

| | | |
|--|--------------------|-----------------------------------|
| Référence : MS-DEFENDER | Niveau : Avancé | Prochaines sessions |
| Durée : 2 jours | Tarif : 1 500,00 € | Intra à distance. |
| Nombre de participants par session : 8 maximum | | Intra sur site. |
| Pour toutes demandes concernant cette formation Nous Contacter | | |

La plateforme Microsoft 365 centralise les données des entreprises dans différentes applications qui stockent les données de l'entreprise.

Les données de l'entreprise doivent être suivies et maîtrisées selon des règles de sécurité qui sont mises en place par les services de sécurité.

Afin de vérifier et de contrôler l'application des procédures de sécurité un centre d'administration dédié à la sécurité et à ce métier est apparu dans Microsoft 365.

L'objectif de centre est de permettre aux services de conformité d'administrer et de contrôler la bonne application des règles définies au sein de l'entreprise.

Etant donné le caractère "ouvert" de la plateforme et son exposition possible, le centre de sécurité est l'outil principal pour contrôler et détecter les menaces .

Cette formation permet à un service de conformité ou d'audit interne, DPO, RSSI et à toute personne en charge de la sécurité de connaître les outils et les possibilités offertes par la plateforme dans ce domaine. Pour être à même dans un second temps de fixer les règles et les procédures à suivre dans le cadre de la sécurité.

Public

Service de sécurité ou de cybersécurité.
Administrateur de plateforme Microsoft 365

Pré-requis

Expérience de l'administration et de la sécurité d'un système d'information.
Connaissances de la plateforme Microsoft 365.

Avant ce Stage

[Administration des services Microsoft 365](#)

Après ce Stage

[Gestion de la conformité dans Microsoft 365 PurView](#)

Pédagogie

50 % de cours et démonstrations / 50% de mise en pratique

Objectifs

- Comprendre le centre de sécurité Microsoft 365

- Etre en mesure de sécuriser les identités
- Détecter et répondre aux menaces
- Protéger les informations dans Microsoft 365
- Conduire des simulations d'attaques
- Sécuriser les applications cloud
- Crypter les contenus

Profil de l'animateur

Consultant expert, certifié Microsoft 365

Méthode d'évaluation

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation.

L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.

Module 1 - Présentation de Microsoft 365 Defender

- Vue d'ensemble des services Defender
- Conditions préalables
- Vue d'ensemble

Travaux Pratiques

- Mise en place de la plateforme M365
- Activation des services Defender

Module 2 - Sécurisation des identités

- Gouvernance des identités
- Azure AD Identity Protection
- Privileged Identity Management

Travaux Pratiques

- Administration des groupes Microsoft 365
- Configuration de la réinitialisation des mots de passes
- Configuration de Azure ADM Smart Lockout

Module 3 - Sécurité dans Microsoft 365

- Vecteurs de menaces et failles
- posture de sécurité et bonnes pratiques
- Services Defender de protection
- Score de sécurité

Travaux Pratiques

- Création d'une règle d'accès conditionnelle
- Mise en place de PIM et affectations de rôles
- Désactivation de rôles
- Suivi de l'affectation des rôles et alertes

Module 4 - Protections contre les menaces

- Exchange Online Protection (EOP)
- Defender pour Office 365
- Gestion des pièces jointes, des liens sécurisés
- Defender for Identity, for EndPoint
- Simulation d'attaques

Travaux Pratiques

- Amélioration du score de sécurité
- Mise en place de stratégies de sécurité ATP
- Créer une simulation d'attaque d'usurpation d'identité

Module 5 - Gestion des menaces

- Tableau de bord de sécurité
- Répondre et détecter les menaces
- Azure Sentinel
- Analyse Avancée des menaces
- Activation de la simulation et analyse des résultats

Travaux Pratiques

- Conduire une simulation d'attaque d'usurpation d'identité
- Analyse de la réaction des utilisateurs ciblés

Module 6 - Sécurité des applications cloud

- Déploiement de Cloud Application Security
- Administration et suivi des applications cloud

Travaux Pratiques

- Autorisation d'une application d'entreprise
- Choix du mode de consentement utilisateur
- Désactivation des consentements utilisateurs

Module 7 - IRM et Cryptages des données

- Présentation d'Information Rights Management
- Configuration du S-MIME
- Cryptage dans Office 365

Travaux Pratiques

- Configuration du cryptage Microsoft 365
- Vérification du fonctionnement IRM dans Exchange et SharePoint

Clôture de Stage

Rappel en synthèse de la formation, votre avis sur la formation et vos suggestions.