Programme de cours
Configurer les opérations de sécurité SIEM à l'aide de Microsoft Sentinel

Durée :	1 jour soit 7 heures	Référence :	SC-5001

Public visé :

Cette formation s'adresse principalement à des professionnels des technologies de l'information (TI) et de la cybersécurité ayant une expérience préalable avec Microsoft Azure et des connaissances de base sur Microsoft Sentinel. Plus précisément :

- **Analystes SOC (Security Operations Center)** responsables de la détection, de la gestion et de la réponse aux menaces de sécurité.
- **Administrateurs de sécurité informatique** chargés de configurer et d'optimiser les outils de surveillance et d'analyse de la sécurité.
- **Ingénieurs SIEM/SOAR** qui conçoivent, déploient et maintiennent des solutions d'opérations de sécurité basées sur Microsoft Sentinel.
- **Consultants ou architectes en cybersécurité** cherchant à mettre en œuvre des solutions Microsoft Sentinel.

Pré-requis :

- Connaissances fondamentales de Microsoft Azure
- Compréhension de base de Microsoft Sentinel
- Expérience de l'utilisation du langage de requête Kusto (KQL) dans Microsoft Sentinel

Objectifs pédagogiques :

- Décrire l'architecture de l'espace de travail Microsoft Sentinel
- Installer un espace de travail Microsoft Sentinel
- Gérer un espace de travail Microsoft Sentinel
- Connecter les connecteurs de services Microsoft
- Expliquer comment les connecteurs créent automatiquement des incidents dans Microsoft Sentinel
- Connecter des 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
- Expliquer l'importance des analyses de Microsoft Sentinel
- Expliquer les différents types de règles d'analyse
- Créer des règles à partir de modèles
- Créer de nouvelles règles d'analyse et des requêtes à l'aide de l'assistant de règles d'analyse
- Gérer les règles avec des modifications
- Expliquer les options d'automatisation dans Microsoft Sentinel
- Créer des règles d'automatisation dans Microsoft Sentinel
- Créer et configurer un espace de travail Microsoft Sentinel
- Déployer des solutions et des connecteurs de données du Microsoft Sentinel Content Hub
- Configurer les règles de collecte de données Microsoft Sentinel, les règles analytiques NRT et l'automatisation
- Effectuer une attaque simulée pour valider les règles analytiques et d'automatisation

Compétences acquises à l'issue de la formation :

- Configurer et gérer les espaces de travail Microsoft Sentinel. Être capable de planifier, créer, configurer et administrer des espaces de travail Sentinel, y compris la gestion multi-locataires via Azure Lighthouse.
- Intégrer et connecter les services Microsoft à Microsoft Sentinel. Savoir connecter Microsoft 365, Microsoft Entra, Azure Activity et d'autres connecteurs pour centraliser les journaux et données de sécurité.
- Connecter et superviser les hôtes Windows et collecter des données Sysmon. Maîtriser la connexion de machines virtuelles Azure et d'hôtes non-Azure à Sentinel, y compris l'installation et la configuration de l'agent Log Analytics pour collecter les événements Sysmon.
- Créer et personnaliser des règles d'analyse dans Microsoft Sentinel. Être capable de concevoir des règles analytiques en utilisant des modèles, des assistants et des requêtes KQL pour détecter les menaces.
- Analyser et répondre aux menaces de sécurité. Utiliser les outils d'analyse de Sentinel pour détecter, examiner et répondre aux incidents de sécurité en temps réel.
- Automatiser les opérations de sécurité dans Microsoft Sentinel Configurer et mettre en œuvre des règles d'automatisation et des playbooks pour améliorer l'efficacité des réponses aux incidents.
- Déployer et configurer des connecteurs de données à partir du Content Hub. Appréhender le déploiement de solutions prêtes à l'emploi et de connecteurs depuis le Content Hub pour enrichir les capacités de collecte et d'analyse de Sentinel.
- Valider et optimiser les règles analytiques et d'automatisation. Réaliser des simulations d'attaques pour tester, ajuster et optimiser les règles analytiques et les automatisations dans un environnement de production.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo

- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Description / Contenu

Module 1 : Créer et gérer des espaces de travail Microsoft Sentinel

- Planifier l'espace de travail Microsoft Sentinel
- Créer un espace de travail Microsoft Sentinel
- Gérer les espaces de travail à travers des locataires à l'aide d'Azure Lighthouse
- Comprendre les permissions et rôles de Microsoft Sentinel
- Gérer les paramètres de Microsoft Sentinel
- Configurer les journaux

Module 2 : Connect Microsoft services to 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
- Connecter le connecteur Azure Activity

Module 3 : Connecter les hôtes Windows à Microsoft Sentinel

- Planifier le connecteur des événements de sécurité des hôtes Windows
- Connecter en utilisant le connecteur Windows Security Events via AMA
- Connecter en utilisant le connecteur Security Events via l'agent hérité
- Collecter les journaux des événements Sysmon

Module 4 : Détection des menaces avec les analyses de Microsoft Sentinel

- Exercice - Détecter les menaces avec les analyses de Microsoft Sentinel
- Qu'est-ce que Microsoft Sentinel Analytics ?
- Types de règles d'analyse
- Créer une règle d'analyse à partir de modèles
- Créer une règle d'analyse à partir de l'assistant
- Gérer les règles d'analyse

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

- Exercice - Configurer les opérations SIEM à l'aide de Microsoft Sentinel
- Exercice - Installer les solutions et les connecteurs de données du Microsoft Sentinel Content Hub
- Exercice - Configurer une règle de collecte de données pour un connecteur de données
- Exercice - Effectuer une attaque simulée pour valider les règles analytiques et d'automatisation