Microsoft 365 - Administration de la sécurité Microsoft 365

Référence MS500

5 jours - 35 heures

Session sur demande

Niveau intermédiaire

Cours officiel Microsoft

Présentiel

Cas pratiques

INTER 2500€ HT/ pers.
INTRA - Tarif sur demande

Taux de satisfaction -

Taux de réussite -

Présentation

Apprenez à travers cette formation comment mettre en oeuvre, gérer et surveiller les solutions de sécurité et de conformité Microsoft 365.
La formation est basée sur le cours officiel Microsoft.

Public et prérequis

- Public: Administrateur, Administrateur poste de travail, Administrateur Microsoft
- Prérequis: avoir des connaissances de base Microsoft 365 ou avoir suivi la formation MS900 - Fondamentaux Microsoft 365; Avoir une expérience de Windows 10; Maitriser l'anglais technique

Objectifs

- Mettre en œuvre, gérer les identités et administrer les accès,
- Mettre en œuvre et gérer la protection contre les menaces,
- Mettre en œuvre et gérer la protection des informations
- Gérer les options de gouvernance et de conformité dans Microsoft 365.

Programme

Jour 1

Module 1 : Implement and manage identity and access

- Identify core Microsoft 365 capabilities
- Describe options for deploying and supporting Windows and Office
- Describe analytics capabilities in Microsoft 365

Jour 2

Suite module 1

- Describe Microsoft 365 collaboration solutions
- Implement roles and role groups
- Configure and manage identity governance
- Implement Azure AD Identity Protection

Jour 3

Module 2 : Implement and manage threat protection

- Implement and manage Microsoft Defender for Identity
- Implement device threat protection
- Implement and manage device and application protection

Jour 4

Module 3: Implement and manage information protection

- Manage sensitive information
- Manage Data Loss Prevention (DLP)
- Manage data governance and retention

Jour 5

Module 4 : Manage governance and compliance features in Microsoft 365

- Configure and analyze security reporting
- Manage and analyze audit logs and reports
- Discover and respond to compliance queries in Microsoft 365
- Manage regulatory compliance
- Manage insider risk solutions in Microsoft 365

N° de déclaration d'activité 32591118259

Programme détaillé

Implement and manage identity and access

Secure Microsoft 365 hybrid environments
• plan Azure AD authentication options
• plan Azure AD synchronization options
• monitor and troubleshoot Azure AD Connect events

Secure Identities
• implement Azure AD group membership
• implement password management
• manage external identities in Azure AD and Microsoft 365 workloads

Implement authentication methods
• implement multi-factor authentication (MFA) by using conditional access policy
• manage and monitor MFA
• plan and implement device authentication methods like Windows Hello

Implement conditional access
• plan for compliance and conditional access policies
• configure and manage device compliance policies
• implement and manage conditional access
• test and troubleshoot conditional access policies

Implement roles and role groups
• plan for roles and role groups
• configure roles and role groups
• audit roles for least privileged access

Configure and manage identity governance
• implement Azure AD Privileged Identity Management
• implement and manage entitlement management
• implement and manage access reviews

Implement Azure AD Identity Protection
• implement user risk policy
• implement sign-in risk policy
• configure Identity Protection alerts
• review and respond to risk events

Implement and manage threat protection

Implement and manage Microsoft Defender for Identity
• plan a Microsoft Defender for Identity solution
• install and configure Microsoft Defender for Identity
• monitor and manage Microsoft Defender for Identity

Implement device threat protection
• plan a Microsoft Defender for Endpoint solution
• implement Microsoft Defender for Endpoint
• manage and monitor Microsoft Defender for Endpoint

Implement and manage device and application protection
• plan for device and application protection
• configure and manage Microsoft Defender Application Guard
• configure and manage Microsoft Defender Application Control
• configure and manage exploit protection
• configure and manage Windows device encryption
• configure and manage non-Windows device encryption
• implement application protection policies
• configure and manage device compliance for endpoint security

Implement and manage Microsoft Defender for Office 365
• configure Microsoft Defender for Office 365
• monitor for and remediate threats using Microsoft Defender for Office 365
• conduct simulated attacks using Attack simulation training

Monitor Microsoft 365 Security with Microsoft Sentinel
• plan and implement Microsoft Sentinel
• configure playbooks in Microsoft Sentinel
• manage and monitor with Microsoft Sentinel
• respond to threats using built-in playbooks in Microsoft Sentinel

Implement and manage Microsoft Defender for Cloud Apps
• plan Microsoft Defender for Cloud Apps implementation
• configure Microsoft Defender for Cloud Apps
• manage cloud app discovery
• manage entries in the Microsoft Defender for Cloud Apps catalog
• manage apps in Microsoft Defender for Cloud Apps
• configure Microsoft Defender Cloud Apps connectors and OAuth apps
• configure Microsoft Defender for Cloud Apps policies and templates
review, interpret and respond to Microsoft Defender for Cloud Apps alerts, reports,
dashboards, and logs

Implement and manage information protection

Manage sensitive information
• plan a sensitivity label solution
• create and manage sensitive information types
• configure sensitivity labels and policies.
• configure and use Activity Explorer
• use sensitivity labels with Teams, SharePoint, OneDrive and Office apps

Manage Data Loss Prevention (DLP)
• plan a DLP solution
• create and manage DLP policies for Microsoft 365 workloads
• create and manage sensitive information types
• monitor DLP reports
• manage DLP notifications
• implement Endpoint DLP

Manage data governance and retention
• plan for data governance and retention
• review and interpret data governance reports and dashboards
• configure retention labels and policies
• configure retention in Microsoft 365 workloads
• find and recover deleted Office 365 data
• configure and use Microsoft 365 Records Management

Manage governance and compliance features in Microsoft 365

Configure and analyze security reporting
• monitor and manage device security status using Microsoft Endpoint Manager admin center
• manage and monitor security reports and dashboards using Microsoft 365 Defender portal
• plan for custom security reporting with Graph Security API
• use secure score dashboards to review actions and recommendations

Manage and analyze audit logs and reports
• plan for auditing and reporting
• perform audit log search
• review and interpret compliance reports and dashboards
• configure alert policies

Discover and respond to compliance queries in Microsoft 365
• plan for content search and eDiscovery
• delegate permissions to use search and discovery tools
• use search and investigation tools to discover and respond
• manage eDiscovery cases

Manage regulatory compliance
• plan for regulatory compliance in Microsoft 365
• manage Data Subject Requests (DSRs)
• administer Compliance Manager in Microsoft 365 compliance center
• use Compliance Manager

Manage insider risk solutions in Microsoft 365
• implement and manage Customer Lockbox
• implement and manage communication compliance policies
• implement and manage Insider risk management policies
• implement and manage information barrier policies
• implement and manage privileged access management

Organisation

Accessibilité & Modalités d'accès :

La salle formation se situe chez sumit au sein du centre Régus de Villeneuve d'Ascq.
Les locaux et équipements sont adaptés aux personnes à mobilité réduite. N'hésitez pas à nous contacter pour toute demande spécifique.
La responsable pédagogique et le formateur sont en charge de l'accueil des stagiaires.

Moyens pédagogiques, techniques et d'encadrement :

sumit garantit la mise à disposition de :

- *1 salle équipée d'un projecteur ou écran permettant la diffusion des supports de formation*
- *1 tableau blanc avec fournitures nécessaires*

La formation est dispensée par un formateur dans une salle de cours, en présentiel.

Modalités spécifiques :

- *Chaque stagiaire dispose de son propre poste de travail adapté aux besoins de la formation.*

Méthodes mobilisées :

Le formateur alterne entre théorie, cas pratiques, et jeux de questions/réponses pour faire participer les stagiaires.

Modalités d'évaluation :

Nous réalisons un test QCM avec auto-positionnement à l'entrée et à la sortie de la formation afin de s'assurer de la maitrise des prérequis listés et d'évaluer la bonne assimilation des notions abordées en formation.

Notre formateur

Le formateur sumit qui anime cette session de formation est un consultant confirmé sur son domaine de compétences.

Valentin

Technical Leader

9 ans d'expérience

Certifié
Microsoft Certified Trainer (MCT)
Azure Solutions Architect Expert,
Teams Administrator Associate,
MS365 Developer Associate,
Devops Engineer Expert

Votre contact commercial

Coraline Gaippe** - **Chargée de Développement Formation
06 59 45 29 95 - formation@sumit.fr