Microsoft 365 Fundamentals

Objectifs pédagogiques

- Gérer les utilisateurs et les groupes dans Microsoft 365
- Ajouter un domaine personnalisé
- Configurer les rôles administratifs
- Déployer les applications Microsoft 365
- Gérer les identités synchronisées
- Analyser les vecteurs de menace
- Mettre en œuvre Microsoft 365 Defender
- Mettre en œuvre la gestion des identités privilégiées (PIM)
- Sécuriser les points de terminaison
- Protéger la messagerie

Prérequis

- Avoir une bonne compréhension du DNS et une expérience fonctionnelle de base avec les services Microsoft 365
- Une bonne compréhension des pratiques informatiques générales

Programme détaillé

Configurez votre expérience Microsoft 365

- Introduction
- Configurer votre expérience Microsoft 365
- Gérer les abonnements de vos locataires dans Microsoft 365
- Intégrer Microsoft 365 avec des applications dédiées à la relation client
- Terminer la configuration de vos locataires dans Microsoft 365

Gérer les utilisateurs, les licences et les contacts de messagerie dans Microsoft 365

- Introduction
- Déterminer le modèle d'identité de l'utilisateur pour votre organisation
- Créer des comptes utilisateurs dans Microsoft 365
- Gérer les paramètres des comptes d'utilisateurs dans Microsoft 365
- Gérer les licences d'utilisateur dans Microsoft 365
- Récupérer les comptes d'utilisateurs supprimés dans Microsoft 365
- Effectuer la maintenance des utilisateurs en bloc dans Azure Active Directory
- Créer et gérer des utilisateurs invités
- Créer et gérer des contacts de messagerie

Gestion des groupes dans Microsoft 365

- Introduction
- Examiner les groupes dans Microsoft 365
- Créer et gérer des groupes dans Microsoft 365
- Créer des groupes dynamiques à l'aide d'Azure rule builder

- Créer une stratégie de dénomination de groupe Microsoft 365
- Créer des groupes dans Exchange Online et SharePoint Online

Ajouter un domaine personnalisé dans Microsoft 365

- Introduction
- Prévoir un domaine personnalisé pour votre déploiement de Microsoft 365
- Planifier les zones DNS pour un domaine personnalisé
- Planifier les exigences en matière d'enregistrement DNS pour un domaine personnalisé
- Créer un domaine personnalisé dans Microsoft 365

Configurer la connectivité du client à Microsoft 365

- Introduction
- Examiner le fonctionnement de la configuration automatique des clients
- Explorer les enregistrements DNS nécessaires à la configuration du client
- Configurer les clients Outlook
- Dépanner la connectivité des clients

Configurer les rôles administratifs dans Microsoft 365

- Introduction
- Explorer le modèle de permission de Microsoft 365
- Explorer les rôles d'administrateur de Microsoft 365
- Attribuer des rôles d'administrateur aux utilisateurs dans Microsoft 365
- Déléguer des rôles d'administrateur à des partenaires
- Gérer les autorisations à l'aide d' OU (Organizational Units) dans Azure Active Directory
- Élever les privilèges à l'aide d'Azure AD Privileged Identity Management (gestion des identités privilégiées)

Gérer l'état de fonctionnement des locataires et les services dans Microsoft 365

- Introduction
- Surveillez la santé de vos services Microsoft 365
- Surveiller la santé des locataires à l'aide de Microsoft 365 Adoption Score
- Surveiller la santé des locataires à l'aide de l'analyse de l'utilisation de Microsoft 365
- Développer un plan de réponse aux incidents
- Demander de l'aide à Microsoft

Déployer Microsoft 365 Apps pour l'entreprise

- Introduction
- Découvrez les fonctionnalités d'entreprise de Microsoft 365 Apps
- Explorez la compatibilité de vos applications en utilisant la boîte à outils de préparation (Readiness Toolkit)
- Effectuer une installation en libre-service de Microsoft 365 Apps for enterprise
- Déployer Microsoft 365 Apps pour l'entreprise avec Microsoft Configuration Manager
- Déployer Microsoft 365 Apps pour l'entreprise à partir du cloud

- Déployer Microsoft 365 Apps pour l'entreprise à partir d'une source locale
- Gérer les mises à jour de Microsoft 365 Apps for enterprise
- Explorer les canaux de mise à jour pour Microsoft 365 Apps for enterprise
- Gérer vos applications en cloud à l'aide du centre d'administration de Microsoft 365 Apps

Analysez les données de votre environnement de travail Microsoft 365 à l'aide de Microsoft Viva Insights

- Introduction
- Examiner les fonctions analytiques de Microsoft Viva Insights
- Créer des analyses personnalisées avec Microsoft Viva Insights
- Configurer Microsoft Viva Insights
- Examiner les sources de données Microsoft 365 utilisées dans Microsoft Viva Insights
- Préparer les données organisationnelles dans Microsoft Viva Insights

Explorer la synchronisation des identités

- Introduction
- Examiner les modèles d'identité pour Microsoft 365
- Examiner les options d'authentification pour le modèle d'identité hybride
- Explorer la synchronisation des annuaires

Préparer la synchronisation des identités avec Microsoft 365

- Introduction
- Planifier le déploiement d'Azure Active Directory
- Préparer la synchronisation de l'annuaire
- Choisir l'outil de synchronisation d'annuaire
- Planifier la synchronisation d'annuaires à l'aide d'Azure AD Connect
- Planifier la synchronisation d'annuaires à l'aide d'Azure AD Connect Cloud Sync

Mettre en œuvre des outils de synchronisation des annuaires

- Introduction
- Configurer les prérequis d'Azure AD Connect
- Configurer Azure AD Connect
- Surveiller les services de synchronisation à l'aide de Azure AD Connect Health
- Configurer les prérequis d'Azure AD Connect Cloud Sync
- Configurer Azure AD Connect Cloud Sync

Gérer les identités synchronisées

- Introduction
- Gérer les utilisateurs avec la synchronisation des annuaires
- Gérer les groupes avec la synchronisation des annuaires
- Utiliser les groupes de sécurité Azure AD Connect Sync pour maintenir la synchronisation de l'annuaire
- Configurer les filtres d'objets pour la synchronisation d'annuaire
- Dépanner la synchronisation d'annuaire

Gérer l'accès sécurisé des utilisateurs dans Microsoft 365

- Introduction
- Gérer les mots de passe des utilisateurs
- Activer l'authentification pass-through
- Activer l'authentification multi-facteurs
- Activer la connexion sans mot de passe avec Microsoft Authenticator
- Explorer la gestion des mots de passe en libre-service
- Explorer Windows Hello for Business
- Mettre en œuvre Azure AD Smart Lockout
- Mettre en œuvre des stratégies d'accès conditionnel
- Explorer les valeurs par défaut de la sécurité dans Azure AD
- Examiner les problèmes d'authentification à l'aide des journaux de connexion

Examiner les vecteurs de menace et les violations de données

- Introduction
- Explorer le paysage actuel du marché du travail et des menaces
- Examiner comment le phishing récupère des informations sensibles
- Examiner comment le spoofing trompe les utilisateurs et compromet la sécurité des données
- Comparer le spam et les logiciels malveillants
- Examiner comment une violation de compte compromet un compte d'utilisateur
- Examiner les attaques par élévation de privilèges
- Examiner comment l'exfiltration de données déplace des données hors de votre locataire
- Examiner comment les attaquants suppriment les données de votre locataire
- Examiner comment la fuite de données expose les données en dehors de votre locataire
- Examiner d'autres types d'attaques

Explorer le modèle de sécurité "Zero Trust" (confiance zéro)

- Introduction
- Examiner les principes et les composantes du modèle de confiance zéro
- Planifier la mise en place d'un modèle de sécurité de confiance zéro dans votre organisation
- Examiner la stratégie de Microsoft pour un réseau de confiance zéro
- Adopter une approche de confiance zéro

Explorer les solutions de sécurité dans Microsoft 365 Defender

- Introduction
- Renforcez la sécurité de votre messagerie en utilisant Exchange Online Protection et Microsoft Defender pour Office 365
- Protégez les identités de votre organisation avec Microsoft Defender for Identity
- Protégez votre réseau d'entreprise contre les menaces avancées avec Microsoft Defender for Endpoint
- Protéger contre les cyberattaques avec Microsoft 365 Threat Intelligence
- Fournir un aperçu des activités suspectes à l'aide de Microsoft Cloud App Security

- Examiner les rapports de sécurité dans Microsoft 365 Defender

Examiner Microsoft Secure Score

- Introduction
- Explorer Microsoft Secure Score
- Évaluer votre posture de sécurité avec Microsoft Secure Score
- Améliorer votre score de sécurité
- Suivez l'historique de votre Microsoft Secure Score et atteignez vos objectifs

Examiner la gestion des identités privilégiées

- Introduction
- Explorer la gestion des identités privilégiées dans Azure AD
- Configurer la gestion des identités privilégiées
- Auditer la gestion des identités privilégiées
- Explorer Microsoft Identity Manager
- Contrôler les tâches d'administration privilégiées à l'aide de la gestion des accès privilégiés

Examiner Azure Identity Protection

- Introduction
- Présentation d'Azure Identity Protection
- Activer les stratégies de protection par défaut dans Azure Identity Protection
- Explorer les vulnérabilités et les événements à risque détectés par Azure Identity Protection
- Planifier votre analyse sur l'identité

Examiner la protection d'Exchange Online

- Introduction
- Examiner le circuit de la protection contre les logiciels malveillants
- Détecter les messages contenant du spam ou des logiciels malveillants à l'aide de la purge automatique zéro heure
- Explorer la protection anti-spoofing fournie par Exchange Online Protection
- Explorer d'autres protections anti-spoofing
- Examiner le filtrage des spams sortants

Examiner Microsoft Defender pour Office 365

- Introduction
- Passer de l'EOP à Microsoft Defender pour Office 365
- Étendre les protections EOP en utilisant les pièces jointes et les liens sécurisés
- Gérer les renseignements falsifiés
- Configurer les stratégies de filtrage des spams sortants
- Débloquer l'envoi d'e-mails par les utilisateurs

Gérer les pièces jointes en sécurité

- Introduction
- Protéger les utilisateurs contre les pièces jointes malveillantes en utilisant les pièces jointes sécurisées
- Créer des stratégies de pièces jointes sécurisées à l'aide de Microsoft Defender pour Office 365
- Créer des stratégies de pièces jointes sécurisées à l'aide de PowerShell
- Modifier une stratégie de pièces jointes sécurisées existante
- Créer une règle de transport pour contourner une stratégie de pièces jointes sécurisées
- Examiner l'expérience de l'utilisateur final avec les pièces jointes sécurisées

Gérer les liens sécurisés

- Introduction
- Protéger les utilisateurs contre les URL malveillantes en utilisant des liens sûrs
- Créer des stratégies de liens sécurisés à l'aide de Microsoft 365 Defender
- Créer des stratégies de liens sécurisés à l'aide de PowerShell
- Modifier une stratégie de Safe Links existante
- Créer une règle de transport pour contourner une politique de Safe Links
- Examiner l'expérience de l'utilisateur final avec les Safe Links

Explorer la détection des menaces dans Microsoft 365 Defender

- Introduction
- Explorer le graphe de sécurité intelligent de Microsoft
- Explorer les règles d'alerte dans Microsoft 365
- Exécuter des enquêtes et des réponses automatisées
- Explorer la chasse aux menaces avec Microsoft Threat Protection
- Explorer la chasse aux menaces avancée dans Microsoft 365 Defender
- Découvrir l'analyse des menaces dans Microsoft 365
- Identifier les problèmes liés aux menaces à l'aide des rapports de Microsoft Defender

Mettre en œuvre la protection des applications en utilisant Microsoft Defender for Cloud Apps

- Introduction
- Explorer Microsoft Defender Cloud Apps
- Déployer Microsoft Defender pour Cloud Apps
- Configurer les stratégies de fichiers dans Microsoft Defender for Cloud Apps
- Gérer et répondre aux alertes dans Microsoft Defender for Cloud Apps
- Configurer Cloud Discovery dans Microsoft Defender for Cloud Apps
- Dépanner Cloud Discovery dans Microsoft Defender for Cloud Apps

Mettre en œuvre la protection des points de terminaison à l'aide de Microsoft Defender for Endpoint

- Introduction
- Découvrir Microsoft Defender pour Endpoint
- Configurer Microsoft Defender for Endpoint dans Microsoft Intune

- Intégrer des périphériques dans Microsoft Defender for Endpoint
- Gérer les vulnérabilités des terminaux avec Microsoft Defender Vulnerability Management
- Gérer la découverte des périphériques et l'évaluation des vulnérabilités
- Réduire l'exposition aux menaces et aux vulnérabilités

Mettre en œuvre une protection contre les menaces en utilisant Microsoft Defender pour Office 365

- Introduction
- Explorer la stack de protection de Microsoft Defender pour Office 365
- Enquêter sur les attaques de sécurité à l'aide de Threat Explorer
- Identifier les problèmes de cybersécurité à l'aide de Threat Trackers
- Se préparer aux attaques grâce à la formation à la simulation d'attaques