Programme de formation
MS-101: Microsoft 365 Mobility and Security

(Préparation certification Microsoft MS-101)

DESCRIPTION DE LA FORMATION :

Cette formation aborde trois éléments essentiels de l'administration pour les entreprises utilisant Microsoft 365. Vous découvrirez la synchronisation des identités Microsoft 365, l'accent est mis sur Azure Active Directory. Ensuite, sur le bloc gestion des clients et des services de Microsoft 365 vous apprendrez à concevoir votre abonnement, configurer et gérer votre souscription Microsoft 365. Enfin, vous examinerez les principaux composants de la gestion d'Office 365. Vous découvrirez les différentes fonctionnalités d'Office 365 et apprendrez à configurer Office 365.

OBJECTIFS PEDAGOGIQUES :

A l'issue de cette formation, les participants seront en capacité de :

- Examiner les vecteurs de menace et les violations de données
- Découvrir le modèle de sécurité Zero Trust
- Explorer les solutions de sécurité dans Microsoft 365 Defender
- Examiner le score de sécurité Microsoft
- Examiner la gestion des identités privilégiées et examiner Azure Identity Protection
- Examiner la protection en ligne d'Exchange et examiner Microsoft Defender pour Office 365
- Gérer les pièces jointes sécurisées et gérer des liens fiables
- Explorer les renseignements sur les menaces dans Microsoft 365 Defender
- Implémenter la protection des applications à l'aide de Microsoft Defender pour les applications cloud
- Implémenter la protection des points de terminaison à l'aide de Microsoft Defender pour point de terminaison
- Implémenter la protection contre les menaces à l'aide de Microsoft Defender pour Office 365
- Examiner les solutions de gouvernance et de conformité dans Microsoft Purview
- Explorer l'archivage et la gestion des enregistrements dans Microsoft 365
- Explorer la rétention dans Microsoft 365
- Découvrir le chiffrement des messages Microsoft Purview
  Explorer la conformité dans Microsoft 365
- Mettre en œuvre la gestion des risques Microsoft Purview Insider
- Créer des barrières d'informations dans Microsoft 365
- Explorer la prévention des pertes de données dans Microsoft 365
- Mettre en œuvre des politiques de prévention de la perte de données
- Mettre en œuvre la classification des données des informations sensibles
- Explorer les étiquettes de sensibilité et mettre en œuvre des étiquettes de sensibilité
- Rechercher du contenu dans le portail de conformité Microsoft Purview

- Gérer l'audit Microsoft Purview (standard) et gérer l'audit Microsoft Purview (Premium)
- Gérer Microsoft Purview eDiscovery (standard) et gérer Microsoft Purview eDiscovery (Premium)
- Explorer la gestion des appareils à l'aide de Microsoft Endpoint Manager
- Préparer vos appareils Windows pour la cogestion
- Planifier la gestion des applications mobiles dans Microsoft Intune
- Examiner les scénarios de déploiement du client Windows
- Explorer des modèles de déploiement Windows Autopilot
- Planifier votre stratégie d'activation d'abonnement client Windows
- Explorer la gestion des appareils mobiles et déployer la gestion des appareils mobiles
- Inscrire des appareils à la gestion des appareils mobiles et gérer la conformité des appareils
- Implémenter la sécurité des terminaux dans Microsoft Intune

MÉTHODES & 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 sera remis aux participants au format électronique.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Prérequis évalués avant la formation, questions régulières, travaux pratiques, QCM ou autres méthodes).
- Formateur : le tout animé par un formateur expérimenté 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.
- Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
- Cette formation peut être dispensée en format inter-entreprises ou intra-entreprise sur demande et en mode présentiel comme en distanciel.

PROGRAMME DE FORMATION :

Examiner les vecteurs de menace et les violations de données

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

Découvrir le modèle de sécurité Zero Trust

- Décrire l'approche Zero Trust de la sécurité dans Microsoft 365.
- Décrire les principes et les composants du modèle de sécurité Zero Trust.
- Décrire les 5 étapes de mise en œuvre d'un modèle Zero Trust dans son organisation.
- Expliquer l'histoire et la stratégie de Microsoft autour du réseau Zero Trust.

Explorer les solutions de sécurité dans Microsoft 365 Defender

- Identifier les fonctionnalités de Microsoft Defender pour Office 365 améliorant la sécurité de la messagerie dans un déploiement Microsoft 365.
- Prévenir, détecter, enquêter et répondre aux menaces avec Microsoft Defender pour Endpoint.
- Identifier, détecter et enquêter sur les menaces, les identités compromises et les actions internes malveillantes dirigées contre son organisation avec Microsoft Defender pour Identity.

- Décrire comment Microsoft 365 Threat Intelligence peut être bénéfique pour les responsables de la sécurité et les administrateurs de votre organisation.
- Décrire comment Microsoft Cloud App Security améliore la visibilité et le contrôle sur votre locataire Microsoft 365 à travers trois domaines principaux.

Examiner le score de sécurité Microsoft

- Décrire les avantages de Secure Score et quels types de services peuvent être analysés.
- Décrire comment 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 augmenteront votre sécurité en atténuant les risques.
- Expliquer où chercher pour déterminer les menaces que chaque action atténuera et l'impact qu'elle a sur les utilisateurs.

Examiner la gestion des identités privilégiées

- Gérer, contrôler et surveiller l'accès aux ressources importantes de votre organisation avec Privileged Identity Management.
- Configurer Privileged Identity Management pour une utilisation dans votre organisation.
- Décrire comment l'historique d'audit de Privileged Identity Management vous permet de voir les affectations et activations d'utilisateurs au cours d'une période donnée pour les rôles privilégiés.
- Gérer les utilisateurs, les informations d'identification, les politiques et l'accès au sein de leurs organisations et des environnements hybrides avec Microsoft Identity Manager.
- Fournir un contrôle d'accès granulaire sur les tâches d'administration privilégiées dans Microsoft 365 avec Privileged Access Management.

Examiner Azure Identity Protection

- 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 l'environnement Azure Active Directory contre les failles de sécurité.

Examiner la protection en ligne d'Exchange

- Analyser les e-mails pour fournir une protection contre les programmes malveillants avec Exchange Online Protection.
- Répertorier plusieurs mécanismes utilisés par Exchange Online Protection pour filtrer le spam et les logiciels malveillants.
- Aider les administrateurs à fournir une protection supplémentaire contre le phishing et l'usurpation d'identité.
- Comprendre comment EOP offre une protection contre le spam sortant.

Examiner Microsoft Defender pour Office 365

- Décrire comment la fonctionnalité de pièces jointes approuvées dans Microsoft Defender pour Office 365 bloque les logiciels malveillants de type « zero-day » dans les PJ et les documents.
- Décrire comment la fonctionnalité de liens fiables dans Microsoft Defender pour Office 365 protège les utilisateurs contre les URL malveillantes intégrées dans les e-mails et les documents qui pointent vers des sites Web malveillants.
- Créer des politiques de filtrage des spams sortants.

- Débloquer les utilisateurs qui ont enfreint les politiques de filtrage anti-spam afin qu'ils puissent reprendre l'envoi d'e-mails.

Gérer les pièces jointes sécurisées

- Créer et modifier une stratégie de pièces jointes approuvées à l'aide de Microsoft 365 Defender.
- Créer une stratégie de pièces jointes approuvées à l'aide de PowerShell.
- Configurer une stratégie de pièces jointes approuvées.
- Décrire comment une règle de transport désactive une stratégie de pièces jointes approuvées.
- Décrire l'expérience de l'utilisateur lorsqu'une pièce jointe est analysée et jugée malveillante.

Gérer des liens fiables

- Créer et modifier une stratégie de liens fiables à l'aide de Microsoft 365 Defender.
- Créer une stratégie de liens fiables à l'aide de PowerShell.
- Configurer une stratégie de liens fiables.
- Décrire comment une règle de transport peut désactiver une stratégie de liens fiables.
- Décrire l'expérience utilisateur 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 le web.

Explorer les renseignements sur les menaces dans Microsoft 365 Defender

- Décrire comment les renseignements sur les menaces dans Microsoft 365 sont optimisés par 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 365 Defender.
- Décrire comment la chasse aux menaces permet aux opérateurs de sécurité d'identifier les menaces de cybersécurité.
- Décrire comment la recherche avancée dans Microsoft 365 Defender inspecte proactivement 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

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

Implémenter la protection des points de terminaison à l'aide de Microsoft Defender

- Décrire comment Microsoft Defender pour Endpoint aide les réseaux d'entreprise à prévenir, détecter, enquêter et répondre aux menaces avancées.
- Implémenter le module de gestion des menaces et des vulnérabilités pour identifier, évaluer et corriger efficacement les faiblesses des terminaux.
- Configurer la découverte d'appareils pour trouver des appareils non gérés connectés à votre réseau d'entreprise.
- Réduire l'exposition aux menaces et aux vulnérabilités de votre organisation en corrigeant les problèmes en fonction des recommandations de sécurité hiérarchisées.
- Intégrer les appareils pris en charge à Microsoft Defender pour Endpoint.

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 qui vous fournissent 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 et de conformité dans Microsoft Purview

- Protéger les données sensibles avec Microsoft Purview Information Protection.
- Gérer 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.

Explorer l'archivage et la gestion des enregistrements 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.
- Utiliser les étiquettes de rétention pour autoriser ou bloquer des actions lorsque des documents et des e-mails sont déclarés enregistrements.
- Créer votre plan de fichiers pour les paramètres et les actions de conservation et de suppression.
- Déterminer quand les éléments doivent être marqués comme enregistrements en important un plan existant (si vous en avez déjà un) ou créez de nouvelles étiquettes de rétention.
- Restaurer les données supprimées dans Exchange Online et SharePoint Online.

Explorer la rétention dans Microsoft 365

- Expliquer le fonctionnement des stratégies 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.
- Expliquer les principes de la rétention.
- Identifier les différences entre les paramètres de rétention et les conservations eDiscovery.
- Restreindre les modifications de conservation en utilisant le verrouillage de conservation.

Découvrir le chiffrement des messages Microsoft Purview

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

Explorer la conformité dans Microsoft 365

- Gérer les risques, protéger les données et rester en conformité avec les réglementations et les normes grâce à 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.

Créer des barrières d'informations dans Microsoft 365

- 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 à l'information et activer les barrières à l'information.
- Découvrir comment les modes de barrière des informations aident à renforcer qui peut être ajouté ou supprimé d'une équipe Microsoft, d'un compte OneDrive et d'un site SharePoint.
- Empêcher les utilisateurs ou groupes de communiquer grâce aux barrières d'informations.

Explorer la prévention des pertes de données dans Microsoft 365

- Décrire comment la prévention de la perte de données (DLP) est gérée dans Microsoft 365.
- Utilise les types d'informations sensibles et les modèles de recherche dans Microsoft 365.
- Etendre les capacités de surveillance et protection des activités grâce à 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.

Mettre en œuvre des politiques de prévention de la perte de données

- Créer un plan de mise en œuvre de la prévention des pertes de données.
- Implémentez la stratégie DLP par défaut de Microsoft 365.
- 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 points faibles de la création d'un cadre de classification des données.
- Identifier la classification des données des éléments sensibles dans Microsoft 365.
- Utiliser des classificateurs entraînables pour protéger la donnée sensible avec Microsoft 365.
- Créer, puis recycler des classificateurs formables personnalisés.
- Analyser les résultats de vos efforts de classification 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 protéger les données de votre organisation grâce aux étiquettes de confidentialité.
- Identifier les raisons pour lesquelles les organisations utilisent 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 sensibilité.

- Expliquer l'importance de l'ordre des étiquettes de sensibilité dans votre centre d'administration.
- Décrire ce que les stratégies d'étiquetage peuvent faire.

Mettre en œuvre des étiquettes de sensibilité

- Décrire le processus global de création, de configuration et de publication d'étiquettes de confidentialité.
- Identifier les autorisations administratives qui doivent être attribuées aux membres de l'équipe de conformité pour mettre en œuvre les étiquettes de confidentialité.
- Développer un cadre de classification des données qui constitue la base de vos étiquettes de sensibilité.
- Créer et configurer des étiquettes de confidentialité.
- Publier des étiquettes de confidentialité en créant une stratégie d'étiquette.
- Identifier les différences entre la suppression et la suppression des étiquettes de sensibilité.

Rechercher du contenu dans le portail de conformité Microsoft Purview

- Utiliser la recherche de contenu dans le portail de conformité Microsoft Purview.
- Concevoir et créer une recherche de contenu.
- Prévisualiser les résultats de la recherche.
- Afficher les statistiques de recherche.
- Exporter les résultats de la recherche et le rapport de recherche.
- Configurer le filtrage des autorisations de recherche.

Gérer l'audit Microsoft Purview (standard)

- Décrire les différences entre Audit (Standard) et Audit (Premium).
- Identifier les principales fonctionnalités de la solution Audit (Standard).
- Configurer et implémenter la recherche dans les journaux d'audit à l'aide de la solution Audit
- Exporter, configurez et affichez les enregistrements du journal d'audit.
- Utiliser la recherche dans le journal d'audit pour résoudre les problèmes de support courants.

Gérer l'audit Microsoft Purview (Premium)

- Décrire les différences entre Audit (Standard) et Audit (Premium).
- Configurer et mettre en œuvre Microsoft Purview Audit (Premium).
- Créer des stratégies de conservation des journaux d'audit.
- Effectuer des enquêtes médico-légales sur les comptes d'utilisateurs compromis.

Gérer Microsoft Purview eDiscovery (standard)

- Décrire comment Microsoft Purview eDiscovery (Standard) s'appuie sur la fonctionnalité de recherche et d'exportation de base de la recherche de contenu.
- Décrire le flux de travail de base d'eDiscovery (Standard).
- Créer un cas eDiscovery.
- Créer une suspension eDiscovery pour un cas eDiscovery.
- Rechercher du contenu dans une requête, puis exportez ce contenu.
- Fermer, rouvrir et supprimer un cas.

Gérer Microsoft Purview eDiscovery (Premium)

- Décrire comment Microsoft Purview eDiscovery (Premium) s'appuie sur eDiscovery (Standard).
- Décrire le flux de travail de base d'eDiscovery (Premium).
- Créer et gérez des cas dans eDiscovery (Premium).

- Gérer les dépositaires et les sources de données non-dépositaires.
- Analyser le contenu des requêtes et utiliser des outils d'analyse pour réduire la taille des ensembles de résultats de recherche.

Explorer la gestion des appareils à l'aide de Microsoft Endpoint Manager

- Décrire les fonctionnalités de gestion des appareils trouvées dans Microsoft Endpoint Manager.
- Décrire comment les appareils Windows peuvent être cogérés dans Endpoint Manager à l'aide de Configuration Manager et Intune.
- Gérer les appareils à l'aide de Configuration Manager et de Microsoft Intune.
- Créer des profils d'appareils dans Microsoft Intune.

Préparer vos appareils Windows pour la cogestion

- Décrire les conditions préalables à l'utilisation de la cogestion.
- Configurer Microsoft Endpoint Configuration Manager pour la cogestion.
- Inscrire des appareils Windows 10 à Intune.

Planifier la gestion des applications mobiles dans Microsoft Intune

- Décrire les fonctionnalités de base de la gestion des applications mobiles dans Microsoft Intune.
- Évaluer les exigences de votre application et ajoutez des applications dans Intune.
- Protéger les données d'entreprise à l'aide de stratégies de protection des applications.
- Implémenter des stratégies de configuration d'application dans Intune pour éliminer les problèmes d'installation d'application.
- Résoudre des problèmes de déploiement de la stratégie de protection des applications dans Intune.

Examiner les scénarios de déploiement du client Windows

- Expliquer comment le modèle Windows as a Service fournit continuellement de nouvelles fonctionnalités et mises à jour tout en maintenant un haut niveau de compatibilité matérielle et logicielle.
- Expliquer comment le modèle de déploiement de Windows 10/11 combine les services classiques locaux et cloud pour une expérience de déploiement rationalisée et rentable.
- Expliquer comment le modèle de déploiement dynamique de Windows 10/11 peut transformer la version de Windows 10/11 incluse sur un appareil en une version personnalisée utilisée dans votre entreprise sans réinstaller Windows.

Explorer des modèles de déploiement Windows Autopilot

- Décrire les exigences de déploiement de Windows Autopilot.
- Créer et attribuer un profil Windows Autopilot.
- Expliquer comment le modèle d'auto-déploiement Autopilot déploie Windows 10 et 11 avec peu ou pas d'interaction avec l'utilisateur.
- Expliquer comment le modèle de déploiement préprovisionné Autopilot permet aux utilisateurs finaux de provisionner de nouveaux appareils en utilisant l'image OEM et les pilotes préinstallés.
- Déployer un modèle piloté par l'utilisation Autopilot pour transformer les nouveaux appareils Windows10 et 11 à partir de leur état par défaut sans exiger que le personnel informatique touche l'appareil.
- Déployer le cryptage BitLocker pour les appareils en pilotage automatique.

Planifier votre stratégie d'activation d'abonnement client Windows

- Décrire l'achat des abonnements Windows 10/11 Entreprise E3 via le fournisseur cloud.
- Configurer Virtual Desktop Access pour l'activation automatique des abonnements sur les VM.
- Déployer automatiquement les licences Windows 10/11 Entreprise sans redémarrage de l'appareil.
-

Explorer la gestion des appareils mobiles

- Décrire les deux solutions d'autorité MDM incluses dans Microsoft 365 - Microsoft Intune et Basic Mobility and Security.
- Comparer les fonctionnalités de base de Microsoft Intune et de Basic Mobility and Security.
- Décrire les paramètres de stratégie pour les appareils mobiles dans Microsoft Intune et Basic Mobility and Security.
- Contrôler l'accès aux e-mails et aux documents avec les appareils gérés par MDM.

Déployer la gestion des appareils mobiles

- Activer et déployer les services de gestion des appareils mobiles dans Microsoft 365.
- Configurer des domaines pour MDM en ajoutant des enregistrements DNS pour que les clients utilisent la découverte automatique lors de l'inscription d'appareils.
- Obtenir un certificat APNS pour inscrire et gérer les appareils Ios.
- Gérer les politiques de sécurité de l'appareil qui peuvent contrôler les paramètres de mot de passe, les paramètres de cryptage et les paramètres qui contrôlent l'utilisation des fonctionnalités de l'appareil.
- Définir une politique d'inscription d'appareils d'entreprise qui peut limiter l'inscription et activer l'authentification multifacteur.

Inscrire des appareils à la gestion des appareils mobiles

- Inscrire des appareils à la gestion des appareils mobiles dans Microsoft Intune.
- Explorer l'utilisation des appareils Azure AD joints et hybrides joints à Azure AD.
- Expliquer comment les utilisateurs peuvent inscrire leurs appareils personnels.
- Décrire les bonnes pratiques et fonctionnalités pour chaque méthode d'inscription d'appareil.
- Configurer l'inscription pour les appareils Windows.

Gérer la conformité des appareils

- Planifier la conformité des appareils en définissant les règles et les paramètres qui doivent être configurés sur un appareil pour qu'il soit considéré comme conforme.
- Configurer des utilisateurs et des groupes conditionnels pour déployer des profils, des stratégies et des applications.
- Créer des stratégies d'accès conditionnel pour automatiser les décisions de contrôle d'accès aux applications cloud.
- Surveiller les appareils inscrits pour contrôler leurs activités Intune et leur état de conformité.

Implémenter la sécurité des terminaux dans Microsoft Intune

- Protéger leurs données et leurs appareils avec Microsoft Intune.
- Sécuriser des points de terminaison dans Microsoft Intune pour protéger les appareils et à atténuer les risques.
- Gérer les appareils avec la sécurité des points de terminaison dans Intune.
- Utiliser des lignes de base de sécurité pour configurer les appareils Windows dans Intune.
- Mettre en place des règles de réduction de la surface d'attaque pour protéger l'organisation.

PRÉREQUIS :

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). Les candidats doivent aussi 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, les candidats doivent avoir suivi la formation "MS-100 : Microsoft 365 Identity and Services" ou détenir un niveau équivalent.

Un niveau d'anglais B1 est requis, retrouvez les niveaux sur ce lien : Classification des niveaux de langue

PRE-CERTIFCIATION :

Cette formation prépare à l'examen de certification Microsoft MS-101 « Microsoft 365 Mobility and Security »

DUREE : 5 jours (35 heures)

INTERLOCUTEURS : Administrateurs

NIVEAU : Intermédiaire