

Symantec Endpoint Protection 11.x

DESCRIPTIF DU COURS

Le cours intitulé Symantec Endpoint Protection (SEP) 11.x est conçu pour les professionnels du réseau, de la sécurité informatique et de l'administration des systèmes, qui sont chargés de l'architecture, de l'implémentation et du contrôle des solutions antivirus et contre les logiciels espions, ainsi que des solutions de pare-feu client. Ce cours explore comment définir, déployer, installer, configurer, et contrôler Symantec Endpoint Protection 11.x.

Les participants apprendront également à créer et implémenter des politiques de pare-feu client, de prévention contre les intrusions et les comportements qui permettent de protéger l'entreprise contre les virus, les pirates et le courrier indésirable. De plus, les participants apprendront à dépanner les gestionnaires de politiques de SEP 11.x et les systèmes clients de SEP 11.x.

Mode d'administration

Cours dispensé par un formateur

Durée

Cinq jours

Objectifs du cours

A la fin de ce cours vous devriez être en mesure de :

- Décrire les menaces de sécurité auxquelles se trouvent confrontés aujourd'hui les clients des entreprises et les solutions offertes par Symantec afin d'atténuer ces risques.
- Décrire les produits, composants, dépendances de produits et la hiérarchie de système de SEP.
- Installer et configurer la gestion de SEP et les composants client.
- Gérer les politiques antivirus et contre les logiciels espions.
- Configurer la protection proactive contre les menaces.
- Etablir une stratégie de sécurité des terminaux clients.
- Contrôler et maintenir l'environnement SEP.
- Configurer les politiques de pare-feu et de prévention d'intrusion.
- Gérer les groupes, les emplacements et l'héritage.
- Gérer les composants du pare-feu client de SEP.
- Configurer la protection de prévention d'intrusion de l'hôte (HIPS).

Audience concernée

Ce cours s'adresse aux directeurs réseau, aux revendeurs, aux administrateurs système, aux administrateurs de sécurité client, aux professionnels des systèmes, et aux consultants qui sont chargés de l'installation, de la configuration et de la gestion quotidienne de Symantec Endpoint Protection dans divers environnements réseau, et qui sont responsables du dépannage des performances de SEP 11.x en entreprise.

Prérequis

De bonnes connaissances en terminologie informatique avancée, y compris la terminologie réseau TCP/IP et Internet, sont nécessaires, ainsi que des connaissances de niveau administrateur des systèmes d'exploitation Microsoft Windows 2000/XP/2003.

Formation pratique

Ce cours comprend des exercices pratiques vous permettant de tester vos nouvelles compétences et de commencer à les utiliser dans un environnement professionnel.

PLAN DU COURS

• Introduction

- Présentation du cours
- Environnement labo de la classe
-

• **Leçon 1 : Le paysage informatique actuel de la sécurité**

- Risques de sécurité
- Gestion et protection des systèmes
- Politiques de sécurité d'entreprise et diagnostics de sécurité
-

• **Leçon 2 : La solution du produit Symantec Endpoint Protection**

- Symantec Endpoint Protection
- Groupes, héritage, emplacement et politiques
- Mode de communication des clients avec les serveurs
-

• **Leçon 3 : Installation de SEP**

- Identification de la configuration logicielle requise

- Préparation des serveurs et clients
- Installation de Symantec Endpoint Protection Manager (SEPM)
- Navigation dans Symantec Endpoint Protection Manager (SEPM)
- **Leçon 4 : Déploiement des clients**
 - Préparation de l'installation des clients
 - Choix de la méthode d'installation des clients
 - Réalisation de l'installation
 - Analyse des clients
 - Gestion de l'environnement de l'utilisateur final
- **Leçon 5 : Adaptation de SEP 11.x pour des déploiements à plus grande échelle**
 - Installation d'un serveur LiveUpdate central
 - Configuration de LiveUpdate
 - Installation et configuration de la quarantaine
 - Ouverture de l'environnement de gestion
 -
- **Leçon 6 : Configuration des politiques antivirus et de protection contre les logiciels espions**
 - Définition de paramètres de sécurité générale
 - Types d'analyse
 - Configuration des analyses Auto-Protect pour le système de fichiers
 - Configuration des analyses antivirus
 - Mise en quarantaine de fichiers
 -
- **Leçon 7 : Configuration d'une protection complémentaire**
 - Différences de protection proactive contre les menaces
 - Configuration de l'analyse de protection proactive contre les menaces
 - Gestion des journaux d'affichage de la protection proactive contre les menaces
 - Modification de la politique de protection contre les interventions par défaut
 - Configuration des exceptions centralisées
 - Mise en quarantaine de fichiers
 -
- **Leçon 8 : Réalisation de la gestion du serveur et de la base de données**
 - Gestion du certificat du serveur
 - Configuration d'un client RSA
 - Configuration des paramètres de SEPM
 - Communication avec d'autres serveurs
 - Importation et exportation des paramètres de serveur
 - Ajout d'administrateurs
 - Gestion de la base de données
 -
- **Leçon 9 : Contrôle de votre environnement antivirus et de protection proactive contre les menaces**
 - Affichage des journaux
 - Affichage des notifications
 - Configuration et affichage des journaux
 -
- **Leçon 10 : Conception d'une stratégie de sécurité des terminaux clients**
 - Critères clés de déploiement
 - Conception d'un exemple de stratégie de déploiement
 -
- **Leçon 11 : Introduction à la protection de menaces réseau**
 - Différences de protection antivirus et de pare-feu
 - Comment les données traversent le réseau
 - Fonctions réseau d'un pare-feu hôte
 - Protection multi-niveau basée sur l'hôte
 -
- **Leçon 12 : Configuration d'une politique de pare-feu**
 - Éléments d'une politique de pare-feu
 - Configuration de règles de pare-feu par défaut
 - Gestion du filtrage Smart Traffic
 - Configuration du trafic et des paramètres de masquage
 -
- **Leçon 13 : Gestion de la hiérarchie de SAV pour les politiques de pare-feu et de prévention d'intrusion**
 - Groupes
 - Héritage
 - Gestion des emplacements
 - Application des politiques
 -
- **Leçon 14 : Gestion des composants pare-feu client de SEP**
 - Caractéristiques des clients et composants
 - Configuration des modes de protection des clients
 - Dépannage des clients
 -
- **Leçon 15 : Gestion des politiques du système de prévention d'intrusion (IPS)**
 - Concepts du système de prévention d'intrusion
 - Configuration de l'IPS
 - Gestion des politiques du système de prévention d'intrusion
 -
- **Leçon 16 : Configuration de la prévention HIPS**
 - Prévention d'intrusion de l'hôte
 - Configuration des politiques de protection des logiciels

- Configuration des politiques de protection au niveau du matériel
- Application et retrait des politiques
- Gestion du blocage du système et des listes de signatures de fichiers
- Configuration de la protection du débordement de tampon
-
- **Leçon 17 : Contrôle de la protection de menaces réseau**
 - Contrôle de la page d'accueil
 - Exécution et affichage de rapports de pare-feu
 - Configuration de la consignation et des notifications
 - Affichage du résumé du contrôle