Configurer les opérations de sécurité SIEM à l’aide de Microsoft Sentinel (SC-5001)

Description

Maîtrisez la configuration de Microsoft Sentinel pour sécuriser vos systèmes

La cybersécurité est un enjeu majeur pour toutes les entreprises. Avec l’augmentation des cyberattaques, il est essentiel d’avoir un système efficace pour surveiller, détecter et répondre aux menaces. La formation SC-5001 « Configurer les opérations de sécurité SIEM à l’aide de Microsoft Sentinel » vous permet d’acquérir les compétences nécessaires pour mettre en place une surveillance avancée avec Microsoft Sentinel.

Grâce à cette formation en cybersécurité, vous apprendrez à configurer votre espace de travail dans Azure, à connecter différents services Microsoft et à exploiter Azure Log Analytics pour analyser les journaux d’événements. Vous découvrirez aussi comment optimiser la détection des menaces avec des règles analytiques et automatiser certaines tâches grâce à Azure Logic Apps. L’objectif est clair : renforcer votre posture de sécurité et protéger efficacement vos infrastructures IT.

Contenu du cours
Module 1 : 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 2 : 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 3 : Connecter des hôtes Windows à Microsoft Sentinel

- Configurer le connecteur Événements de sécurité Windows
- Collecter et analyser les journaux d’événements Windows

Module 4 : 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 5 : Automatisation dans Microsoft Sentinel

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

Module 6 : Configurer les opérations de sécurité SIEM à l’aide de Microsoft Sentinel

- Installer des solutions d’hub de contenu Microsoft Sentinel et des connecteurs de données
- Configurer un connecteur de données Règle de collecte de données
- Effectuer une attaque simulée pour valider les règles d’analytique et d’automatisation

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.

Profils des participants

- Analystes en cybersécurité
- Administrateurs systèmes et réseaux
- Ingénieurs en sécurité informatique
- Consultants en sécurité des systèmes d’information
- Responsables de la sécurité des systèmes d’information (RSSI)

Connaissances Préalables

- Comprendre les bases de Microsoft Azure
- Avoir une connaissance élémentaire de Microsoft Sentinel
- Maîtriser le langage de requête Kusto (KQL) dans Microsoft Sentinel

Objectifs

- Configurer et gérer un espace de travail Microsoft Sentinel
- Connecter les services Microsoft et intégrer des journaux d’événements
- Exploiter Azure Log Analytics pour surveiller et analyser les données
- Mettre en place des règles analytiques pour détecter les menaces
- Automatiser la gestion des incidents avec Azure Logic Apps
- Optimiser la protection et la surveillance des infrastructures IT

Description
Configurer les opérations de sécurité SIEM à l’aide de Microsoft Sentinel (SC-5001)
Niveau

Intermédiaire
Prix de l'inscription en Présentiel (CHF)
900
Prix de l'inscription en Virtuel (CHF)
850
Durée (Nombre de Jours)
1
Reference
SC-5001