

Objectif

À la fin de ce cours pratique, les stagiaires seront à même d'effectuer les tâches suivantes :

- définir la justification économique de la sécurité pour l'entreprise ;
- appliquer la gestion des risques de sécurité pour faire en sorte qu'une entreprise devienne et reste aussi sécurisée que possible ;
- utiliser plusieurs couches de défense pour réduire au minimum les chances de succès des attaques visant une organisation ;
- réagir efficacement aux incidents de sécurité ;
- mettre en œuvre des méthodes conseillées pour améliorer au maximum la sécurité d'un environnement réseau ;
- décrire les dix règles immuables de la sécurité ;
- comprendre les processus développés par Microsoft pour répondre aux attaques contre les systèmes, ainsi que la manière d'appliquer une stratégie de gestion des correctifs efficace ;
- utiliser les outils et processus de gestion des correctifs pour mettre en œuvre la gestion de correctifs dans leur organisation ;
- décrire la stratégie adoptée par Microsoft pour continuer de fournir à ses clients des outils, des technologies et des informations sans cesse améliorés pour la gestion des correctifs ;
- comprendre l'importance de la sécurité des serveurs ;
- comprendre les principes de sécurité de base des serveurs ;
- utiliser la structure Active Directory appropriée et les stratégies de groupe pour gérer la sécurité des serveurs ;
- appliquer les modèles fournis dans le guide Windows Server 2003 Security Guide pour renforcer la protection des serveurs ;
- gérer les paramètres de stratégie des contrôleurs de domaine ;
- renforcer la protection des serveurs pour des rôles spécifiques :
 - serveurs d'infrastructure,
 - serveurs de fichiers,
 - serveurs d'impression,
 - serveurs IIS (services Internet) ;
- renforcer la protection des serveurs autonomes ;
- comprendre les contraintes de sécurisation des ordinateurs clients dans les environnements comprenant des serveurs Windows Server 2003, Windows 2000 et Windows NT 4.0 ;
- comprendre les stratégies antivirus et les méthodes conseillées pour le déploiement des logiciels antivirus ;
- comprendre les technologies de pare-feu client et les méthodes conseillées pour la mise en œuvre d'un pare-feu client ;
- utiliser la structure Active Directory appropriée et les stratégies de groupe pour gérer la sécurité des postes de travail ;
- appliquer les modèles de sécurité fournis par le Windows XP Security Guide v2 (en anglais) pour améliorer la sécurité des ordinateurs de bureau et des portables ;
- utiliser les modèles d'administration et les méthodes conseillées permettant de sécuriser les applications ;
- utiliser une stratégie de restriction logicielle pour gérer et augmenter la sécurité des ordinateurs au sein d'une organisation ;
- utiliser des paramètres de stratégie de groupe locale pour augmenter la sécurité des postes clients autonomes.

Participant

Les participants sont des professionnels de l'informatique qui utilisent Microsoft Windows 2000 Server ou Microsoft Windows Server™ 2003 et qui connaissent les concepts de Microsoft Active Directory. Dans leurs entreprises, les stagiaires sont responsables de la gestion de la sécurité ainsi que des déploiements associés à leur infrastructure réseau interne et à des services Internet ou intranet.

Prérequis

Pour suivre ce cours pratique, les stagiaires doivent avoir une expérience pratique dans les domaines suivants :

- Expérience pratique des outils de gestion Windows 2000 ou Windows Server 2003.
- Expérience d'Active Directory et des stratégies de groupe.

Programme

1. Sécurité informatique : Notions fondamentales

Justification économique de la sécurité
Gestion des risques de sécurité
Défense en profondeur
Réponse à un incident de sécurité
10 règles immuables de sécurité
Méthodes conseillées

2. Mise en œuvre d'une gestion des mises à jour de sécurité

Vue d'ensemble de la gestion des mises à jour
Processus de gestion des mises à jour
Outils de gestion des mises à jour

3. Mise en œuvre de la sécurité de vos serveurs Windows 2000 et Windows Server 2003

Introduction à la sécurisation des serveurs
Sécurité de base des serveurs
Sécurité Active Directory
Renforcement de la protection des serveurs membres
Renforcement de la protection des contrôleurs de domaine
Renforcement de la protection des serveurs pour des rôles spécifiques
Renforcement de la protection des serveurs autonomes

4. Mise en œuvre de la sécurité de vos postes de travail Windows 2000 et Windows XP

Sécurité de base des clients
Protection contre les logiciels malveillants
Pare-feu clients
Sécurisation des clients à l'aide d'Active Directory
Utilisation d'une stratégie de groupe pour sécuriser les clients
Sécurisation des applications
Stratégie de restriction logicielle

Guide Microsoft pour la sécurité - Formation 1

1
Jour
[7 Heures]

MS2750FR



Plan de cours disponible à l'adresse <http://www.adhara.fr/MS2750FR.aspx>

Paramètres de stratégie de groupe locale pour les clients autonomes