CCSA, Check Point Certified Security Administrator R81, preparación para la certificación

Curso práctico de 4 días - 28h
Ref.: CPQ - Precio 2024: 2 290€ sin IVA

Este curso le permitirá adquirir todas las técnicas y metodologías necesarias para aprobar el examen de certificación CCSA R81. Aprenderá a implementar una política de seguridad, la traducción de direcciones (NAT) y el módulo del sistema de prevención de intrusiones (IPS).

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Instalación y configuración de Check Point R81

Implantación de la traducción de direcciones (NAT)

Implantación de una política de seguridad y supervisión del tráfico

Preparación del examen oficial para obtener la certificación CCSA

Implantación de políticas de control de aplicaciones, filtrado de URL y gestión de usuarios

CERTIFICACIÓN

Para realizar el examen de certificación, sólo tiene que registrarse en el sitio web de Check Point. A continuación, puede realizar el examen directamente en línea o en un centro autorizado.

PARTICIPANTES

Técnicos, administradores e ingenieros de sistemas, redes y seguridad.

REQUISITOS PREVIOS

Buenos conocimientos de TCP/IP. Conocimientos básicos de seguridad informática.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

PROGRAMA

última actualización: 02/2024

1) Visión general de la arquitectura Check Point R81

- Productos Check Point.
- Novedades de la versión R81.

2) Despliegue de Gaia: Instalación de dispositivos Check Point

- Elementos de la arquitectura de tres niveles.
- Arquitectura modular de hojas de software.
- Check Point Infinity.
- Presentación del sistema Gaïa.
- Arquitectura distribuida e independiente.
- El servidor de gestión. El protocolo SIC.

Trabajo práctico : Instalación de Check Point R81.

3) Gestión de la seguridad Gestión de servidores

- Primeros pasos con la SmartConsole R81.
- Política de seguridad. Gestión de reglas.
- Políticas unificadas.
- Inspección de paquetes.
- "Políticas en línea".

Trabajo práctico : Instalación de la SmartConsole. Creación de objetos. Creación de una política de seguridad. Activación del anti-spoofing.

4) Traducción de direcciones (NAT)

- Reglas de traducción de direcciones con IPv4 e IPv6.
- NAT estática (One To One NAT) y NAT dinámica (Many To One NAT)/PAT.
- ARP y enrutamiento.
- Manual NAT.

Trabajo práctico : Implementación de NAT estático automático, Hide y reglas de transacción manuales.

5) Visibilidad: gestión de registros, supervisión e informes

- Política de gestión de registros.
- Realice un seguimiento de las conexiones con Logs & Monitor (antes SmartView Tracker).
- SmartView Monitor, funciones y umbrales de alerta.

Trabajo práctico : Activar la supervisión, utilizar el protocolo de supervisión de actividades sospechosas, ver el tráfico, supervisar el estado de la política de seguridad.

6) Política de prevención de amenazas basada en el usuario

- Identity Awareness R81 métodos de autenticación.
- Necesidad de recuperar las identidades de los usuarios.
- Objetos "Función de acceso".
- La política de Prevención de Amenazas y su Software Blades.
- Gestión de normas.
- Perfiles de seguridad.
- Prevención autónoma de amenazas.

Autenticación: implantación de Identity Awareness, creación de roles y accesos.
Antivirus y Anti-Bot.

7) Gestión de licencias y multisede

- Estructura de la licencia.
- Gestión de licencias en SmartUpdate y SmartConsole.
- Tipos de licencia.
- Gestión de contratos y servicios.

Trabajo práctico : Definición de paquetes de políticas.

8) Gestión de paquetes de políticas.

- Definición y tipos de "Capas".
- Inspección de paquetes en una "capa ordenada".
- Política de capas compartidas.

9) Gestión de administradores

- "Perfiles de permiso.
- Limitación del ámbito de actuación de los administradores.
- Gestión de usuarios concurrentes.
- Gestión de la sesión.

Trabajo práctico : Creación de un nuevo "Perfil de permiso" con autorizaciones limitadas.

10) Descifrado HTTPS

- Creación de normas.
- Gestión de certificados.
- Indicaciones del nombre del servidor (SNI).

Trabajo práctico : Implementación de la inspección HTTPS.

FECHAS

Contacto