VMware vSphere - Manage and Design for Security

Durée	**3 jours**	**Référence Formation**	**4-VS-MDS**

Objectifs

Cette formation présente les meilleures pratiques pour concevoir, déployer et gérer la sécurité dans un environnement VMware vSphere. Il est nécessaire d'avoir les compétences de base sur vSphere 4 afin de profiter pleinement du contenu de cette formation.

Participants

Pré-requis

Administrateur système, ingénieurs systèmes et consultants responsable de la mise en place de la sécurité lors d'une installation vSphere.

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants
Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME

Module 1: Introduction
- Plan de la formation
- Ressource en ligne autour de la sécurité et de la conformité

Module 2: Sécurité d'un environnement virtuel
- Revue des concepts de sécurité et de gestion des risques
- Comment la virtualisation impacte la sécurité et la conformité
- Les principales vulnérabilités dans un environnement virtuel
- Les principes de base pour sécuriser un environnement virtuel

- Les outils et technologies de sécurité

Module 3: Réseau virtuel sécurisé
- vNetwork : architecture securisé
- Segmentation du réseau et isolation du traffic
- Configuration d'un réseau virtuel sécurisé
- Isolation du trafic avec les : «private VLANs»

Module 4: Protection des modes de gestion de l'environnement
- Autentification avec vCenter Server, privilèges et autorisations avec certificat SSL
- Renforcement du système vCenter Server

Module 5: Protection des VMware ESX/ESXi Host Systems
- Architecture sécurisée ESX et ESXi
- Contrôle de l'accès au stockage
- Renforcement des ESX et ESXi

Module 6: Renforcement des machines virtuelles
- Architecture sécurisée des machines virtuelles
- Configuration des paramètres de sécurités

Module 7: Gestion de la configuration et des changements
- Gestion de la configuration et des changement : guides et objectifs
- Maintient de la configuration adéquate des composants vSphere
- Suivi des logs liés aux événements de sécurité
- Gestion de la configuration et des changements : outils et technologies