Configurer les opérations de sécurité SIEM avec Microsoft Sentinel

Détectez, analysez et répondez aux menaces en temps réel

A distance

7 h

Prix inter : 950,00 € HT
Forfait intra : 2.850,00 € HT

Réf.: MSSC5001

Microsoft Sentinel est une solution **SIEM cloud-native conçue pour fournir des analyses intelligentes, une détection proactive des menaces et une réponse automatisée**. Cette formation opérationnelle vous guide dans la configuration de Microsoft Sentinel, depuis la connexion de sources de données jusqu'à la création de règles d'analytique et de règles d'automatisation (playbooks).
Les participants découvrent comment collecter des données avec les connecteurs intégrés, gérer les journaux d'activité, créer et ajuster des règles d'alerte, ainsi que piloter la réponse aux incidents à l'aide de **SOAR**. Une montée en compétence essentielle pour **sécuriser les environnements cloud et hybrides** grâce à une visibilité complète et en temps réel sur les menaces.

A qui s'adresse cette formation ?

Pour qui

- Analyste des opérations de sécurité

Prérequis

- Comprendre les bases de Microsoft Azure
- Connaissance élémentaire de Microsoft Sentinel
- Savoir utiliser le langage de requête Kusto (KQL) dans Microsoft Sentinel
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Créer et gérer des espaces de travail Microsoft Sentinel

- Comprendre l'architecture d'un espace de travail Microsoft Sentinel
- Déployer un espace de travail Microsoft Sentinel
- Administrer et gérer un espace de travail Microsoft Sentinel

2 - Connecter des services Microsoft à Microsoft Sentinel

- Configurer les connecteurs de services Microsoft dans Microsoft Sentinel
- Comprendre comment les connecteurs génèrent automatiquement des incidents dans Microsoft Sentinel

3 - Connecter des hôtes Windows à Microsoft Sentinel

- Connecter des machines virtuelles Windows hébergées dans Azure à Microsoft Sentinel
- Connecter des hôtes Windows hors Azure à Microsoft Sentinel
- Installer et configurer un connecteur de données pour la collecte des événements Sysmon

4 - Détection des menaces avec Analytique Microsoft Sentinel

- Comprendre l'importance de l'analytique dans Microsoft Sentinel pour la détection des menaces
- Identifier les différents types de règles analytiques disponibles dans Microsoft Sentinel
- Créer des règles analytiques à partir de modèles prédéfinis

- Concevoir des règles et requêtes personnalisées avec l'assistant de création de règles analytiques
- Gérer et modifier les règles analytiques en fonction de l'évolution des besoins

5 - Automatisation dans Microsoft Sentinel

- Découvrir les options d'automatisation disponibles dans Microsoft Sentinel
- Créer et configurer des règles d'automatisation pour orchestrer les réponses aux incidents

6 - Configurer les opérations de sécurité SIEM à l'aide de Microsoft Sentinel

- Mettre en place et configurer un espace de travail Microsoft Sentinel
- Déployer des solutions du Content Hub et configurer les connecteurs de données
- Paramétrer les règles de collecte, d'analyse en temps réel (NRT) et d'automatisation dans Microsoft Sentinel
- Simuler une attaque pour valider les règles d'analyse et d'automatisation
  Atelier

  Configurer les opérations SIEM avec Microsoft Sentinel

  Installer des solutions depuis le Content Hub et connecter des sources de données

  Définir une règle de collecte de données pour un connecteur spécifique

  Simuler une attaque pour tester les règles d'analyse et d'automatisation

Les objectifs de la formation

- Créer et configurer un workspace Sentinel opérationnel
- Déployer Content Hub et activer les connecteurs de données
- Établir des règles analytiques NRT pour détecter les menaces
- Mettre en place des règles d'automatisation et playbooks
- Simuler une attaque et valider l'efficacité des règles analytic et automation
- Intégrer Sentinel avec Defender XDR pour une réponse coordonnée

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Alternance entre explications théoriques et exercices pratiques
- Vérification opérationnelle grâce à des scénarios réalistes (attaque simulée + intégration Defender XDR)
- Projet guidé pour valider l'ensemble des compétences SIEM/SOAR acquises

Dates 2025 - Référence MSSC5001

Dernières places disponibles Session garantie

le 15 déc.
- le 15 déc. 9h00 -> 17h00