Gestion d'infrastructure et Supervision

Analyste des opérations de sécurité Microsoft

4 jours (28h00) | ★★★★½ 4,6/5 | MSSC200 | Certification Microsoft SC-200 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Expliquer comment Microsoft Defender for Endpoint peut résoudre les risques dans votre environnement
- Administrer un environnement Microsoft Defender for Endpoint
- Configurer les règles de réduction de la surface d'attaque sur les périphériques Windows
- Effectuer des actions sur un appareil à l'aide de Microsoft Defender for Endpoint
- Examiner les domaines et les adresses IP dans Microsoft Defender for Endpoint
- Analyser les comptes d'utilisateur dans Microsoft Defender for Endpoint
- Configurer les paramètres d'alerte dans Microsoft 365 Defender
- Effectuer des recherches dans Microsoft 365 Defender
- Gérer les incidents dans Microsoft 365 Defender
- Expliquer comment Microsoft Defender for Identity peut résoudre les risques dans votre environnement
- Examiner les alertes DLP dans Microsoft Defender pour les applications Cloud
- Expliquer les types d'actions que vous pouvez effectuer dans le cas d'une gestion des risques Insider
- Configurer l'approvisionnement 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'évènement, de la gravité, du domaine et d'autres données pertinentes à l'aide de KQL
- Extraire des données à partir de champs de chaînes non structurés à l'aide de KQL
- Gérer un espace de travail Microsoft Sentinel
- Utiliser KQL pour accéder à la watchlist dans Microsoft Azure Sentinel
- Gérer les indicateurs de menace dans Microsoft Azure Sentinel
- Expliquer les différences entre Common Event Format (CEF) et le connecteur Syslog dans Microsoft Sentinel
- Connecter les machines virtuelles Windows Azure à Microsoft Sentinel
- Configurer l'agent Log Analytics pour collecter les événements Sysmon
- Créer de nouvelles règles et requêtes analytiques à l'aide de l'assistant de règles d'analyse
- Concevoir un playbook pour automatiser une réponse à un incident
- Utiliser des requêtes pour chasser les menaces
- Observer les menaces dans le temps avec le stream en direct.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances fondamentales de Microsoft 365, des produits de sécurité, de conformité et d'identité Microsoft, ainsi que des concepts scripting. Avoir des connaissances intermédiaires de Windows ainsi que des services Azure, en particulier Azure SQL Database et Azure Storage. Etre familier avec des machines virtuelles Azure et des réseaux virtuels.

Public concerné

Analystes des opérations de sécurité Microsoft.

Partenaire / Éditeur

Microsoft Partner
Microsoft
Gold Datacenter
Silver Cloud Productivity
Silver Messaging
Silver Communications
Silver Collaboration and Content

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Atténuation des menaces avec Microsoft 365 Defender

- Introduction à la protection contre les menaces de Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Protéger vos identités avec Azure AD Identity Protection
- Corriger les risques avec Microsoft Defender pour Microsoft 365
- Protéger votre environnement avec Microsoft Defender for Identity
- Sécuriser vos applications et services en Cloud avec Microsoft Defender pour les applications Cloud
- Répondre aux alertes de prévention des pertes de données avec Microsoft 365
- Gérer les risques liés aux initiés dans Microsoft 365

Atténuation des menaces avec Microsoft Defender for Endpoint

- Protéger contre les menaces avec Microsoft Defender for Endpoint
- Déployer l'environnement Microsoft Defender for Endpoint
- Implémenter les améliorations de la sécurité de Windows avec Microsoft Defender for Endpoint
- Effectuer des investigations sur les périphériques dans Microsoft Defender for Endpoint
- Réaliser des actions sur un dispositif à l'aide de Microsoft Defender for Endpoint
- Effectuer des enquêtes sur les preuves et les entités à l'aide de Microsoft Defender for Endpoint
- Configurer et gérer l'automatisation à l'aide de Microsoft Defender for Endpoint
- Configurer les alertes et les détections dans Microsoft Defender for Endpoint
- Utiliser la gestion des vulnérabilités dans Microsoft Defender for Endpoint

Atténuation des menaces avec Microsoft Defender pour le Cloud

- Planifier la protection des charges de travail dans le Cloud à l'aide de Microsoft Defender pour le Cloud
- Connecter les ressources Azure à Microsoft Defender pour le Cloud
- Connecter les ressources non-Azure à Microsoft Defender pour le Cloud
- Gérer votre posture de sécurité dans le Cloud
- Expliquer les protections des charges de travail du Cloud dans Microsoft Defender pour le Cloud
- Corriger les alertes de sécurité à l'aide de Microsoft Defender pour le Cloud

Création de requêtes pour Microsoft Sentinel avec KQL (Langage Kusto Query)

- Construire des instructions KQL pour Microsoft Sentinel
- Analyser les résultats d'une requête à l'aide de KQL
- Construire des requêtes multi-tables avec KQL
- Travailler avec des données dans Microsoft Sentinel en utilisant Kusto Query Language

Configuration de votre environnement Microsoft Sentinel

- Présentation de Microsoft Sentinel
- Créer et gérer des espaces de travail Microsoft Sentinel
- Journaux de requêtes dans Microsoft Sentinel
- Utiliser des watchlists dans Microsoft Sentinel
- Utiliser les renseignements sur les menaces dans Microsoft Sentinel

Connexion de journaux à Microsoft Sentinel

- Connecter

- Des données à Microsoft Sentinel à l'aide de connecteurs de données
- Des services Microsoft à Microsoft Sentinel
- Microsoft 365 Defender à Microsoft Sentinel
- Des hôtes Windows à Microsoft Sentinel
- Des journaux Common Event Format à Microsoft Sentinel
- Des sources de données Syslog à Microsoft Sentinel
- Des indicateurs de menace à Microsoft Sentinel

Création de détections et investigations avec Microsoft Sentinel

- Détection des menaces avec Analytique Microsoft Sentinel
- Automatisation dans Microsoft Sentinel
- Réponse aux menaces avec les playbooks Microsoft Sentinel
- Gestion des incidents de sécurité dans Microsoft Sentinel
- Identification des menaces grâce à l'analyse du comportement des entités dans Microsoft Sentinel
- Normalisation des données dans Microsoft Sentinel
- Interroger, visualiser et surveiller les données dans Microsoft Sentinel
- Gestion du contenu dans Microsoft Sentinel

Repérage des menaces dans Microsoft Sentinel

- Expliquer les concepts de chasse des menaces dans Microsoft Sentinel
- Repérage des menaces avec Microsoft Sentinel
- Utiliser des travaux de recherche dans Microsoft Sentinel
- Repérer les menaces à l'aide de notebooks dans Microsoft Sentinel

Certification (en option)

- Prévoir l'achat d'un voucher en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectuera en ligne

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation et/ou une certification éditeur (proposée en option)

Les + de la formation

Un lien URL sera fourni aux stagiaires lors de la formation, afin de récupérer le support.

Le support de cours et les Microsoft Labs Online sont en anglais.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.