+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 03/06/2024

S'inscrire

Formation Préparation à la Certification SC-200

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

3 jours (21 heures)

Présentation

Microsoft Security Operations Analyst connu sous le nom SC-200 est une certification qui valide vos compétences dans la gestion des incidents de sécurité et la résolution des menaces en utilisant les solutions de sécurité fournis par Microsoft.

Nous aborderons plusieurs thématiques telles que l'analyse des menaces, répondre aux incidents et protéger les environnements de l'entreprise. Vos compétences seront mises à l'épreuve afin de traiter et de résoudre tous les incidents de sécurité.

Durant ce cours, vous utiliserez des outils et des technologies de Microsoft mis à votre disposition comme Microsoft Sentinel pour la gestion des informations et des événements de sécurité (SIEM), Microsoft Defender, pour la protection contre les menaces (ATP).

En obtenant la certification SC-200, cela renforcera votre crédibilité en tant que professionnel de la sécurité et d'améliorer vos opportunités de carrière dans le domaine de la cybersécurité.

Comme pour toutes nos formations, celle-ci vous présentera les toutes dernières nouveautés concernant Microsoft.

Objectifs

- Atténuer les menaces avec Microsoft Defender pour le Cloud
- Configurer l'environnement de votre entreprise avec Microsoft Sentinel
- Créer des détections et effectuer des investigations
- Découvrir et analyser les menaces sur l'environnement Microsoft 365

Public visé

- Professionnels de la sécurité
- Analystes SOC
- Administrateurs systèmes

Pré-requis

- Familiarité avec Microsoft 365 et Azure
- Expérience en sécurité informatique
- Compétences en administration système

PROGRAMME DE NOTRE FORMATION SC-200

Découverte des menaces sur l'environnement Microsoft 365

- Enquêter, répondre et remédier aux menaces qui pèsent sur Microsoft Teams, SharePoint Online et OneDrive
- Examiner les alertes générées par les politiques de prévention des pertes de données (DLP) et y répondre
- Découvrir et gérer les applications à l'aide de Microsoft Defender for Cloud Apps
- Identifier, étudier et remédier aux risques de sécurité à l'aide de Defender for Cloud Apps
- Importance de LINQ dans les projets modernes .NET

Réduire les risques des points d'extremité avec Defender for Endpoint

- Gérer la rétention des données, les notifications d'alerte et les fonctionnalités avancées
- Recommander la réduction de la surface d'attaque (ASR) pour les appareils
- Répondre aux incidents et aux alertes
- Configurer et gérer les groupes d'appareils
- Identifier les dispositifs à risque en utilisant Microsoft Defender Vulnerability Management
- Gérer les indicateurs de menace des terminaux
- Identifier les appareils non gérés en utilisant la découverte des appareils

Protéger vos identités

- Découverte des fonctionnalités de Microsoft Entra
- Atténuer les risques de sécurité liés aux événements de protection d'identité Azure AD
- Diminuer les risques de sécurité en utilisant Microsoft Defender pour Identity

Gérer la détection et les réponses étendues (XDR)

- Gestion des actions et des soumissions dans le portail Microsoft 365 Defender
- Identifier les menaces en utilisant KQL
- Identifier et remédier aux risques de sécurité en utilisant Microsoft Secure Score

- Analyser les analyses de menace dans le portail Microsoft 365 Defender
- Configurer et gérer les détections et les alertes personnalisées

Mettre en œuvre et maintenir la gestion de la posture de sécurité cloud

- Attribuer et gérer les politiques de conformité réglementaire avec le benchmark de sécurité cloud Microsoft (MCSB)
- Améliorer le score de sécurité de Defender
- Configurer les plans et les agents pour Microsoft Defender pour Servers
- Configurer et gérer Microsoft Defender pour DevOps

Configurer les paramètres d'environnement dans Defender pour le Cloud

- Configurer les rôles de Defender
- Évaluer et recommander la protection des charges de travail cloud
- Activer les plans Microsoft Defender
- Configurer l'intégration automatique pour les ressources Azure
- Connecter les ressources de calcul en utilisant Azure Arc
- Connecter les ressources multicloud en utilisant les paramètres d'environnement

Répondre aux alertes et incidents dans Defender pour Cloud

- Configurer les notifications par e-mail
- Création et gestion des règles de suppression d'alertes
- Conception et configuration de l'automatisation des workflows dans Defender
- Remédier aux alertes et incidents en utilisant les recommandations de Defender
- Gérer les alertes et incidents de sécurité
- Analyser les rapports de renseignement sur les menaces de Defender pour Cloud

Concevoir et configurer un espace de travail Microsoft Sentinel

- Planifier un espace de travail Microsoft Sentinel
- Configurer les rôles de Microsoft Sentinel
- Concevoir et configurer le stockage des données de Microsoft Sentinel

Gérer les menaces en utilisant l'analyse comportementale des entités

- Configurer les paramètres de comportement des entités
- Enquêter sur les menaces en utilisant les pages d'entités
- Configurer les règles analytiques de détection des anomalies

Concevoir et configurer un espace de travail Microsoft Sentinel

- Planifier un espace de travail Microsoft Sentinel

- Configurer les rôles de Microsoft Sentinel
- Concevoir et configurer le stockage des données de Microsoft Sentinel

Gérer les menaces en utilisant l'analyse comportementale des entités

- Configurer les paramètres de comportement des entités
- Enquêter sur les menaces en utilisant les pages d'entités
- Configurer les règles analytiques de détection des anomalies

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.