

Symantec Endpoint Protection 11.0

DESCRIZIONE DEL CORSO

Il corso su *Symantec Endpoint Protection 11.0* è progettato per i professionisti addetti all'amministrazione di rete, sicurezza IT e sistemi con compiti di architettura, implementazione e monitoraggio delle soluzioni antivirus, antispyware e firewall client. Il corso illustra come progettare, distribuire, installare, configurare e monitorare Symantec Endpoint Protection (SEP).

Gli studenti apprenderanno anche come creare e implementare policy firewall client, di prevenzione delle intrusioni e di protezione comportamentale in grado di difendere l'azienda da virus, hacker e spamming. Inoltre, gli studenti apprenderanno come risolvere i problemi di manager e client SEP.

Metodo di erogazione

Con istruttore

Durata

Cinque giorni

Obiettivi del corso

Al termine di questo corso, i partecipanti saranno in grado di:

- descrivere le minacce per la sicurezza che le moderne aziende devono affrontare e le soluzioni offerte da Symantec per mitigare tali rischi;
- descrivere i prodotti e i componenti SEP, le dipendenze del prodotto e la gerarchia del sistema;
- installare e configurare i componenti client e di gestione SEP;
- distribuire i client SEP;
- gestire policy antivirus e antispyware;
- configurare una protezione attiva dalle minacce;
- progettare una distribuzione di Endpoint Protection;
- monitorare e gestire l'ambiente SEP;
- configurare policy di prevenzione delle intrusioni e firewall;
- personalizzare la protezione dalle minacce di rete;
- gestire l'interfaccia utente client.

Destinatari del corso

Il corso è rivolto a responsabili di rete, rivenditori, amministratori di sistema, amministratori della sicurezza dei client, professionisti dei sistemi e consulenti che sono incaricati dell'installazione, configurazione e gestione quotidiana di Symantec Endpoint Protection in diversi ambienti di rete e che sono responsabili della risoluzione dei problemi e dell'ottimizzazione delle prestazioni del prodotto nell'ambiente aziendale.

Requisiti per la partecipazione

È necessario disporre di una conoscenza operativa della terminologia avanzata del settore informatico, compresi i termini relativi alle reti TCP/IP e a Internet, e una conoscenza a livello di amministratore dei sistemi operativi Microsoft Windows 2000/XP/2003.

Esercitazioni

Il corso include esercitazioni pratiche che consentono di testare le nuove competenze e iniziare a utilizzarle in un ambiente di lavoro.

PROFILO DEL CORSO

Introduzione

- Panoramica del corso
- L'ambiente di esercitazione

Lezione 1. Quadro attuale della sicurezza

- Rischi per la sicurezza
- Gestione e protezione dei sistemi
- Policy di sicurezza aziendali e valutazioni della sicurezza

Lezione 2. La soluzione Symantec Endpoint Protection

- Symantec Endpoint Protection (SEP)
- La gerarchia di SEP
- Modalità di comunicazione dei client con i server di gestione

Lezione 3. Installazione di SEP

- Identificazione dei requisiti software
- Preparazione di server e client
- Installazione di Symantec Endpoint Protection Manager
- Navigazione in Symantec Endpoint Protection Manager

Lezione 4. Distribuzione dei client

- Preparazione dell'installazione dei client
- Scelta del metodo di installazione dei client
- Installazione dei client
- Scansione dei client
- Gestione dell'ambiente degli utenti finali

Lezione 5. Installazione di componenti di gestione aggiuntivi

- Installazione di un server LiveUpdate centrale
- Configurazione di LiveUpdate
- Installazione e configurazione di Central Quarantine
- Espansione dell'ambiente di gestione

Lezione 6. Configurazione di policy antivirus e antispyware

- Configurazione delle impostazioni di sicurezza generali
- Configurazione delle scansioni di Auto-Protect
- Configurazione delle scansioni definite dall'amministratore
- Quarantena dei file

Lezione 7. Configurazione di protezione aggiuntiva

- Configurazione della scansione di protezione attiva dalle minacce
- Configurazione delle eccezioni
- Configurazione del blocco del sistema e della protezione dalle manomissioni

Lezione 8. Monitoraggio antivirus e antispyware

- Visualizzazione e gestione dei registri
- Configurazione e visualizzazione delle notifiche
- Configurazione e visualizzazione dei report

Lezione 9. Gestione di server e database

- Amministrazione dei server di gestione
- Gestione della sicurezza dei server
- Comunicazione con altri server
- Gestione degli amministratori
- Gestione del database

Lezione 10. Progettazione di una distribuzione di Endpoint Security

- Criteri di distribuzione chiave
- Progettazione di una strategia di distribuzione campione

Lezione 11. Introduzione alla protezione dalle minacce di rete e al controllo di applicazioni e dispositivi

- Concetti di base sulla protezione dalle minacce di rete
- Il firewall
- Prevenzione delle intrusioni
- Controllo di applicazioni e dispositivi

Lezione 12. Configurazione di una policy firewall

- Configurazione degli elementi di una policy firewall
- Configurazione delle regole firewall
- Configurazione del filtro intelligente del traffico
- Configurazione delle impostazioni di traffico e stealth

Lezione 13. Gestione delle policy IPS (Intrusion Prevention System)

- Configurazione di IPS
- Gestione delle firme personalizzate

Lezione 14. Gestione del controllo applicazioni e dispositivi

- Controllo di applicazioni e dispositivi
- Creazione di policy di controllo applicazioni e dispositivi
- Personalizzazione delle policy di controllo applicazioni e dispositivi

Lezione 15. Personalizzazione della protezione dalle minacce di rete e del controllo di applicazioni e dispositivi

- Gestione delle posizioni di un gruppo
- Gestione dei componenti di una policy
- Configurazione dell'apprendimento dell'applicazione

Lezione 16. Monitoraggio della protezione dalle minacce di rete e del controllo di applicazioni e dispositivi

- Monitoraggio della pagina iniziale
- Visualizzazione e gestione dei report firewall e IPS
- Configurazione delle funzioni di registrazione e notifica
- Visualizzazione del riepilogo dei monitoraggi