

Symantec Endpoint Protection 11.0

DESCRIPCIÓN DEL CURSO

El curso de *Symantec Endpoint Protection 11.0* está diseñado para el profesional de redes, seguridad informática y gestión de sistemas que se encarga de crear, implementar y monitorizar soluciones de firewall de cliente, antivirus y antispyware. Esta clase abarca cómo diseñar, implementar, instalar, configurar y monitorizar Symantec Endpoint Protection (SEP).

Los estudiantes también aprenden cómo crear e implementar firewall de cliente, prevención de intrusiones y políticas de protección de conductas que protegen la empresa contra virus, piratas informáticos y spam. Además, aprenden a solucionar problemas de administradores y clientes de SEP.

Método de enseñanza

Formación dirigida por un instructor

Duración

Cinco días

Objetivos del curso

Al finalizar el curso, usted podrá:

- Describir las amenazas de seguridad que afrontan los clientes empresariales en la actualidad y las soluciones que ofrece Symantec para mitigar estos riesgos.
- Describir productos, componentes, dependencias de productos y jerarquía de sistemas de SEP.
- Instalar y configurar componentes de clientes y gestión de SEP.
- Implementar clientes de SEP.
- Gestionar políticas sobre antivirus y antispyware.
- Configurar protección anticipada contra amenazas.
- Diseñar una implementación de Endpoint Protection.
- Monitorizar y mantener el entorno SEP.
- Configurar políticas sobre firewall y prevención de intrusiones.
- Personalizar la protección contra amenazas de la red.
- Administrar la IU del cliente.

¿Quién debería asistir?

Este curso está dirigido a administradores de redes, distribuidores, administradores de sistemas, administradores de seguridad de clientes, profesionales de sistemas y asesores que están a cargo de la instalación, configuración y gestión diaria de Symantec Endpoint Protection en una variedad de entornos de redes y que son responsables de resolver

problemas y optimizar el rendimiento de este producto en el entorno empresarial.

Prerrequisitos

Conocimientos prácticos sobre terminología informática avanzada, por ejemplo, términos de redes TCP/IP y de Internet, y conocimientos de administradores de sistemas operativos Microsoft Windows 2000/XP/2003.

Prácticas

Este curso incluye ejercicios prácticos simples que le permiten evaluar sus nuevos conocimientos y comenzar a aplicarlos en su ambiente de trabajo.

RESUMEN DEL CURSO

Introducción:

- Descripción general del curso
- El entorno de laboratorio de la clase

Lección 1: El panorama de seguridad actual

- Riesgos para la seguridad
- Gestión y protección de sistemas
- Políticas de seguridad empresarial y evaluaciones de seguridad

Lección 2: Solución de productos de Symantec Endpoint Protection

- Symantec Endpoint Protection (SEP)
- La jerarquía de SEP
- Cómo se comunican los clientes con los servidores de administración

Lección 3: Instalación de SEP

- Identificación de los requisitos de software
- Preparación de servidores y clientes
- Instalación de Symantec Endpoint Protection Manager
- Navegación en Symantec Endpoint Protection Manager

Lección 4: Implementación de clientes

- Preparación de la instalación de clientes
- Elección del método de instalación del cliente
- Instalación de clientes
- Análisis de clientes
- Gestión del entorno del usuario final

Lección 5: Instalación de componentes de gestión adicionales

- Instalación de un servidor central de LiveUpdate
- Configuración de LiveUpdate
- Instalación y configuración de cuarentena central
- Ampliación del entorno de gestión

Lección 6: Configuración de políticas sobre antivirus y antispyware

- Configuración de los ajustes de seguridad general
- Configuración de análisis de auto protección
- Configuración de análisis definidos por el administrador
- Archivos en cuarentena

Lección 7: Configuración de protección adicional

- Configuración de análisis de protección anticipada contra amenazas
- Configuración de excepciones
- Configuración de bloqueo del sistema y protección contra manipulaciones

Lección 8: Monitorización de antivirus y antispyware

- Visualización y gestión de registros
- Configuración y visualización de notificaciones
- Configuración y visualización de informes

Lección 9: Gestión del rendimiento del servidor y de la base de datos

- Administración de servidores de administración
- Gestión de la seguridad del servidor
- Comunicación con otros servidores
- Gestión de administradores
- Gestión de la base de datos

Lección 10: Diseño de una implementación de Endpoint Security

- Criterios clave de implementación
- Diseño de una estrategia de implementación de muestra

Lección 11: Introducción a la protección contra amenazas de red y el control de dispositivos y aplicaciones

- Conceptos básicos de protección contra amenazas de red
- Firewall
- Prevención de intrusiones
- Control de dispositivos y aplicaciones

Lección 12: Configuración de una política de firewall

- Configuración de los elementos de la política de firewall
- Configuración de normas de firewall
- Configuración de filtrado de tráfico inteligente
- Configuración de los ajustes de tráfico y ocultación

Lección 13: Gestión de políticas del sistema de prevención contra intrusos (IPS)

- Configuración de IPS
- Gestión de firmas personalizadas

Lección 14: Gestión del control de dispositivos y aplicaciones

- Control de dispositivos y aplicaciones

- Creación de políticas sobre control de dispositivos y aplicaciones
- Personalización de políticas sobre control de dispositivos y aplicaciones

Lección 15: Personalización de la protección contra amenazas de red y el control de dispositivos y aplicaciones

- Gestión de las ubicaciones del grupo
- Gestión de los componentes de las políticas
- Configuración del aprendizaje de la aplicación

Lección 16: Monitorización de la protección contra amenazas de red y el control de dispositivos y aplicaciones

- Monitorización de la página de inicio
- Visualización y gestión de informes sobre IPS y firewall
- Configuración de creación de registros y notificaciones
- Visualización del resumen de los monitores