Formation Microsoft 365 Security Administration (Examen MS-500)

Durée :	3 jours
Public :	Administrateurs Systèmes Microsoft avec bonnes connaissances d'Azure
Pré-requis :	Avoir de bonnes connaissances de l'administration Windows Server / Active Directory, de 365 et d'Azure
Objectifs :	Mettre en œuvre et gérer l'identité et l'accès 365 - Mettre en œuvre et gérer la protection contre les menaces - Gérer les fonctions de gouvernance et de conformité dans Microsoft 365
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	CLO101252-F
Note de satisfaction des participants:	Pas de données disponibles
Certifications :	MICROSOFT : Microsoft 365 Security Administration Pas de données disponibles au 01/06/2024

Mettre en œuvre et gérer l'identité et l'accès (30 à 35 %)

Environnements hybrides Microsoft 365 sécurisés

planifier les options d'authentification AD Azure
planifier les options de synchronisation Azure AD
surveiller et dépanner les événements Azure AD Connect

Identités sécurisées

mettre en œuvre l'adhésion dynamique du groupe Azure AD
mettre en œuvre la gestion des mots de passe
configurer et gérer la gouvernance de l'identité

Mettre en œuvre des méthodes d'authentification

sécurité de signature du plan
mettre en œuvre l'authentification multifactorielle (MFA)
gérer et surveiller la MFA
planifier et mettre en œuvre des méthodes d'authentification comme Windows Hello
configurer et gérer les options d'authentification des utilisateurs Azure AD

Mettre en œuvre l’accès conditionnel

plan de conformité et politiques d’accès conditionnel
configurer et gérer la conformité des appareils pour la sécurité des terminaux
mettre en œuvre et gérer l’accès conditionnel

Mettre en œuvre le contrôle d’accès basé sur les rôles (RBAC)

planifier les rôles
configurer les rôles
rôles de vérification

Mettre en œuvre Azure AD Privileged Identity Management (PIM)

plan pour Azure PIM
implémenter et configurer les rôles Azure PIM
gérer les missions de rôle Azure PIM

Mettre en œuvre Azure AD Identity Protection

mettre en œuvre une politique sur les risques pour les utilisateurs
mettre en œuvre une politique sur les risques de signature
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 (20 à 25 %)

Mettre en œuvre une solution hybride de protection des menaces pour l’entreprise

planifier une solution Azure Advanced Threat Protection (ATP)
installer et configurer Azure ATP
surveiller et gérer Azure ATP

Mettre en œuvre la protection contre les menaces liées aux appareils

planifier une solution Microsoft Defender ATP
mettre en œuvre Microsoft Defender ATP
gérer et surveiller Microsoft Defender ATP

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

plan de protection du dispositif et de l’application
configurer et gérer Microsoft Defender Application Guard
configurer et gérer Microsoft Defender Application Control
configurer et gérer Microsoft Defender Exploit Guard
configurer Secure Boot
configurer et gérer le chiffrement des périphériques Windows
configurer et gérer le chiffrement des périphériques non Windows
plan pour sécuriser les données des applications sur les appareils
mettre en œuvre des politiques de protection des applications

Mettre en œuvre et gérer Office 365 ATP

configurer Office 365 ATP
surveiller Office 365 ATP
effectuer des attaques simulées en utilisant Attack Simulator Monitor Microsoft 365 Security avec Azure Sentinel
planifier et mettre en œuvre Azure Sentinel
configurer les playbooks dans Azure Sentinel
gérer et surveiller Azure Sentinel
répondre aux menaces à Azure Sentinel

Mettre en œuvre et gérer la protection de l'information (15 à 20 %)

Accès sécurisé aux données dans Office 365

planifier un accès sécurisé aux données dans Office 365
mettre en œuvre et gérer le système Customer Lockbox
configurer l'accès aux données dans les workloads de collaboration Office 365
configurer le partage B2B pour les utilisateurs externes

Gérer les étiquettes de sensibilité

planifier une solution d'étiquette de sensibilité
configurer les étiquettes et les politiques de sensibilité
configurer et utiliser l'analyse des étiquettes
utiliser des étiquettes de sensibilité avec les applications Teams, SharePoint, OneDrive et Office

Gérer la prévention de la perte de données (DLP)

planifier une solution DLP
créer et gérer des politiques DLP
créer et gérer des types de renseignements sensibles
surveiller les rapports DLP
gérer les notifications DLP

Mettre en œuvre et gérer Microsoft Cloud App Security

Planifier la mise en œuvre de la sécurité des applications infonuagiques
configurer Microsoft Cloud App Security
gérer la découverte d'applications en nuage
gérer les entrées dans le catalogue d'applications Cloud
gérer les applications dans Cloud App Security
gérer la sécurité de l'application Microsoft Cloud
configurer les connecteurs Cloud App Security et les applications Oauth
configurer les politiques et les modèles de sécurité de l'application Cloud
examiner, interpréter et répondre aux alertes, rapports, tableaux de bord et journaux de sécurité de l'application Cloud

Gérer les fonctions de gouvernance et de conformité dans Microsoft 365 (25-30 %)

Configurer et analyser les rapports de sécurité

surveiller et gérer l'état de sécurité des appareils à l'aide de Microsoft Endpoint Manager Admin Centre
gérer et surveiller la sécurité et les tableaux de bord à l'aide de Microsoft 365 Security Center

planifier des rapports de sécurité personnalisés avec l’API Graph Security
configurer les politiques d’alerte dans le centre d’administration Sécurité et conformité

Gérer et analyser les journaux et rapports d’audit

plan de vérification 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 la politique d’alerte d’audit

Gérer la gouvernance et la conservation des données

plan de gouvernance et de conservation des données
examiner et interpréter les rapports et les tableaux de bord sur la gouvernance des données
configurer les politiques de conservation
définir les types d’événements de gouvernance des données
définir les politiques de supervision
configurer les retenues d’information
trouver et récupérer les données Office 365 supprimées
configurer l’archivage des données
gérer les boîtes aux lettres inactives

Gérer la recherche et l’enquête

planifier la recherche de contenu et la preuve électronique
déléguer les autorisations d’utiliser les outils de recherche et de découverte
utiliser des outils de recherche et d’investigation pour effectuer des recherches de contenu
exporter les résultats de recherche de contenu
gérer les cas de preuve électronique

Gérer la conformité de la réglementation sur la confidentialité des données

plan de conformité réglementaire dans Microsoft 365
examiner et interpréter les tableaux de bord et les rapports du RGPD
gérer les demandes des personnes concernées (DSR)
administrer le gestionnaire de la conformité
examiner les rapports du gestionnaire de la conformité
Créer et exécuter les évaluations et les actions du Responsable Conformité