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

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Analystes en cybersécurité (SOC) souhaitant configurer et exploiter une solution SIEM
- Administrateurs systèmes et réseaux impliqués dans la sécurité des environnements TI
- Ingénieurs ou professionnels en sécurité informatique
- Spécialistes de la gestion des incidents et des menaces
- Toute personne souhaitant déployer et opérer Microsoft Sentinel pour la surveillance et la réponse aux incidents

Objectifs de la formation

- Créer et configurer un espace de travail Microsoft Sentinel Déployer des solutions et connecter les sources de données (services Microsoft, événements Windows)
- Configurer des règles d’analytique pour détecter les menaces
- Automatiser les réponses aux incidents à l’aide des capacités SOAR de Sentinel
- Exploiter Microsoft Sentinel pour surveiller, analyser et gérer les opérations de sécurité
- Mettre en place une chaîne complète de détection et de réponse aux menaces

Description sommaire

Les formations Applied Skills sont conçues pour valider des compétences spécifiques en étant orientées vers des scénarios réels. Elles offrent une alternative ciblée aux certifications traditionnelles basées sur des rôles, en mettant l'accent sur l'application des compétences techniques dans des situations professionnelles concrètes.

Démarrez avec les opérations de sécurité Microsoft Sentinel en configurant l'espace de travail Microsoft Sentinel, en connectant les services Microsoft et les événements de sécurité Windows à Microsoft Sentinel, en configurant les règles d'analyse Microsoft Sentinel et en répondant aux menaces avec des réponses automatisées.

Contenu du plan de cours

- Créer et gérer des espaces de travail Microsoft Sentinel
- Connecter les services Microsoft à Microsoft Sentinel
- Connecter les hôtes Windows à Microsoft Sentinel
- Détection des menaces avec l'analyse Microsoft Sentinel
- Automatisation dans Microsoft Sentinel
- Configurer les opérations de sécurité SIEM à l'aide de Microsoft Sentinel

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés.

Les participants configurent et exploitent progressivement les opérations de sécurité SIEM à l’aide de Microsoft Sentinel à travers des exercices concrets inspirés de scénarios réels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à collecter, analyser et corréler les données de sécurité afin de détecter, investiguer et répondre efficacement aux incidents.

Animée par un formateur certifié Microsoft, la formation privilégie l’interactivité et le développement de compétences techniques directement transférables pour renforcer la posture de sécurité des organisations en contexte professionnel.

Prérequis

- Compréhension fondamentale de Microsoft Azure ou contenu équivalent
- Compréhension de base de Microsoft Sentinel ou contenu équivalent
- Expérience de l'utilisation du langage de requête Kusto (KQL) dans Microsoft Sentinel ou contenu équivalent.
-

Vous devez disposer de votre propre abonnement Azure. (Vous avez besoin d'un abonnement Azure pour effectuer les exercices. Si vous ne disposez pas d'un abonnement Azure, créez un compte gratuit et ajoutez un abonnement avant de commencer. Si vous êtes étudiant, vous pouvez profiter de l'offre Azure pour étudiants.)

Recommandations

- Bases en cybersécurité (menaces, surveillance, réponse aux incidents)
- Connaissance des concepts SIEM et SOC Familiarité avec les environnements Microsoft Azure
- Notions de réseautique et gestion des logs
- Compréhension des principes de sécurité des identités (Microsoft Entra ID)