

Security Administrator Associate Microsoft 365

RS : 5443

Les Administrateurs de la sécurité Microsoft 365 sont chargés de sécuriser de manière proactive les environnements d'entreprise et hybrides Microsoft 365, de mettre en œuvre et de gérer les solutions de sécurité et de conformité, de répondre aux menaces et de faire appliquer la gouvernance des données.

Les candidats à cet examen sont familiers avec les charges de travail M365 et possèdent de solides compétences et expériences en matière de protection des identités, de protection des informations, de protection contre les menaces, de gestion de la sécurité et de gouvernance des données. Ce rôle se concentre sur l'environnement M365 et inclut les environnements hybrides.

Microsoft



Programme

Mettre en œuvre et gérer l'identité et l'accès

Sécuriser les environnements hybrides Microsoft 365

- Planifier les options d'authentification Azure AD
- Planifier les options de synchronisation Azure AD
- Surveiller et dépanner les événements Azure AD Connect

Identités sécurisées

- Implémenter l'appartenance à un groupe Azure AD
- Mettre en œuvre la gestion des mots de passe
- Gérer les identités externes dans les charges de travail Azure AD et Microsoft 365

Implémenter des méthodes d'authentification

- Implémenter l'authentification multi facteur (MFA) à l'aide de la stratégie d'accès conditionnel
- Gérer et surveiller l'authentification multifacteur
- Planifier et implémenter des méthodes d'authentification des appareils telles que Windows Hello

Implémenter l'accès conditionnel

- Planifier les stratégies de conformité et d'accès conditionnel
- Configurer et gérer la conformité des appareils pour les stratégies de sécurité des terminaux
- Mettre en œuvre et gérer l'accès conditionnel
- Tester et dépanner les stratégies d'accès conditionnel

Implémenter des rôles et des groupes de rôles

- Planifier les rôles et les groupes de rôles
- Configurer des rôles et des groupes de rôles
- Rôles d'audit pour l'accès le moins privilégié

Configurer et gérer la gouvernance des identités

- Implémenter Azure AD Privileged Identity Management implémenter et gérer la gestion des droits implémenter et gérer les révisions d'accès

LE PUBLIC VISÉ :

- Administrateur

DURÉE :

- 4 jours soit en total 28 heures

NIVEAU :

- Intermédiaire

TARIF :

- 2900€/personne

ELIGIBLE CPF :

- OUI Sous le N° RS5443

Implémenter Azure AD Identity Protection

- Mettre en œuvre une politique de risque pour les utilisateurs
- Implémenter une stratégie de risque de connexion
- Configurer les alertes de protection d'identité
- Examiner les événements à risque et y réagir

Mettre en œuvre et gérer la protection contre les menaces

- Implémenter et gérer Microsoft Defender for Identity
- Planifier une solution Microsoft Defender for Identity
- installer et configurer Microsoft Defender for Identity
- Surveiller et gérer Microsoft Defender for Identity

Mettre en œuvre la protection contre les menaces des appareils

- planifier une solution Microsoft Defender for Endpoint
- Implémenter Microsoft Defender pour Endpoint
- Gérer et surveiller Microsoft Defender for Endpoint

Mettre en œuvre et gérer la protection des appareils et des applications

- Planifier la protection des appareils et des applications
- Configurer et gérer Microsoft Defender Application Guard
- Configurer et gérer le contrôle d'application Microsoft Defender
- Configurer et gérer la protection contre les exploits
- Configurer et gérer le chiffrement des appareils Windows
- Configurer et gérer le chiffrement des appareils non Windows
- Mettre en œuvre des stratégies de protection des applications
- Configurer et gérer la conformité des appareils pour la sécurité des terminaux

Implémenter et gérer Microsoft Defender pour Office 365

- Configurer Microsoft Defender pour Office 365
- Surveiller et corriger les menaces à l'aide de Microsoft Defender pour Office 365
- Mener des attaques simulées à l'aide d'Attack Simulator

Surveiller la sécurité Microsoft 365 avec Azure Sentinel

- Planifier et implémenter Azure Sentinel
- Configurer des playbooks dans Azure Sentinel
- Gérer et surveiller avec Azure Sentinel
- Répondre aux menaces à l'aide de playbooks intégrés dans Azure Sentinel

Implémenter et gérer Microsoft Cloud App Security

- Planifier la mise en œuvre de Cloud App Security
- Configurer Microsoft Cloud App Security
- Gérer la découverte d'applications cloud
- Gérer les entrées dans le catalogue d'applications Cloud
- Gérer les applications dans Cloud App Security
- Configurer les connecteurs Cloud App Security et les applications OAuth
- Configurer les stratégies et les modèles Cloud App Security
- Examiner, interpréter et répondre aux alertes, rapports, tableaux de bord et journaux Cloud App Security

Mettre en œuvre et gérer la protection des informations

Gérer les informations sensibles

- Planifier une solution d'étiquette de sensibilité
- Créer et gérer des types d'informations sensibles • configurer des étiquettes et des stratégies de sensibilité.
- Configurer et utiliser l'Explorateur d'activités
- Utiliser des étiquettes de sensibilité avec les applications Teams, SharePoint, OneDrive et Office

Gérer la protection contre la perte de données (DLP)

- Planifier une solution DLP
- Créer et gérer des stratégies DLP pour les charges de travail Microsoft 365
- Créer et gérer des types d'informations sensibles
- Surveiller les rapports DLP
- Gérer les notifications DLP
- Implémenter Endpoint DLP

Gérer la gouvernance et la conservation des données

- Planifier la gouvernance et la conservation des données
- Examiner et interpréter les rapports et les tableaux de bord sur la gouvernance des données
- Configurer des étiquettes et des stratégies de rétention
- Définir et gérer des stratégies de conformité des communications
- Configurer la rétention dans les charges de travail Microsoft 365
- Rechercher et récupérer des données Office 365 supprimées
- Configurer et utiliser Microsoft 365 Records Management

Gérer les fonctionnalités de gouvernance et de conformité dans Microsoft 365

Configurer et analyser les rapports de sécurité

- Surveiller et gérer l'état de sécurité des appareils à l'aide de Microsoft Endpoint Manager Admin Center.
- Gérer et surveiller les rapports de sécurité et les tableaux de bord à l'aide du portail Microsoft 365 Defender
- Planifier des rapports de sécurité personnalisés avec l'API Graph Security
- Utiliser des tableaux de bord de score sécurisés pour examiner les actions et les recommandations

Gérer et analyser les journaux et rapports d'audit

- Plan d'audit et de production de rapports
- Effectuer une recherche dans le journal d'audit
- Examiner et interpréter les rapports de conformité et les tableaux de bord
- Configurer les stratégies d'alerte d'audit

Découvrir et répondre aux requêtes de conformité dans Microsoft 365

- Planifier la recherche de contenu et la découverte électronique
- Déléguer des autorisations pour utiliser les outils de recherche et de découverte
- Utiliser des outils de recherche et d'enquête pour découvrir et répondre
- Gérer les cas de découverte électronique

Gérer la conformité réglementaire

- Planifier la conformité réglementaire dans Microsoft 365
- Gérer les demandes des personnes concernées (DSR)
- Administrer compliance Manager dans microsoft 365 compliance center
- Utiliser compliance manager

Gérer les solutions de gestion des risques internes dans Microsoft 365

- Mettre en œuvre et gérer Customer Lockbox
- Mettre en œuvre et gérer des politiques de conformité des communications
- Mettre en œuvre et gérer des politiques de gestion des risques d'initiés
- Mettre en œuvre et gérer les politiques relatives aux obstacles à l'information
- Mettre en œuvre et gérer la gestion des accès privilégiés

Objectifs pédagogiques

Les candidats à cet examen mettent en œuvre, gèrent et surveillent les solutions de sécurité et de conformité pour Microsoft 365 et les environnements hybrides. Les Administrateurs de la sécurité Microsoft 365 sont chargés de sécuriser de manière proactive les environnements d'entreprise Microsoft 365, de répondre aux menaces, de mener des enquêtes et de faire appliquer la gouvernance des données. Ils collaborent avec les Administrateurs d'entreprise Microsoft 365, les parties prenantes de l'entreprise et d'autres administrateurs de charges de travail pour planifier et mettre en œuvre des stratégies de sécurité et veiller à la conformité des solutions aux stratégies et réglementations de l'organisation.

A l'issu de cette formation les candidats seront en mesure de :

- Gérer l'identité et l'accès Microsoft 365
- Mettre en œuvre de la protection contre les menaces Microsoft 365
- Mettre en œuvre de la protection des informations Microsoft 365
- Administrer la conformité Microsoft 365 intégrée.

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 distrayantes 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 :

- Mettre en œuvre et gérer les identités et les accès (35 à 40%)
- Mettre en œuvre et gérer la protection contre les menaces (25 à 30%)
- Mettre en œuvre et gérer la protection des informations (10 à 15%)
- Gérer les options de gouvernance et de conformité dans Microsoft 365 (20 à 25%)

Pour qui ?

Les candidats à cet examen sont familiers avec les charges de travail M365 et possèdent de solides compétences et expériences en matière de protection des identités, de protection des informations, de protection contre les menaces, de gestion de la sécurité et de gouvernance des données. Ce rôle se concentre sur l'environnement M365 et inclut les environnements hybrides.

Pré-requis

Les candidats à cet examen sont familiarisés aux charges de travail de Microsoft 365 et possèdent des compétences solides et de l'expérience dans la protection de l'identité, la protection des informations, la protection contre les menaces, la gestion de la sécurité et la gouvernance des données. Ce rôle se concentre sur l'environnement Microsoft 365 et comprend des environnements hybrides.

Administration Sécurité Microsoft 365 (MS 500)

Pré certification

Cette formation ouvre la voie à la certification « Microsoft « MS 500 Administration Sécurité Microsoft 365 »