Analyse des opérations de sécurité Microsoft

Durée: 4 Jours **Réf de cours: M-SC200**

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour atténuer les cybermenaces à l'aide de Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender. Ces derniers configureront et utiliserot Azure Sentinel et utiliser Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la création de rapports.
Mise à jour : 14.12.2022

Public visé:

Cette formation s'adresse aux personnes qui occupent un poste dans le domaine des opérations de sécurité et notamment les analystes des opérations de sécurité Microsoft.
L'analyste des opérations de sécurité Microsoft collabore avec les parties prenantes de l'organisation pour sécuriser les systèmes informatiques de l'organisation. Leur objectif est de réduire les risques organisationnels en corrigeant rapidement les attaques actives dans l'environnement, en conseillant sur les améliorations des pratiques de protection contre les menaces et en référant les violations des politiques organisationnelles aux parties prenantes appropriées. Les responsabilités incluent la gestion, la surveillance et la réponse aux menaces en utilisant une variété de solutions de sécurité dans leur environnement.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Créer un environnement Microsoft Defender pour Endpoint
- Examiner les domaines, les adresses IP et les comptes d'utilisateurs dans Microsoft Defender pour Endpoint
- Décrire la configuration des paramètres d'alerte dans Microsoft Defender pour Endpoint
- Examiner les alertes DLP dans Microsoft Cloud App Security
- Décrire la configuration de l'approvisionnement automatique dans Azure Defender
- Corriger les alertes dans Azure Defender
- Filtrer les recherches en fonction de l'heure de l'événement, de la gravité, du domaine et d'autres données pertinentes à l'aide de KQL
- Décrire la gestion d'un espace de travail et expliquer les indicateurs de menace dans Azure Sentinel
- Configurer l'agent Log Analytics pour collecter les événements Sysmon
- Créer un playbook pour automatiser une réponse à un incident

Pré-requis:

- Compréhension de base de Microsoft 365
- Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft
- Compréhension intermédiaire de Windows 10
- Etre familier avec les services Azure, en particulier Azure SQL Database et Azure Storage
- Connaissance des machines virtuelles Azure et des réseaux virtuels
- Compréhension de base des concepts de script.

Test et certification

Cette formation prépare les participants qui le souhaitent à passer l'examen SC-200: Microsoft Security Operations Analyst. (Non inclus dans le prix de la formation)

Contenu:

Atténuer les menaces à l'aide de Microsoft Defender pour Endpoint

- Se protéger contre les menaces avec Microsoft Defender pour Endpoint
- Déployer l'environnement Microsoft Defender pour Endpoint
- Mettre en œuvre les améliorations de la sécurité de Windows 10
- Gérer les alertes et les incidents
- Effectuer des enquêtes sur les appareils
- Effectuer des actions sur un appareil
- Effectuer des enquêtes sur les preuves et les entités
- Configurer et gérer l'automatisation
- Configurer les alertes et les détections
- Utiliser la gestion des menaces et des vulnérabilités

Atténuer les menaces à l'aide de Microsoft 365 Defender

- Introduction à la protection contre les menaces avec Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger vos identités avec Azure AD Identity Protection
- Remédier aux risques avec Microsoft Defender pour Office 365
- Protéger votre environnement avec Microsoft Defender for Identity
- Sécuriser vos applications et services cloud avec Microsoft Cloud App Security
- Répondre aux alertes de prévention de la perte de données à l'aide de Microsoft 365
- Gérer les risques internes dans Microsoft 365

Atténuer les menaces à l'aide d'Azure Defender

- Planifier les protections de la charge de travail cloud
- Expliquer les protections des charges de travail cloud
- Connecter les actifs Azure
- Connecter des ressources non-Azure
- Corriger les alertes de sécurité

Créer des requêtes pour Azure Sentinel à l'aide du langage de requête Kusto (KQL)

- Construire des instructions KQL pour Azure Sentinel
- Analyser les résultats des requêtes à l'aide de KQL
- Créer des instructions multi-tables à l'aide de KQL
- Travailler avec des données dans Azure Sentinel à l'aide du langage de requête Kusto

Configurer votre environnement Azure Sentinel

- Introduction à Azure Sentinel
- Créer et gérer des espaces de travail Azure Sentinel
- Requête des journaux dans Azure Sentinel
- Utiliser des listes de surveillance dans Azure Sentinel
- Utiliser l'intelligence des menaces dans Azure Sentinel

Connecter les journaux de logs à Azure Sentinel

- Connecter les données à Azure Sentinel à l'aide de connecteurs de données
- Connecter les services Microsoft à Azure Sentinel
- Connecter Microsoft 365 Defender à Azure Sentinel
- Connecter les hôtes Windows à Azure Sentinel
- Connecter les journaux du format d'événement commun à Azure Sentinel
- Connecter les sources de données Syslog à Azure Sentinel
- Connecter les indicateurs de menace à Azure Sentinel

Créer des détections et effectuer des enquêtes à l'aide d'Azure Sentinel

- Détection des menaces avec l'analyse Azure Sentinel
- Réponse aux menaces avec les playbooks Azure Sentinel
- Gestion des incidents de sécurité dans Azure Sentinel
- Utiliser l'analyse du comportement des entités dans Azure Sentinel
- Interroger, visualiser et surveiller des données dans Azure Sentinel

Effectuer une recherche de menaces dans Azure Sentinel

- Chasse aux menaces avec Azure Sentinel
- Traquer les menaces à l'aide de blocs-notes dans Azure Sentinel

Méthodes pédagogiques :

Accès fourni au contenu digital officiel Microsoft
Important
Microsoft a sécurisé ses offres de formation en ajoutant l'authentification multi-facteurs (MFA) pour accéder aux tenants de Microsoft 365 et Dynamics 365.
Pour accéder à certains TP, les stagiaires devront activer la MFA. Ils auront besoin d'un téléphone portable pour configurer et vérifier la MFA. Ils auront également besoin d'une application capable de générer des codes d'authentification. L'application suggérée est Microsoft Mobile Phone Authenticator, qui est gratuite.
Voici le lien de téléchargement de l'application ainsi que la procédure d'installation :
Download the Microsoft Mobile Phone Authenticator App
Set up your Microsoft 365 sign-in for multi-factor authentication

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