
- Compréhension intermédiaire de Windows 10
- Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure
- Connaissance des machines virtuelles Azure et des réseaux virtuels
- Compréhension de base des concepts de script

Disposez-vous des connaissances nécessaires pour suivre cette formation ? N'hésitez pas à suivre ce test de positionnement : Auto-évaluation

Objectifs

À l'issue de ce cours, vous serez capable de :

- Être capable d'expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement
- Savoir créer un environnement Microsoft Defender pour Endpoint
- Apprendre à configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10
- Comprendre comment effectuer des actions sur un appareil à l'aide de Microsoft Defender pour Endpoint
- Pouvoir examiner les domaines et les adresses IP dans Microsoft Defender pour Endpoint
- Être en mesure d'examiner les comptes d'utilisateurs et configurer les paramètres d'alerte dans Microsoft Defender pour Endpoint
- Comprendre comment effectuer une recherche avancée dans Microsoft 365 Defender
- Savoir gérer les incidents dans Microsoft 365 Defender
- Expliquer comment Microsoft Defender for Identity peut remédier aux risques dans votre environnement
- Pouvoir examiner les alertes DLP dans Microsoft Cloud App Security
- Apprendre à configurer l'approvisionnement automatique dans Azure Defender
- Comprendre comment corriger les alertes dans Azure Defender
- Savoir construire des instructions KQL
- Pouvoir 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
- Comprendre comment extraire des données de champs de chaîne non structurés à l'aide de KQL
- Savoir gérer un espace de travail Azure Sentinel
- Apprendre à utiliser KQL pour accéder à la liste de surveillance dans Azure Sentinel
- Pouvoir gérer les indicateurs de menace dans Azure Sentinel
- Être capable de connecter les machines virtuelles Azure Windows à Azure Sentinel
- Apprendre à configurer l'agent Log Analytics pour collecter les événements Sysmon
- Savoir créer de nouvelles règles et requêtes d'analyse à l'aide de l'assistant de règle d'analyse
- Pouvoir utiliser des requêtes pour rechercher les menaces

Contenu

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 oeuvre les améliorations de la 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

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 les identités avec Azure AD Identity Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protéger son environnement avec Microsoft Defender for Identity
- Sécuriser ses applications et services cloud avec Microsoft Cloud App Security
- Répondre aux alertes de prévention de la perte de données à l'aide de Microsoft 365
- Gérer les risques internes dans Microsoft 365

ATTÉNUER LES MENACES À L'AIDE D'AZURE DEFENDER

- Planifier les protections de la charge de travail cloud à l'aide d'Azure Defender
- Expliquer les protections des charges de travail cloud dans Azure Defender
- Connecter les actifs Azure à Azure Defender
- Connecter des ressources non-Azure à Azure Defender
- Corriger les alertes de sécurité à l'aide d'Azure Defender

CRÉER DES REQUÊTES POUR AZURE SENTINEL À L'AIDE DU LANGAGE DE REQUÊTE KUSTO (KQL)

- Construire des instructions KQL pour Azure Sentinel
- Analyser les résultats des requêtes à l'aide de KQL
- Créer des instructions multi-tables à l'aide de KQL
- Travailler avec des données dans Azure Sentinel à l'aide du langage de requête Kusto

CONFIGURER VOTRE ENVIRONNEMENT AZURE SENTINEL

- Introduction à Azure Sentinel
- Créer et gérer des espaces de travail Azure Sentinel
- Requête des journaux dans Azure Sentinel
- Utiliser des listes de surveillance dans Azure Sentinel
- Utiliser l'intelligence des menaces dans Azure Sentinel

CONNECTER LES JOURNAUX À AZURE SENTINEL

- Connecter les 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 du format d'événement commun à Azure Sentinel
- Connecter les sources de données Syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel

CRÉER DES DÉTECTIONS ET EFFECTUER DES INVESTIGATIONS À L'AIDE D'AZURE SENTINEL

- Détection des menaces avec l'analyse Azure Sentinel
- Réponse aux menaces avec les playbooks Azure Sentinel
- Gestion des 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

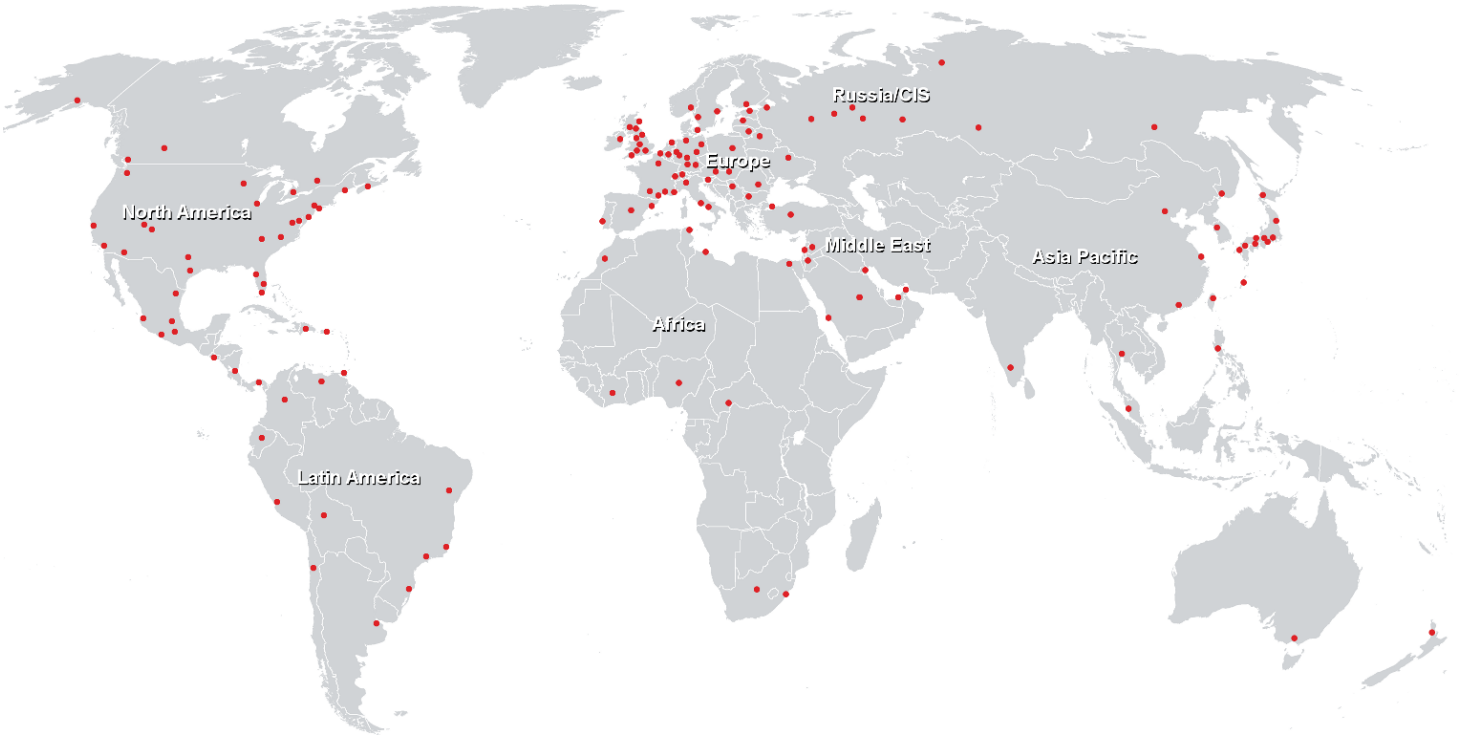
EFFECTUER UNE RECHERCHE DE MENACES DANS AZURE SENTINEL

- Chasse aux menaces avec Azure Sentinel
- Traquer les menaces à l'aide de blocs-notes dans Azure Sentinel

Microsoft Security Operations Analyst (SC-200T00)

Microsoft Solutions Partner
Microsoft Cloud Training Services

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch