Défendre contre les cybermenaces avec la plate-forme d'opérations de sécurité de Microsoft (SC-200T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

L’analyste des opérations de sécurité Microsoft collabore avec les parties prenantes organisationnelles pour sécuriser les systèmes informatiques de l’organisation. Son objectif est de réduire les risques organisationnels en remédiant rapidement aux 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 des menaces, la surveillance et la réponse en utilisant diverses solutions de sécurité dans leur environnement. Le rôle consiste principalement à enquêter, répondre et chasser les menaces à l’aide de Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Cloud et des produits de sécurité tiers. Comme l’analyste des opérations de sécurité consomme les résultats opérationnels de ces outils, il est également un intervenant clé dans la configuration et le déploiement de ces technologies.

Objectifs de la formation

À la fin de ce cours, les participants seront en mesure de/:

- Enquêter, analyser et répondre aux cybermenaces à l’aide de Microsoft Sentinel, Microsoft Defender XDR et Microsoft Defender for Cloud.
- Détecter et atténuer les incidents de sécurité touchant les identités, les points de terminaison, les applications infonuagiques et les services Microsoft 365.
- Renforcer la protection des identités avec Entra ID Protection et Microsoft Defender for Identity.
- Corriger les risques et protéger les données avec Microsoft Defender for Office 365 et les solutions Microsoft Purview.
- Créer et interpréter des requêtes Kusto Query Language (KQL) pour détecter, analyser et produire des rapports sur les événements de sécurité.

- Configurer et gérer les espaces de travail Microsoft Sentinel, les listes de surveillance, le renseignement sur les menaces et les intégrations avec Defender XDR.
- Connecter et ingérer des journaux provenant des services Microsoft, des hôtes Windows, des sources CEF, des systèmes syslog et des indicateurs de menace.
- Créer des règles d'analyse, automatiser les réponses et gérer les incidents de sécurité dans Microsoft Sentinel.
- Effectuer une chasse proactive aux menaces à l'aide des travaux de recherche, des notebooks et de l'analyse comportementale.
- Déployer, configurer et gérer Microsoft Defender for Endpoint, incluant les enquêtes, l'automatisation, les alertes et la gestion des vulnérabilités.

Description sommaire

Apprenez à enquêter, répondre et chasser les menaces à l'aide de Microsoft Sentinel, Microsoft Defender XDR et Microsoft Defender for Cloud. Dans ce cours, vous apprendrez à atténuer les cybermenaces en utilisant ces technologies. Plus précisément, vous configurerez et utiliserez Microsoft Sentinel ainsi que le langage Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la production de rapports. Le cours est conçu pour les personnes travaillant dans un rôle d'analyste des opérations de sécurité et aide les apprenants à se préparer à l'examen du SC 200.

Contenu du plan de cours

Parcours d'apprentissage 1 : Atténuer les menaces avec Microsoft Defender XDR

- Module 1 : Introduction à la protection contre les menaces Microsoft 365
- Module 2 : Atténuer les incidents avec Microsoft Defender XDR
- Module 3 : Protéger vos identités avec Entra ID Protection
- Module 4 : Corriger les risques avec Microsoft Defender pour Office 365
- Module 5 : Protéger votre environnement avec Microsoft Defender for Identity
- Module 6 : Sécuriser vos applications et services infonuagiques avec Microsoft Defender for Cloud Apps

Parcours d’apprentissage 2 : Commencer avec Microsoft Copilot for Security

- Module 1 : Fondements de l’IA générative
- Module 2 : Décrire Microsoft Copilot for Security
- Module 3 : Décrire les fonctionnalités principales de Microsoft Copilot for Security
- Module 4 : Décrire les expériences intégrées de Microsoft Copilot for Security

Parcours d’apprentissage 3 : Atténuer les menaces avec Microsoft Purview

- Module 1 : Solutions de conformité Microsoft Purview
- Module 2 : Répondre aux alertes de prévention de perte de données avec Microsoft Purview
- Module 3 : Gérer les risques internes dans Microsoft Purview
- Module 4 : Enquêter sur les menaces avec la recherche de contenu dans Microsoft Purview
- Module 5 : Enquêter sur les menaces avec Microsoft Purview Audit

Parcours d’apprentissage 4 : Atténuer les menaces avec Microsoft Defender for Endpoint

- Module 1 : Protéger contre les menaces avec Microsoft Defender for Endpoint
- Module 2 : Déployer l’environnement Microsoft Defender for Endpoint
- Module 3 : Mettre en œuvre les améliorations de sécurité Windows avec Microsoft Defender for Endpoint
- Module 4 : Effectuer des enquêtes sur les appareils dans Microsoft Defender for Endpoint
- Module 5 : Effectuer des actions sur un appareil avec Microsoft Defender for Endpoint
- Module 6 : Effectuer des enquêtes sur les preuves et entités avec Microsoft Defender for Endpoint
- Module 7 : Configurer et gérer l’automatisation avec Microsoft Defender for Endpoint
- Module 8 : Configurer les alertes et détections dans Microsoft Defender for Endpoint
- Module 9 : Utiliser la gestion des vulnérabilités dans Microsoft Defender for Endpoint

Parcours d’apprentissage 5 : Créer des requêtes pour Microsoft Sentinel avec Kusto Query Language (KQL)

- Module 1 : Construire des requêtes KQL pour Microsoft Sentinel
- Module 2 : Analyser les résultats de requêtes avec KQL
- Module 3 : Construire des requêtes multi tables avec KQL
- Module 4 : Travailler avec les données dans Microsoft Sentinel à l’aide de KQL

Parcours d’apprentissage 6 : Configurer votre environnement Microsoft Sentinel

- Module 1 : Introduction à Microsoft Sentinel
- Module 2 : Créer et gérer les espaces de travail Microsoft Sentinel
- Module 3 : Interroger les journaux dans Microsoft Sentinel
- Module 4 : Utiliser les listes de surveillance dans Microsoft Sentinel
- Module 5 : Utiliser le renseignement sur les menaces dans Microsoft Sentinel
- Module 6 : Intégrer Microsoft Defender XDR avec Microsoft Sentinel

Parcours d’apprentissage 7 : Connecter les journaux à Microsoft Sentinel

- Module 1 : Connecter les données à Microsoft Sentinel à l’aide de connecteurs
- Module 2 : Connecter les services Microsoft à Microsoft Sentinel
- Module 3 : Connecter Microsoft Defender XDR à Microsoft Sentinel
- Module 4 : Connecter les hôtes Windows à Microsoft Sentinel
- Module 5 : Connecter les journaux Common Event Format à Microsoft Sentinel
- Module 6 : Connecter les sources de données syslog à Microsoft Sentinel
- Module 7 : Connecter les indicateurs de menace à Microsoft Sentinel

Parcours d’apprentissage 8 : Créer des détections et effectuer des enquêtes dans Microsoft Sentinel

- Module 1 : Détection des menaces avec les analyses Microsoft Sentinel

Module 2 : Automatisation dans Microsoft Sentinel

- Module 3 : Réponse aux menaces avec les playbooks Microsoft Sentinel
- Module 4 : Gestion des incidents de sécurité dans Microsoft Sentinel
- Module 5 : Identifier les menaces avec l'analyse comportementale des entités dans Microsoft Sentinel
- Module 6 : Normalisation des données dans Microsoft Sentinel
- Module 7 : Interroger, visualiser et surveiller les données dans Microsoft Sentinel
- Module 8 : Gérer le contenu dans Microsoft Sentinel

Parcours d'apprentissage 9 : Effectuer la chasse aux menaces dans Microsoft Sentinel

- Module 1 : Expliquer les concepts de chasse aux menaces dans Microsoft Sentinel
- Module 2 : Chasse aux menaces avec Microsoft Sentinel
- Module 3 : Utiliser les travaux de recherche dans Microsoft Sentinel
- Module 4 : Chasser les menaces à l'aide des notebooks dans Microsoft Sentinel

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés. Les participants configurent progressivement et exploitent les opérations de sécurité en tant qu'analyste SOC avec Microsoft Sentinel à travers des exercices inspirés de scénarios réels, favorisant une application immédiate des apprentissages.

Ils apprennent à détecter, analyser et répondre aux incidents de sécurité à l'aide des outils de protection et de surveillance Microsoft.

Animée par un formateur certifié Microsoft (MCT), la formation met l'accent sur l'interactivité et le développement de compétences techniques directement transférables pour assurer la surveillance et la réponse aux menaces en contexte professionnel.

Prérequis

Les participants doivent posséder les connaissances et l'expérience suivantes avant de suivre ce cours :

- Compréhension de base de Microsoft 365
- Compréhension fondamentale des produits Microsoft de sécurité, conformité et identité
- Compréhension intermédiaire de Microsoft Windows
- Familiarité avec les services Azure, notamment Azure SQL Database et Azure Storage
- Familiarité avec les machines virtuelles Azure et le réseau virtuel
- Compréhension de base des concepts de script

Recommandations

Prérequis facultatifs :

- Compréhension générale des concepts de sécurité et de gestion des menaces
- Familiarité avec les outils de sécurité Microsoft (Sentinel, Defender XDR, Defender for Cloud)
- Connaissance de base du langage Kusto Query Language (KQL)
- Notions de gouvernance et de conformité des données

  Expérience préalable en opérations de sécurité (SOC)
- Compréhension des risques organisationnels et des pratiques de remédiation
- Familiarité avec les environnements Microsoft 365 et Azure

Certifications

Microsoft certifié : Analyste des opérations de sécurité associé

Notes légales