Security Operations Analyst Associate Microsoft

RS :

L'analyste des opérations de sécurité Microsoft collabore avec les parties prenantes de l'organisation pour sécuriser les systèmes de technologie de l'information pour l'organisation.

L'objectif de l'analyste des opérations de sécurité est de réduire les risques organisationnels en corrigeant rapidement les attaques actives dans l'environnement, en conseillant sur l'amélioration des pratiques de protection contre les menaces et en renvoyant les violations des politiques organisationnelles aux parties prenantes appropriées.

Programme

Atténuer les menaces à l'aide de Microsoft 365 Defender

Détecter, étudier, répondre et corriger les menaces pesant sur l'environnement de productivité à l'aide de Microsoft Defender pour Office 365

- Détecter, enquêter, répondre et corriger les menaces pesant sur Microsoft Teams, SharePoint et OneDrive
- Détecter, enquêter, répondre, corriger les menaces pesant sur la messagerie électronique à l'aide de Defender pour Office 365
- Gérer les alertes de stratégie de prévention de la perte de données
- Évaluer et recommander des étiquettes de sensibilité
- Évaluer et recommander des politiques de risque d'initié

Détecter, étudier, répondre et corriger les menaces de point de terminaison à l'aide de Microsoft Defender pour Endpoint

- Gérer la conservation des données, la notification des alertes et les fonctionnalités avancées
- Configurer les règles de réduction de la surface d'attaque des périphériques
- Configurer et gérer des détections et des alertes personnalisées
- Répondre aux incidents et aux alertes
- Gérer les enquêtes et les mesures correctives automatisées
- Évaluer et recommander des configurations de point de terminaison pour réduire et corriger les vulnérabilités à l'aide de la solution de gestion des menaces et des vulnérabilités de Microsoft.
- Gérer les indicateurs de menace Microsoft Defender for Endpoint
- Analyser l'analyse des menaces Microsoft Defender for Endpoint

Détectez, enquêtez, répondez et corrigez les menaces d'identité

- Identifier et corriger les risques de sécurité liés aux stratégies de risque de connexion
- Identifier et corriger les risques de sécurité liés aux événements d'accès conditionnel
- Identifier et corriger les risques de sécurité liés à Azure Active Directory
- Identifier et corriger les risques de sécurité à l'aide de Secure Score
- Identifier, enquêter et corriger les risques de sécurité liés aux identités privilégiées
- Configurer des alertes de détection dans Azure AD Identity Protection
- Identifier et corriger les risques de sécurité liés aux services de domaine Active Directory à l'aide de Microsoft Defender for Identity

Microsoft

Microsoft CERTIFIED
SECURITY OPERATIONS ANALYST
ASSOCIATE

LE PUBLIC VISÉ :
- Analyste des opérations de sécurité

DURÉE :
- 4 jours soit en total 28 heures

NIVEAU :
- Intermédiaire

TARIF :
- 2900€/personne

ELIGIBLE CPF :
- NON

Détecter, enquêter, répondre et corriger les menaces applicatives

- Identifier, étudier et corriger les risques de sécurité à l'aide de Microsoft Cloud Application Security (MCAS)
- Configurer mcAS pour générer des alertes et des rapports pour détecter les menaces

Gérer les enquêtes inter-domaines dans le portail Microsoft 365 Defender

- Gérer les incidents sur les produits Microsoft 365 Defender
- Gérer les actions en attente d'approbation entre les produits
- Effectuer une chasse avancée aux menaces

• Atténuer les menaces à l'aide d'Azure Microsoft Defender pour le cloud

Concevoir et configurer une implémentation Defender Microsoft Defender pour le cloud

- Planifier et configurer les paramètres Microsoft Defender pour Cloud, y compris la sélection des abonnements cibles et de l'espace de travail
- Configurer Microsoft Defender pour les rôles Cloud
- Configurer des stratégies de rétention des données
- Évaluer et recommander la protection des charges de travail dans le cloud

Planifier et implémenter l'utilisation de connecteurs de données pour l'ingestion de sources de données dans Microsoft Defender pour le cloud

- Identifier les sources de données à ingérer pour Microsoft Defender pour le cloud
- Configurer l'intégration automatisée pour les ressources Azure
- Connecter des ordinateurs locaux
- Connecter les ressources cloud AWS
- Connecter les ressources cloud GCP
- Configurer la collecte de données

Gérer les règles d'alerte Microsoft Defender pour Cloud

- Valider la configuration des alertes
- Configurer les notifications par e-mail
- Créer et gérer des règles de suppression d'alerte

Configurer l'automatisation et la correction

- Configurer des réponses automatisées dans Center Microsoft Defender pour le cloud
- Concevoir et configurer l'automatisation du flux de travail du Center Microsoft Defender pour le cloud
- Corriger les incidents à l'aide de Center Conseils Microsoft Defender pour le cloud
- Créer une réponse automatique à l'aide d'un modèle Azure Resource Manager

Enquêter sur les alertes et les incidents Microsoft Defender pour le cloud

- Décrire les types d'alerte pour les charges de travail Azure
- Gérer les alertes de sécurité
- Gérer les incidents de sécurité
- analyzer Center Microsoft Defender for Cloud threat intelligence
- Répondre aux alertes Microsoft Defender Cloud for Key Vault
- Gérer les données utilisateurs découverts au cours d'une enquête

Atténuer les menaces à l'aide de Microsoft Sentinel

Concevoir et configurer un espace Microsoft Sentinel

- Planifier Microsoft Sentinel workspace
- Configurer les rôles Microsoft Sentinel
- Concevoir le stockage de données Azure Microsoft Sentinel
- Configurer les paramètres de sécurité et l'accès pour Azure Microsoft Sentinel

Administration Sécurité Microsoft 365 (MS 500)

Planifier et implémenter l'utilisation de connecteurs de données pour l'ingestion de sources de données dans Microsoft Sentinel

- Identifier les sources de données à ingérer pour Microsoft Sentinel
- Identifier les conditions préalables pour un connecteur de données
- Configurer et utiliser les connecteurs de données Microsoft Sentinel
- Configurer des connecteurs de données à l'aide d'Azure Policy
- Concevoir et configurer des collections d'événements Syslog et CEF
- Concevoir et configurer des collections d'événements de sécurité Windows
- Configurer des connecteurs de renseignements sur les menaces personnalisés
- Créer des journaux personnalisés dans Azure Log Analytics pour stocker des données personnalisées

Gérer les règles d'analyse Microsoft Sentinel

- Concevoir et configurer des règles d'analyse
- Créer des règles d'analyse personnalisées pour détecter les menaces
- Activer les règles d'analyse de sécurité Microsoft
- Configurer les requêtes planifiées fournies par le connecteur
- Configurer des requêtes planifiées personnalisées
- Définir la logique de création d'incident

Configurer Security Orchestration Automation and Réponse (SOAR) dans Microsoft Sentinel

- Créer des playbooks Microsoft Sentinel
- Configurer des règles et des incidents pour déclencher des playbooks
- Utiliser des playbooks pour remédier aux menaces
- Utiliser des playbooks pour gérer les incidents
- Utiliser des playbooks dans les solutions Microsoft Defender

Identifier sur les incidents Sentinel

- Enquêter sur les incidents dans Microsoft Sentinel
- Trier des incidents dans Microsoft Sentinel
- Répondre aux incidents dans Microsoft Sentinel
- Enquêter sur les incidents impliquant plusieurs espaces de travail
- Identifier les menaces avancées avec l'analyse du comportement des utilisateurs et des entités (UEBA)

Utiliser les classeurs Microsoft Sentinel pour analyser et interpréter les données

- Activer et personnaliser les modèles de classeur Microsoft Sentinel
- Créer des classeurs personnalisés
- Configurer les visualisations avancées
- Afficher et analyser des données Microsoft Sentinel à l'aide de classeurs
- Suivre les mesures d'incident à l'aide du classeur d'efficacité des opérations de sécurité

Rechercher les menaces à Microsoft Sentinel

- Créer des requêtes de hunting personnalisées
- Exécuter des requêtes de chasse manuellement
- Surveiller les requêtes de chasse à l'aide de Livestream
- Effectuer une chasse avancée avec des cahiers
- Suivre les résultats de la requête avec des signets
- Utiliser des signets de chasse pour les enquêtes sur les données
- Convertir une requête de chasse en requête analytique

Objectifs pédagogiques

L'objectif de l'analyste des opérations de sécurité est de réduire les risques organisationnels en corrigeant rapidement les attaques actives dans l'environnement, en conseillant sur l'amélioration des pratiques de protection contre les menaces et en renvoyant les violations des politiques organisationnelles aux parties prenantes appropriées.
Les responsabilités comprennent la gestion, la surveillance et la réponse aux menaces en utilisant une variété de solutions de sécurité dans leur environnement. Le rôle est d'étudier, répondre et traquer principalement les menaces à l'aide de Microsoft Sentinel, Defender Microsoft pour le cloud, Microsoft 365 Defender et de produits de sécurité tiers.
Étant donné que l'analyste des opérations de sécurité consomme la sortie opérationnelle de ces outils, il est également un acteur essentiel dans la configuration et le déploiement de ces technologies.

Administration Sécurité Microsoft 365 (MS 500)

Objectifs pédagogiques

A l'issu de l'examen le candidat sera en mesure de :

- Définir les fonctionnalités de Microsoft Defender for Sentinel Microsoft.
- Comprendre comment traquer les menaces au sein de votre réseau.
- Expliquez comment Microsoft Defender for Sentinel Microsoft peut réduire les risques dans votre environnement.
- Créer un environnement Microsoft Defender pour Sentinel Microsoft
- Appareils embarqués à surveiller par Microsoft Defender for Sentinel Microsoft
- Configurer les paramètres d'environnement Microsoft Defender for Sentinel Microsoft
- Enquêter sur les incidents dans Microsoft Defender for Sentinel Microsoft
- Enquêter sur les alertes dans Microsoft Defender for Sentinel Microsoft
- Effectuer une chasse avancée dans Microsoft Defender for Sentinel Microsoft
- Configurer les paramètres d'alerte dans Microsoft Defender for Sentinel Microsoft
- Construire des instructions KQL
- Gérer les indicateurs dans Microsoft Defender for Sentinel Microsoft
- Décrire la gestion des menaces et des vulnérabilités dans Microsoft Defender for Sentinel Microsoft
- Identifiez les vulnérabilités sur vos appareils avec Microsoft Defender for Sentinel Microsoft
- Suivre les menaces émergentes dans Microsoft Defender for Sentinel Microsoft

Méthode et modalités pédagogiques

Cette formation sera principalement constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.

Support :
un support de cours officiel Microsoft en français sera remis aux participants au format électronique via la plateforme

Evaluation :
les acquis sont évalués tout au long de la formation et en fin de formation par le formateur (questions régulières, travaux pratiques, QCM ou autres méthodes).

Formateur :
le tout animé par un consultant-formateur expérimenté, nourri d'une expérience terrain, et accrédité Microsoft Certified Trainer.

Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations. Les appréciations que vous avez formulées font l'objet d'un enregistrement et d'une analyse qualitative de la formation et du formateur. ITsystème formation dispose d'un processus qualité qui prend en considération les retours des participants afin d'être proactif quant à la solution corrective adaptée.
Nous veillons à ce que tous les objectifs de l'examen soient couverts en profondeur afin que vous soyez prêt pour toute question de l'examen. Nos tests pratiques sont rédigés par des experts de l'industrie en la matière. Ils travaillent en étroite collaboration avec les fournisseurs de certification pour comprendre les objectifs de l'examen, participer aux tests bêta et passer l'examen eux-mêmes avant de créer de nouveaux tests pratiques.

Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
Les simulations en ligne basées sur la performance offrent une expérience pratique de l'environnement de travail
Les questions sont similaires aux questions d'examen afin que vous testiez votre connaissance des objectifs de l'examen
Des explications détaillées pour les réponses correctes et distractrices renforcent le matériel
Le mode étude couvre tous les objectifs en veillant à ce que les sujets soient couverts
Le mode de certification (chronométré) prépare les étudiants aux conditions de passage des examens
Des rapports de score instantanés et approfondis vous indiquent exactement les domaines sur lesquels vous concentrer.
Cette formation peut être dispensée en mode présentiel comme en distanciel.
Elle prend en charge les compétences ci-dessous ; le pourcentage indique le poids relatif du module dans l'examen global. Plus vous vous concentrez sur des modules avec un pourcentage plus élevé, plus vous obtiendrez probablement plus de notes à l'examen.

Cet examen mesure votre capacité à accomplir les tâches techniques suivantes :

- Atténuer les menaces à l'aide de Microsoft 365 Defender (25-30 %)
- Atténuer les menaces à l'aide d'Azure Microsoft Defender pour le cloud (25 à 30 %)
- Atténuer les menaces à l'aide de Microsoft Sentinel (40-45 %)

Administration Sécurité Microsoft 365 (MS 500)

Pour qui ?

Participants aspirant à la certification SC 200
Tous ceux qui aspirent à travailler dans l'environnement SOC de l'ère moderne
Tout le monde veut apprendre la suite de services M365 defender

Pré-requis

- Compréhension de base de Microsoft 365
- Compréhension intermédiaire des appareils Windows 10
- Découvrir de nouveaux aspects de la sécurité du cloud via Microsoft Defender
- Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft
- Familiarité avec les services Azure, en particulier Azure SQL Database et Azure Storage
- Familiarité avec les machines virtuelles Azure et la mise en réseau virtuelle
- Connaissance fondamentale des réseaux informatiques
- Compréhension de base des concepts de script.

Accessibilité

Il est possible de vous inscrire jusqu'à 2 jours ouvrés avant le début de la formation, sous condition de places disponibles et de réception du devis signé.
Il est aussi possible – sur demande – d'adapter des moyens de la prestation pour les personnes en situation de handicap en fonction du type de handicap.
Le centre de formation ITsystem Formation est situé au :
Grand Paris au
21 rue jean Rostand
91898 ORSAY

Vous pouvez facilement y accéder par les transports en commun suivants :
RER B Le guichet BUS 11 et BUS 7
En voiture : prendre la N118, sortie 9 Centre universitaire Grandes écoles

Pré certification

Cette formation ouvre la voie à la **certification « SC-200 Analyste des opérations de sécurité Microsoft »**