Formation Analyste des opérations de sécurité Microsoft

Maitrisers les outils de sécurité Microsoft pour parer les risques

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Découvrez comment enquêter, répondre et rechercher les menaces à l'aide de Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender. Dans ce cours, vous apprendrez comment atténuer les cybermenaces à l'aide de ces technologies. Plus précisément, vous allez configurer et utiliser Azure Sentinel et utiliser Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la création de rapports. Le cours a été conçu pour les personnes qui occupent un poste dans le domaine des opérations de sécurité et aide les apprenants à se préparer à l'examen SC-200: Analyste des opérations de sécurité Microsoft.

Référence	SEC200
Durée	4 jours (28h)
Tarif	2 695 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 27 au 30 mai 2024
du 29 juil. au 1er août 2024
du 28 au 31 octobre 2024

PARIS

du 27 au 30 mai 2024
du 28 au 31 octobre 2024

VOIR TOUTES LES DATES

Objectifs

| expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement
| administrer un environnement Microsoft Defender pour Endpoint
| configurer les règles de réduction de la surface d'attaque sur les appareils Windows
| examiner les domaines et les adresses IP dans Microsoft Defender pour Endpoint
| examiner les comptes d'utilisateurs et configurer les paramètres d'alerte dans Microsoft Defender
| effectuer une recherche avancée dans Microsoft 365 Defender
| gérer les incidents dans Microsoft 365 Defender
| réduire les risques dans votre environnement avec Microsoft Defender for Identit
| examiner les alertes DLP dans Microsoft Defender pour les applications Cloud
| configurer le pprovisionnement automatique dans Microsoft Defender pour les applications cloud
| corriger les alertes dans Microsoft Defender pour les applications cloud
| construire des instructions KQL
| 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
| extraire des données de champs de chaîne non structurés à l'aide de KQL
| gérer un espace de travail Microsoft Sentinel
| utiliser KQL pour accéder à la liste de surveillance dans Microsoft Sentinel
| gérer les indicateurs de menace dans Microsoft Sentinel
| connecter des machines virtuelles Windows Azure à Microsoft Sentinel
| configurer l'agent Log Analytics pour collecter les événements Sysmon
| créer de nouvelles règles et requêtes d'analyse à l'aide de l'assistant de règle d'analyse
| utiliser des requêtes pour chasser les menaces

Public

| Analystes sécurité
| Ingénieurs sécurité

Prérequis

| Compréhension de base de Microsoft 365
| Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft
| Compréhension intermédiaire de Microsoft Windows

| Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure
| Connaissance des machines virtuelles Azure et des réseaux virtuels
| Compréhension de base des concepts de script

Programme de la formation

Atténuer les menaces à l'aide de Microsoft 365 Defender
| Présentation de la protection contre les menaces Microsoft 365
| Atténuer les incidents à l'aide de Microsoft 365 Defender
| Protéger les identités avec Azure AD Identity Protection
| Corriger les risques avec Microsoft Defender pour Office 365
| Protéger un environnement avec Microsoft Defender pour Identity
| Sécuriser les applications et services cloud avec Microsoft Defender pour les applications cloud
| Répondre aux alertes de prévention des pertes de données à l'aide de Microsoft 365
| Gérer les risques internes dans Microsoft 365

Atténuer les menaces à l'aide de Microsoft Defender for Endpoint
| Se protéger contre les menaces avec Microsoft Defender for Endpoint
| Déployer l'environnement Microsoft Defender pour Endpoint
| Implémenter les améliorations de sécurité de Windows
| 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 vulnérabilités

Atténuer les menaces à l'aide de Microsoft Defender pour le cloud
| Planifier les protections des charges de travail cloud à l'aide de Microsoft Defender pour le cloud
| Connecter les actifs Azure à Microsoft Defender pour le Cloud
| Connecter des ressources non Azure à Microsoft Defender pour le cloud
| Gérer la gestion de votre posture de sécurité cloud
| Expliquer les protections de charge de travail cloud dans Microsoft Defender pour le cloud
| Corriger les alertes de sécurité à l'aide de Microsoft Defender for Cloud

Créer des requêtes pour Microsoft Sentinel à l'aide du langage de requête Kusto (KQL)
| Construire des instructions KQL pour Microsoft 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 Microsoft Sentinel à l'aide du langage de requête Kusto

Configurer votre environnement Microsoft Sentinel
| Présentation de Microsoft Sentinel
| Créer et gérer des espaces de travail Microsoft Sentinel
| Interroger les journaux dans Microsoft Sentinel
| Utiliser des listes de surveillance dans Microsoft Sentinel
| Utiliser les renseignements sur les menaces dans Microsoft Sentinel

Connecter les journaux à Microsoft Sentinel
| Connecter des données à Microsoft Sentinel à l'aide de connecteurs de données
| Connecter les services Microsoft à Microsoft Sentinel
| Connecter Microsoft 365 Defender à Microsoft Sentinel
| Connecter des hôtes Windows à Microsoft Sentinel
| Connecter les journaux Common Event Format à Microsoft Sentinel
| Connecter des sources de données syslog à Microsoft Sentinel
| Connecter des indicateurs de menace à Microsoft Sentinel

Créer des détections et effectuer des investigations à l'aide de Microsoft Sentinel
| Détection des menaces avec Microsoft Sentinel Analytics
| Automatisation dans Microsoft Sentinel
| Réponse aux menaces avec les playbooks Microsoft Sentinel
| Gestion des incidents de sécurité dans Microsoft Sentinel
| Identifier les menaces avec l'analyse du comportement des entités dans Microsoft Sentinel
| Normalisation des données dans Microsoft Sentinel
| Interroger, visualiser et surveiller les données dans Microsoft Sentinel

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Gérer le contenu dans Microsoft Sentinel

Effectuer une recherche de menaces dans Microsoft Sentinel
| Expliquer les concepts de chasse aux menaces dans Microsoft Sentinel
| Chasse aux menaces avec Microsoft Sentinel
| Utiliser la recherche d'emplois dans Microsoft Sentinel
| Chasse aux menaces à l'aide de blocs-notes dans Microsoft Sentinel

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.