Administrateur Microsoft 365 MS-102

Programme *(Mis à jour le 28/12/2024)*

Configurer votre expérience Microsoft 365

- Configurer le profil d'organisation de votre entreprise.
  Maintenir les exigences minimales d'abonnement pour votre entreprise.
  Gérer vos services et compléments en attribuant plus de licences, en achetant plus de stockage, etc.
  Créer une liste de contrôle pour confirmer que votre locataire Microsoft 365 répond aux besoins de votre entreprise.

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

- Identifier le modèle d'identité utilisateur le mieux adapté à votre organisation.
  Créer des comptes d'utilisateurs à partir du Centre d'administration Microsoft 365 et de Windows PowerShell.
  Gérer les comptes d'utilisateurs et les licences dans Microsoft 365.
  Récupérer les comptes d'utilisateurs supprimés dans Microsoft 365.
  Effectuer une maintenance groupée des utilisateurs dans Microsoft Entra ID.
  Créer et gérer des invités et collaborez avec eux sur des sites SharePoint.
  Créer et gérer des contacts.

Gérer les groupes dans Microsoft 365

- Décrire les différents types de groupes disponibles dans Microsoft 365.
  Créer et gérer des groupes à l'aide du centre d'administration Microsoft 365 et de Windows PowerShell.
  Créer et gérer des groupes dans Exchange Online et SharePoint Online

Ajouter un domaine personnalisé dans Microsoft 365

- Identifier les facteurs à prendre en compte lors de l'ajout d'un domaine personnalisé à Microsoft 365.
  Planifier les zones DNS utilisées dans un domaine personnalisé.
  Planifier les exigences d'enregistrement DNS pour un domaine personnalisé.
  Ajouter un domaine personnalisé à votre déploiement Microsoft 365.

Configurer la connectivité client à Microsoft 365

- Utiliser la découverte automatique pour connecter un client Outlook à Exchange Online.
  Identifier les enregistrements DNS nécessaires à Outlook et aux autres clients liés à Office pour localiser automatiquement les services dans Microsoft 365 à l'aide du processus de découverte automatique.
  Décrire les protocoles de connectivité qui permettent à Outlook de se connecter à Microsoft 365.
  Identifier les outils qui peuvent vous aider à résoudre les problèmes de connectivité dans les déploiements Microsoft 365.

Gérer les autorisations, les rôles et les groupes de rôles dans Microsoft 365

- Comprendre comment les rôles sont utilisés dans l'écosystème Microsoft 365.
  Décrire le modèle d'autorisation de contrôle d'accès en fonction du rôle Azure utilisé dans Microsoft 365.
  Identifiee les tâches clés affectées aux rôles d'administrateur Microsoft 365 courants.
  Identifier les meilleures pratiques lors de la configuration des rôles d'administrateur.
  Déléguer des rôles d'administrateur aux partenaires.

Référence
THIS3359

Durée
5 jours / 35 heures

Prix HT / stagiaire
3250€

Objectifs pédagogiques

- Configurer votre tenant Microsoft 365
- Gérer votre tenant Microsoft 365
- Implémenter la synchronisation des identités
- Gérer l'identité et l'accès dans Microsoft 365
- Gérer vos services de sécurité dans Microsoft Defender XDR
- Implémenter la protection contre les menaces à l'aide de Microsoft Defender XDR
- Explorer la gouvernance des données dans Microsoft 365
- Implémenter la conformité dans Microsoft 365
- Gérer la conformité dans Microsoft 365

Niveau requis

- Les candidats doivent avoir une connaissance pratique des charges de travail Microsoft 365 et avoir une expérience sur les charges de travail Microsoft 365 (Exchange, SharePoint, Skype Entreprise, Windows en tant que service).
  Il est important d'avoir une connaissance pratique des réseaux, des serveurs d'administration et les fondamentaux informatiques tels que DNS, Active Directory et PowerShell.
  Pour suivre cette formation vous devez avoir suivi une de ces formations MS-203, MS-700 ou SC-300 ou détenir un niveau équivalent.

Public concerné

- Administrateurs Microsoft 365 qui déploient et gèrent Microsoft 365. Ils effectuent l'implémentation et l'administration au niveau du locataire Microsoft 365 des environnements cloud et hybrides.

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez

Implémenter des groupes de rôles dans Microsoft 365.
Gérer les autorisations à l'aide d'unités administratives dans l'ID Microsoft Archivé.
Gérer les autorisations dans SharePoint pour éviter le partage excessif des données.
Élever les privilèges pour accéder aux centres d'administration à l'aide de l'ID Microsoft Privileged Identity Management.

Gérer l'intégrité et les services du tenant dans Microsoft 365

- Surveiller l'intégrité du service Microsoft 365 de votre organisation dans le Centre d'administration Microsoft 365.
  Implémenter la connectivité réseau Microsoft 365 pour les évaluations et les insights.
  Implémenter la sauvegarde Microsoft 365 (préversion) pour une sauvegarde et une restauration de contenu rapides.
  Développer un plan de réponse aux incidents pour gérer les incidents qui peuvent se produire avec votre service Microsoft 365.
  Demander de l'aide à Microsoft pour résoudre les problèmes de support technique, de prévente, de facturation et d'abonnement.

Déployer les Applications Microsoft 365 pour les grandes entreprises

- Décrire la fonctionnalité Applications Microsoft 365 for enterprise.
  Planifier une stratégie de déploiement pour Microsoft 365 Apps for enterprise.
  Effectuer une installation pilotée par l'utilisateur de Microsoft 365 Apps for enterprise.
  Déployer Applications Microsoft 365 avec Microsoft Endpoint Configuration Manager.
  Identifier les mécanismes de gestion des déploiements centralisés d'applications Microsoft 365 for enterprise.
  Déployer Microsoft 365 Apps for enterprise avec le Kit de ressources déploiement d'Office.
  Gérer les mises à jour de Microsoft 365 Apps for enterprise.
  Déterminer le canal de mise à jour et la méthode d'application qui s'appliquent à votre organisation.

Analyser les données de votre espace de travail Microsoft 365 à l'aide de Microsoft Viva Insight

- Améliorer la collaboration dans votre organisation ave Microsoft Viva Insights
  Analyser votre façon de travailler avec Personal Insights.
  Offrir une visibilité sur les habitudes de travail en équipe susceptibles d'entraîner stress et épuisement professionnel avec l'application Team Insights.
  Vérifier comment la culture du travail affecte le bien-être des employés avec Organization Insights.
  Répondre aux questions critiques sur la résilience et la culture de travail avec Insights avancé.

Explorer la synchronisation des identités

- Décrire les options d'authentification et de provisionnement de Microsoft 365.
  Expliquer les modèles d'identité Microsoft 365 : identité cloud uniquement et identité hybride.
  Expliquer les trois méthodes d'authentification dans le modèle d'identité hybride : synchronisation du hachage du mot de passe, authentification directe et authentification fédérée.
  Utiliser la synchronisation d'annuaires avec Microsoft 365.

Préparer la synchronisation des identités avec Microsoft 365

- Identifier les tâches nécessaires pour configurer votre environnement Entra ID.
  Planifier la synchronisation d'annuaires pour synchroniser vos objets Entra ID.
  Identifier les fonctionnalités de Microsoft Entra Connect Sync et de Microsoft Entra Cloud Sync.
  Choisir la synchronisation d'annuaires adapté à l'environnement et besoins de l'entreprise.

Gérer les identités synchronisées

- Synchroniser efficacement les utilisateurs.
  Gérer les groupes avec la synchronisation d'annuaire.
  Utiliser les groupes de sécurité Microsoft Entra Connect Sync pour aider à

maintenir la synchronisation des annuaires.
Configurer les filtres d'objets pour la synchronisation d'annuaire.
Synchroniser les identités des utilisateurs dans leurs organisations et environnements hybrides avec Microsoft Identity Manager .
Dépanner la synchronisation des annuaires à l'aide de diverses tâches et outils de dépannage

Implémenter des outils de synchronisation d'annuaires

- Configurer les prérequis de Microsoft Entra Connect Sync et de Microsoft Entra Cloud Sync.
  Configurer Microsoft Entra Connect Sync et Microsoft Entra Cloud Sync.
  Surveiller les services de synchronisation à l'aide de Microsoft Entra Connect Health.

Gérer l'accès utilisateur sécurisé dans Microsoft 365

- Gérer les mots de passe utilisateur.
  Créer des stratégies d'accès conditionnel.
  Activer les paramètres de sécurité par défaut.
  Décrire l'authentification directe.
  Activer l'authentification multifacteur.
  Décrire la gestion des mots de passe en libre-service.
  Implémenter le verrouillage intelligent Microsoft Entra.

Examiner les vecteurs de menace et les violations de données

- Connaitre les techniques utilisées par les pirates pour compromettre les comptes d'utilisateurs par e-mail, prendre le contrôle des ressources et compromettre les données.
  Atténuer une violation de compte.
  Empêcher une attaque d'élévation de privilèges.
  Empêcher l'exfiltration, la suppression et la fuite de données.

Découvrir le modèle de sécurité Zero Trust

- Connaitre l'approche Zero Trust de la sécurité dans Microsoft 365.
  Comprendre les principes et les composants du modèle de sécurité Zero Trust.
  Décrire les cinq étapes pour mettre en œuvre un modèle de sécurité Zero Trust dans votre organisation.
  Expliquer l'histoire et la stratégie de Microsoft autour du réseau Zero Trust.

Gérer l'accès sécurisé des utilisateurs dans Microsoft 365

- Gérer les mots de passe utilisateur.
  Créer des stratégies d'accès conditionnel.
  Activer les paramètres de sécurité par défaut.
  Décrire l'authentification directe.
  Activer l'authentification multifacteur.
  Décrire la gestion des mots de passe en libre-service.
  Implémenter le verrouillage intelligent Microsoft Entra.

Explorer les solutions de sécurité dans Microsoft Defender XDR

- Identifier les fonctionnalités de Microsoft Defender pour Office 365 qui améliorent la sécurité de la messagerie dans un déploiement Microsoft 365.
  Identifier, détecter et enquêter sur les menaces avancées, identités compromises et actions internes malveillantes dirigées contre votre organisation avec Microsoft Defender pour Identity.
  Aider les réseaux d'entreprise à prévenir, détecter, enquêter et répondre aux menaces avancées avec Microsoft Defender pour Endpoint.
  Décrire comment Microsoft 365 Threat Intelligence peut être bénéfique pour les responsables de la sécurité et les administrateurs de votre organisation.
  Améliorer la visibilité et le contrôle sur votre locataire Microsoft 365 à travers trois domaines principaux dans Microsoft Cloud App Security.

Examiner le score de sécurité Microsoft

- Décrire les avantages de Secure Score et quels types de services peuvent être analysé.
  Collecter des données à l'aide de l'API Secure Score.
  Identifier les écarts entre votre état actuel et où vous aimeriez en être en matière de sécurité.

Identifier les actions qui augmentent votre sécurité en atténuant les risques.
Chercher ou sont déterminées les menaces de chaque action et l'impact sur les utilisateurs.

Examiner la gestion des identités privilégiées dans Microsoft Entra ID

- Décrire comment Microsoft Entra Privileged Identity Management (PIM) vous permet de gérer, contrôler et surveiller l'accès aux ressources importantes de votre organisation.
  Configurer le processus d'attribution de rôle PIM à utiliser dans votre organisation.
  Utiliser l'historique d'audit PIM pour voir toutes les attributions et activations d'utilisateurs au cours d'une période donnée pour tous les rôles privilégiés.

Examiner la protection Microsoft Entra ID

- Décrire Azure Identity Protection (AIP) et les types d'identités pouvant être protégées.
  Activer les trois politiques de protection par défaut dans AIP.
  Identifier les vulnérabilités et les événements à risque détectés par l'AIP.
  Planifier votre enquête sur la protection des identités basées sur le cloud.
  Planifier la protection de votre environnement Entra ID contre les failles de sécurité.

Examiner la protection du courrier électronique dans Microsoft 365

- Décrire comment Exchange Online Protection analyse les e-mails pour fournir une protection anti-malware et anti-spam.
  Énumérer plusieurs mécanismes utilisés par Exchange Online Protection pour filtrer le spam et les logiciels malveillants.
  Décrire d'autres solutions que les administrateurs pourraient mettre en œuvre pour fournir une protection supplémentaire contre le phishing et l'usurpation d'identité.
  Comprendre comment EOP offre une protection contre le spam sortant.

Améliorer la protection de votre messagerie à l'aide de Microsoft Defender pour Office 365

- Décrire comment la fonctionnalité Pièces jointes sécurisées de Microsoft Defender pour Office 365 bloque les logiciels malveillants Zero Day dans les pièces jointes et les documents.
  Décrire comment la fonctionnalité Liens sécurisés dans Microsoft Defender pour Office 365 protège les utilisateurs contre les URL malveillantes intégrées dans les courriers électroniques et les documents qui pointent vers des sites Web malveillants.
  Créer des politiques de filtrage du spam sortant.
  Gérer l'accès aux e-mails avec la liste Restreindre l'accès et la liste Locataires autorisés/bloqués.
  Envoyer des messages, des URL, des fichiers et des pièces jointes à Microsoft pour analyse.

Gérer les pièces jointes fiables

- Créer et modifier une stratégie de pièces jointes fiables à l'aide de Microsoft Defender XDR.
  Créer une stratégie de pièces jointes fiables à l'aide de PowerShell.
  Configurer une stratégie des pièces jointes fiables.
  Désactiver une stratégie pièces jointes fiables grâce à une règle de transport.
  Décrire l'expérience de l'utilisateur final lorsqu'une pièce jointe est analysée et détectée comme malveillante.

Gérer des liens fiables

- Créer et modifier une stratégie de liens fiables à l'aide de Microsoft Defender XDR.
  Créer une stratégie de liens fiables à l'aide de PowerShell.
  Configurer une stratégie de liens fiables.
  Désactiver une stratégie de liens fiables grâce à une règle de transport
  Décrire l'expérience de l'utilisateur final lorsque des liens fiables identifient un lien vers un site web malveillant incorporé dans un e-mail et un lien vers un fichier malveillant hébergé sur un site web.

Explorer les renseignements sur les menaces dans Microsoft Defender XDR

- Optimiser les renseignements sur les menaces dans Microsoft 365 avec Microsoft Intelligent Security Graph.
  Créer des alertes capables d'identifier les événements malveillants ou suspects.
  Comprendre le fonctionnement du processus d'enquête et de réponse automatisé de Microsoft Defender XDR.
  Identifier les menaces de cybersécurité avec la chasse aux menaces.
  Décrire comment la recherche avancée dans Microsoft Defender XDR inspecte de manière proactive les événements de votre réseau pour localiser les indicateurs de menace et les entités.

Implémenter la protection des applications à l'aide de Microsoft Defender pour les applications cloud

- Décrire comment Microsoft Defender pour les applications cloud offre une meilleure visibilité sur l'activité cloud du réseau et augmente la protection des données critiques dans les applications cloud.
  Déployer Microsoft Defender pour les applications cloud.
  Contrôler vos applications cloud avec des politiques de fichiers.
  Gérer et répondre aux alertes générées par ces politiques.
  Configurer et dépanner Cloud Discovery.

Implémenter endpoint Protection à l'aide de Microsoft Defender pour point de terminaison

- Aider les réseaux d'entreprise à prévenir, détecter, examiner et répondre aux menaces avancées avec Microsoft Defender for Endpoint.
  Intégrer des appareils pris en charge à Microsoft Defender pour point de terminaison.
  Implémenter le module sur la Gestion des menaces et des vulnérabilités pour identifier, évaluer et corriger efficacement les faiblesses du point de terminaison.
  Configurer la détection d'appareils afin de découvrir des appareils non managés connectés à votre réseau d'entreprise.
  Réduire l'exposition aux menaces et aux vulnérabilités de votre organisation en corrigeant des problèmes basés sur des recommandations de sécurité prioritaires.

Implémenter la protection contre les menaces à l'aide de Microsoft Defender pour Office 365

- Décrire la pile de protection fournie par Microsoft Defender pour Office 365.
  Utiliser Threat Explorer pour enquêter sur les menaces et aider à protéger votre locataire.
  Décrire les widgets et les vues Threat Tracker fournissant des informations sur les différents problèmes de cybersécurité susceptibles d'affecter votre entreprise.
  Exécuter des scénarios d'attaque réalistes à l'aide d'Attack Simulator pour aider à identifier les utilisateurs vulnérables avant qu'une véritable attaque n'affecte votre organisation.

Examiner les solutions de gouvernance des données dans Microsoft Purview

- Protéger les données sensibles avec Microsoft Purview Information Protection.
  Gouverner les données organisationnelles à l'aide de Microsoft Purview Data Lifecycle Management.
  Minimiser les risques internes avec Microsoft Purview Insider Risk Management.
  Expliquer les solutions Microsoft Purview eDiscovery.

Découvrir les pratiques de gestion des données dans Microsoft 365

- Activer et désactiver une boîte aux lettres d'archivage dans le portail de conformité Microsoft Purview et via Windows PowerShell.
  Exécuter des tests de diagnostic sur une boîte aux lettres d'archivage.
  Restaurer les données supprimées dans Exchange Online et SharePoint Online.

Explorer la rétention dans Microsoft 365

- Expliquer le fonctionnement des politiques de rétention et des étiquettes de rétention.
  Identifier les capacités des stratégies de rétention et des étiquettes de rétention.

Sélectionner l’étendue appropriée pour une stratégie en fonction des besoins de l’entreprise.
Identifier les différences entre les paramètres de conservation et les conservations eDiscovery.
Restreindre les modifications de conservation en utilisant le verrouillage de préservation.

Utiliser le chiffrement des messages Microsoft Purview

- Décrire les fonctionnalités de Microsoft Purview Message Encryption.
  Configurer et utiliser Microsoft Purview Message Encryption.
  Ajouter une image de marque organisationnelle aux e-mails chiffrés.
  Définir des règles de flux de messagerie qui appliquent des modèles de personnalisation et de chiffrement pour chiffrer les messages électroniques.
  Expliquer les fonctionnalités supplémentaires de Microsoft Purview Advanced Message Encryption.

Explorer la conformité dans Microsoft 365

- Aider les organisations à gérer les risques, à protéger les données et à rester en conformité avec les réglementations et les normes avec Microsoft 365.
  Planifier vos premières tâches de conformité dans Microsoft Purview.
  Gérer vos exigences de conformité avec Compliance Manager.
  Gérer la posture de conformité et les actions d’amélioration à l’aide du tableau de bord du gestionnaire de conformité.
  Expliquer comment le score de conformité d’une organisation est déterminé.

Mettre en œuvre la gestion des risques Microsoft Purview Insider

- Décrire la fonctionnalité de gestion des risques internes dans Microsoft 365.
  Élaborer un plan pour mettre en œuvre la solution Microsoft Purview Insider Risk Management.
  Créer des politiques de gestion des risques internes.
  Gérer les alertes et les cas de gestion des risques internes.

Mettre en œuvre les barrières d’information Microsoft Purview

- Décrire comment les barrières d’information peuvent restreindre ou permettre la communication et la collaboration entre des groupes spécifiques d’utilisateurs.
  Décrire les composants d’une barrière d’information et comment l’activer.
  Découvrir comment les barrières d’information aident à déterminer quels utilisateurs ajouter ou supprimer d’un compte Microsoft Team, OneDrive et d’un site SharePoint.
  Décrire comment les barrières d’information empêchent les utilisateurs ou les groupes de communiquer et de collaborer dans Microsoft Teams, OneDrive et SharePoint.

Découvrir la prevention contre la perte des données Microsoft Purview

- Décrire comment la prévention de la perte de données (DLP) est gérée dans Microsoft 365.
  Comprendre comment DLP dans Microsoft 365 utilise les types d’informations sensibles et les modèles de recherche.
  Etendre les capacités de surveillance et de protection des activités DLP avec Microsoft Endpoint DLP.
  Décrire ce qu’est une politique DLP et ce qu’elle contient.
  Afficher les résultats de la stratégie DLP à l’aide de requêtes et de rapports.
  Comprendre comment la protection adaptative intègre la gestion des risques internes avec DLP.

Mettre en œuvre la prévention des pertes de données Microsoft Purview

- Créer un plan de mise en œuvre de la prévention des pertes de données.
  Créer une stratégie DLP personnalisée à partir d’un modèle DLP et à partir de zéro.
  Créer des notifications par e-mail et des conseils de stratégie pour les utilisateurs lorsqu’une règle DLP s’applique.
  Créer des conseils de stratégie pour les utilisateurs lorsqu’une règle DLP s’applique.
  Configurer les notifications par e-mail pour les stratégies DLP.

Mettre en œuvre la classification des données des informations sensibles

- Expliquer les avantages et les points faibles de la création d'un cadre de classification des données.
  Identifier comment la classification des données des éléments sensibles est gérée dans Microsoft 365.
  Utilise des classificateurs entraînables pour protéger les données sensibles avec Microsoft 365.
  Créer, puis recycler des classificateurs formables personnalisés.
  Analyser les résultats de vos classifications des données dans l'explorateur de contenu et l'explorateur d'activités.
  Implémenter l'empreinte digitale des documents pour protéger les informations sensibles envoyées via Exchange Online.

Explorer les étiquettes de sensibilité

- Classer et de protéger les données de votre organisation avec des étiquettes de confidentialité.
  Identifier les raisons d'utilisation des étiquettes de confidentialité.
  Expliquer ce qu'est une étiquette de sensibilité et ce qu'elle peut faire pour une organisation.
  Configurer la portée d'une étiquette de confidentialité.
  Classer par ordre les étiquettes de sensibilité dans votre centre d'administration.
  Décrire ce que les stratégies d'étiquetage peuvent faire.

Implémenter des étiquettes de sensibilité

- Créer une stratégie de déploiement pour implémenter des étiquettes de confidentialité qui répondent aux exigences de votre organisation.
  Activer les étiquettes de confidentialité dans SharePoint Online et OneDrive pour qu'elles puissent utiliser des fichiers chiffrés.
  Créer et configurer des étiquettes de confidentialité.
  Publier des étiquettes de confidentialité en créant une stratégie d'étiquette.
  Identifier les différences entre le retrait et la suppression des étiquettes de confidentialité.