Configurer les opérations de sécurité SIEM avec Microsoft Sentinel

Durée: 1 Jour **Réf de cours: M-SC5001**

Résumé:

Commencez à utiliser 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 par des réponses automatisées.
Mis à jour Mars 2024.

Public visé:

Ce cours s'adresse principalement aux professionnels souhaitant apprendre à utliser et administrer Microsoft Sentinel.

Objectifs pédagogiques:

- À l'issue de la formation, les participants seront capables de :
- Créer et gérer des espaces de travail Microsoft Sentinel
- Connecter les services Microsoft à Microsoft Sentinel
- Connecter les hôtes Windows à Microsoft Sentinel
- Détecter les menaces avec l'analyse Microsoft Sentinel
- Automatiser les opérations avec Microsoft Sentinel
- Configurer les opérations de sécurité SIEM à l'aide de Microsoft Sentinel

Pré-requis:

Les participants doivent avoir les prérequis suivants :

- Connaissance fondamentale de Microsoft Azure
- Notions de base sur Microsoft Sentinel
- Expérience de l'utilisation de Kusto Query Language (KQL) dans Microsoft Sentinel

Contenu:

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

- Découvrir l'architecture des espaces de travail Microsoft Sentinel pour configurer le système de manière à répondre aux exigences de l'entreprise en matière d'opérations de sécurité.
- Planifier l'espace de travail Microsoft Sentinel
- Créer un espace de travail Microsoft Sentinel
- Gérer les espaces de travail entre les locataires à l'aide d'Azure Lighthouse
- Comprendre les autorisations et les rôles de Microsoft Sentinel
- Gérer les paramètres de Microsoft Sentinel
- Configurer les journaux

Module 2 : Connecter les services Microsoft à Microsoft Sentinel

- Apprendre à connecter les journaux des services Microsoft 365 et Azure à Microsoft Sentinel.
- Planifier les connecteurs de services Microsoft
- Connecter le connecteur Microsoft Office 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

- Une des logs les plus habituelles à collecter est celui des événements de sécurité Windows. Découvrez comment Microsoft Sentinel facilite cette tâche grâce au connecteur Security Events.
- Planifier le connecteur d'événements de sécurité pour les hôtes Windows
- Connexion à l'aide des événements de sécurité Windows via le connecteur AMA
- Connexion à l'aide du connecteur d'événements de sécurité via l'agent hérité
- Collecter les journaux d'événements Sysmon

Module 4 : Détection des menaces avec Microsoft Sentinel Analytics

- Apprendre comment Microsoft Sentinel Analytics peut aider l'équipe SecOps à identifier et à stopper les cyberattaques.
- Exercice - Détecter les menaces avec Microsoft Sentinel Analytics
- 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 d'un assistant
- Gérer les règles d'analyse
- Exercice - Détecter les menaces avec Microsoft Sentinel Analytics

Module 5 : Automatisation dans Microsoft Sentinel

- Utiliser les règles d'automatisation dans Microsoft Sentinel pour automatiser la gestion des incidents.
- Comprendre les options d'automatisation
- Créer des règles d'automatisation

Module 6 : Configurer les opérations de sécurité SIEM avec Microsoft Sentinel

- Dans ce module, vous avez appris à 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 Microsoft Sentinel Content Hub et les connecteurs de données
- Exercice - Configurer un connecteur de données Règle de collecte de données
- Exercice - Effectuer une attaque simulée pour valider les règles d'analyse et d'automatisation

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Un support de cours officiel sera remis aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement