Microsoft 365 Security Administration (Microsoft MS-500)

Cours officiel MS-500T00, préparation à l'examen

Cours Pratique de 4 jours
Réf : SYO - Prix 2023 : 2 690€ HT

Avec cette formation, vous apprendrez à mettre en œuvre, à gérer et à surveiller des solutions de sécurité et de conformité pour Microsoft 365. Vous aborderez aussi la protection des mots de passe des utilisateurs, l'activation de Azure Identity Protection, la configuration et l'utilisation d'Azure AD Connect, l'accès conditionnel dans Microsoft 365, etc.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Administrer l'accès utilisateur et de groupe dans Microsoft 365

Expliquer et gérer Azure Identity Protection

Planifier et mettre en œuvre Azure AD Connect

Gérer les identités synchronisées des utilisateurs

Expliquer et utiliser l'accès conditionnel

Décrire les vecteurs de menace des cyberattaques

Expliquer les solutions de sécurité pour Microsoft 365

Utiliser Microsoft Secure Score pour évaluer et améliorer sa posture de sécurité

Configurer les services de protection avancée contre les diverses menaces pour Microsoft 365

Planifier et déployer des appareils mobiles sécurisés

Planifier et déployer des périphériques mobiles sécurisés

Mettre en œuvre la gestion des droits à l'information

Sécuriser les messages sur Microsoft 365

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel Microsoft (digital MOC) en anglais.

CERTIFICATION

La réussite de l'examen permet d'obtenir la certification "Microsoft 365 Certified: Security Administrator Associate".

PARTICIPANTS

Administrateur sécurité.

PRÉREQUIS

Expérience de Windows 10 et Microsoft 365. Connaissances de base de Microsoft Azure. Connaissance pratique de la gestion des appareils mobiles.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 11/2021

1) Gestion des utilisateurs et des groupes

- Concepts de gestion des identités et des accès.
- Le modèle de confiance zéro.
- Planifier sa solution d'identité et d'authentification.
- Comptes et rôles des utilisateurs.

- Gestion des mots de passe.

Travaux pratiques : Créer son locataire Microsoft 365 et gérer les utilisateurs et les groupes. Configurer la réinitialisation du mot de passe en libre-service (SSPR) pour les comptes d'utilisateurs dans Azure AD. Déployer Azure AD Smart Lockout.

2) Synchronisation et protection de l'identité

- Planifier la synchronisation des répertoires.
- Configurer et gérer les identités synchronisées.
- Azure AD Identity Protection.

Travaux pratiques : Mise en œuvre de la synchronisation des identités.

3) Gestion des identités et des accès

- Gestion des demandes.
- Gouvernance de l'identité.
- Gestion de l'accès aux périphériques.
- Contrôle d'accès en fonction du rôle (RBAC).
- Solutions pour l'accès externe.
- Gestion des identités privilégiées.

Travaux pratiques : Utiliser l'accès conditionnel pour activer l'authentification multi-facteurs (MFA). Configurer la gestion des identités privilégiées.

4) La sécurité dans Microsoft 365

- Vecteurs de menaces et violations des données.
- Stratégie et principes de sécurité.
- Solutions de sécurité de Microsoft.
- Microsoft Secure Score.

Travaux pratiques : Utiliser Microsoft Secure Score : améliorer sa notation de sécurité dans le centre de sécurité Microsoft 365.

5) Protection avancée contre les menaces

- Exchange Online Protection (EOP).
- Microsoft Defender pour Office 365.
- Gestion des pièces jointes sécurisées.
- Gestion des liens sécurisés.
- Microsoft Defender pour Identity.
- Microsoft Defender pour Endpoint.

Travaux pratiques : Gérer Microsoft 365 Security Services : implémenter les politiques de Microsoft Defender.

6) Gestion des menaces

- Utiliser le tableau de bord de sécurité.
- Enquête sur les menaces et réponse.
- Utiliser Azure Sentinel pour Microsoft 365.
- Configuration d'Advanced Threat Analytics.

Travaux pratiques : Utiliser le simulateur d'attaques : simuler une attaque de spear phishing, simuler des attaques sur les mots de passe.

7) Microsoft Cloud Application Security

- Déployer Cloud Application Security.
- Utiliser les informations de Cloud Application Security.

Travaux pratiques : Configurer Azure AD pour Intune : permettre la gestion des dispositifs. Configurer Azure AD pour Intune et créer des politiques Intune.

8) Mobilité

- Mobile Application Management (MAM).
- Mobile Device Management (MDM).
- Déployer les services des appareils mobiles.

- Enregistrer les appareils sur Mobile Device Management.
Travaux pratiques : Gestion des appareils : mettre en œuvre la protection des informations Azure et Windows et créer des politiques de conformité et d'accès conditionnel.

9) Protection de l'information et gouvernance
- Concepts de protection des informations.
- Gouvernance et gestion des documents.
- Labels de sensibilité.
- Archivage dans Microsoft 365.
- Conservation dans Microsoft 365.
- Politiques de conservation dans le centre de conformité Microsoft 365.
- Archivage et conservation dans Exchange.
- Gestion des documents en place dans SharePoint.
Travaux pratiques : Archivage et conservation : initialiser la mise en conformité et configurer les étiquettes et les politiques de conservation.

10) Prévention de la perte de données
- Gestion des droits à l'information (IRM).
- Extension polyvalente sécurisée de courriers Internet (S-MIME).
- Chiffrement des messages Microsoft 365.
Travaux pratiques : Mettre en œuvre les politiques de prévention de la perte de données (DLP) : gérer les politiques DLP. Tester la MRM et les politiques de DLP.

11) Sécurité des applications cloud
- Principes fondamentaux de la prévention des pertes de données (DLP).
- Créer une politique de prévention des pertes de données (DLP).
- Personnaliser une politique DLP.
- Créer une politique DLP pour protéger les documents.
- Conseils de politique.

12) Gestion de la conformité
- Centre de conformité.
Travaux pratiques : Mise en application : utilisation des évaluations pour déterminer le score de conformité. Utilisation du score de conformité pour prendre des décisions organisationnelles.

13) Gestion des risques d'initiés
- Risques d'initié.
- Accès privilégié.
- Obstacles à l'information.
- Construire des murs éthiques dans Exchange Online.
Travaux pratiques : Gestion des accès privilégiés : mettre en place une gestion de l'accès privilégié et traiter une demande.

14) Gestion de la recherche et des enquêtes
- Rechercher du contenu.
- Faire l'audit des enquêtes de journal.
- Advanced eDiscovery.
Travaux pratiques : Gérer la recherche et l'examen : enquêter sur vos données Microsoft 365 et mener une demande de sujet de données

LES DATES

Nous contacter