TEMARIO DEL CURSO

Check Point Deployment Administrator (CPDA) R82

14 horas

OBJETIVOS DEL CURSO

- Adquirir los conocimientos, habilidades y experiencia práctica necesarios para desplegar un nuevo entorno Quantum Security de Check Point R82.
- Instalar y configurar SmartConsole, el sistema operativo Gaia, un Security Management Server y un Security Gateway.
- Crear políticas de seguridad básicas, desplegar clústeres y configurar servidores de log dedicados.
- Realizar tareas de mantenimiento: backups, snapshots y actualizaciones de software.
- Automatizar la importación masiva de objetos y reglas mediante batch import.

A QUIÉN VA DIRIGIDO

- Administradores de despliegue; administradores de seguridad; consultores de seguridad; profesionales de redes con base en TCP/IP, sistemas y seguridad.

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.

— Introducción a Quantum Security

- Componentes principales de la arquitectura Three-Tier de Check Point.
- Funcionamiento conjunto de los componentes en el entorno Check Point.
- Conceptos de Quantum Security Gateway, Security Management Server y SmartConsole.

MÓDULO 02.
— Arquitectura de Quantum Security

- Consideraciones clave para planificar un nuevo despliegue Quantum Security.
- Verificación de los hosts Check Point y documentación del entorno de red.
- Verificación del host cliente A-GUI (SmartConsole).
- Novedades de R82: ElasticXL para clustering, HTTPS inspection mejorada, capacidades de administración asistida por IA.

MÓDULO 03.
— Despliegue del Security Management Server primario

- Flujo de trabajo, directrices y mejores prácticas para el despliegue del Security Management Server primario.
- Laboratorio: instalación del sistema operativo Gaia.
- Laboratorio: configuración del Security Management Server primario.
- Laboratorio: despliegue de SmartConsole.

MÓDULO 04.
— Despliegue del Security Gateway

- Flujo de trabajo, directrices y mejores prácticas para el despliegue del Security Gateway.
- Laboratorio: ejecución del First Time Wizard en el Security Gateway.
- Laboratorio: creación del objeto Security Gateway en SmartConsole.
- Laboratorio: verificación de SIC (Secure Internal Communication) e instalación de licencias.

MÓDULO 05.
— Fundamentos de políticas de seguridad

- Elementos esenciales de una Security Policy en Check Point.
- Funcionalidades para la configuración y gestión avanzada de políticas.
- Laboratorio: creación de un paquete de Access Control Policy.
- Laboratorio: adición y modificación de reglas en la Access Control Policy.

MÓDULO 06.
— Despliegue de clúster de Security Gateways

- Flujo de trabajo, directrices y mejores prácticas para el despliegue de un clúster de Security Gateways (ClusterXL).
- Laboratorio: reconfiguración del entorno de seguridad.
- Laboratorio: configuración de los miembros del clúster como Security Gateways.
- Laboratorio: configuración de interfaces y adición de miembros y licencias al clúster.

MÓDULO 07.

— Despliegue del servidor de log dedicado

- Flujo de trabajo, directrices y mejores prácticas para el despliegue de un Log Server dedicado.
- Laboratorio: configuración y adición del Log Server dedicado al entorno.

MÓDULO 08.

— Fundamentos de mantenimiento

- Estrategia de mantenimiento regular: propósito y planificación.
- Backup y restauración del sistema, gestión de snapshots, carga y guardado de configuraciones.
- Monitorización del hardware, actualizaciones de software.
- Laboratorio: recolección y descarga de backups y snapshots del sistema.

MÓDULO 09.

— Importación masiva de componentes del entorno de seguridad

- Propósito del batch import y casos de uso.
- Flujo de trabajo, directrices y mejores prácticas para la importación masiva.
- Laboratorio: importación y creación de objetos Host, Network y Group.
- Laboratorio: importación y creación de reglas de Access Control.