



ExecuTrain

Impulsamos tu talento tecnológico



MICROSOFT

RED HAT

VIRTUALIZACIÓN

CIBERSEGURIDAD

DESARROLLO

OFFICE

BIG DATA

BLOCK CHAIN

BASES DE DATOS

GESTIÓN DE
SERVICIOS IT

CLOUD
COMPUTING

METODOLOGÍAS
EN PROYECTOS

SISTEMAS
OPERATIVOS

Y MÁS...



www.executrain.com.mx



¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio



Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.



Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.



Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

CheckPoint / Check Point Certified Security Administrator (CCSA)

Este curso permitirá a su equipo administrar y fortalecer la seguridad de su entorno Quantum, aprendiendo a configurar políticas de seguridad, controlar aplicaciones y navegación, monitorear el tráfico, gestionar accesos y detectar y prevenir amenazas.

Con estos conocimientos podrán mejorar la visibilidad, el control y la protección de la infraestructura de seguridad de la empresa.

Audiencia

Administradores de seguridad y redes.
Ingenieros de infraestructura y ciberseguridad.
Administradores de Check Point / Quantum Security.
Profesionales responsables de configurar, monitorear y mantener políticas de seguridad.

Prerrequisitos

-  Conocimientos básicos de sistemas operativos Unix/Linux y/o Windows.
-  Fundamentos de Internet.
-  Fundamentos de Redes.
-  Conocimientos básicos de Seguridad de Redes.
-  Conocimientos de Administración de Sistemas.
-  Conocimientos de redes TCP/I

Módulos

Módulo 1: Introducción a Quantum Security

Identificar los componentes principales de la arquitectura de tres niveles de Check Point y explicar cómo funcionan en conjunto dentro del entorno de Check Point.

Tareas de laboratorio

- Explorar Gaia en el servidor de administración de seguridad
- Explorar Gaia en el servidor de registros dedicado
- Explorar Gaia en los miembros del clúster de Security Gateway
- Conectarse a SmartConsole

- Navegar por las vistas GATEWAYS & SERVERS
- Navegar por las vistas SECURITY POLICIES
- Navegar por las vistas LOGS & EVENTS
- Navegar por las vistas MANAGE & SETTINGS

Módulo 2: Administración de cuentas de administrador

Explicar el propósito de las cuentas de administrador de SmartConsole.

Identificar funciones útiles para la colaboración entre administradores, como la administración de sesiones,

la administración simultánea y la instalación simultánea de políticas.

Tareas de laboratorio

- Crear nuevos administradores y asignar perfiles
- Probar las asignaciones de perfiles de administrador
- Administrar sesiones simultáneas de administradores
- Tomar el control de otra sesión y verificar su estado

Módulo 3: Administración de objetos

Explicar el propósito de los objetos de SmartConsole.

Dar ejemplos de objetos físicos y lógicos de SmartConsole.

Tareas de laboratorio

- Ver y modificar objetos de GATEWAYS & SERVERS
- Ver y modificar objetos de red
- Ver y modificar objetos de servicio

Módulo 4: Administración de políticas de seguridad

Explicar el propósito de las políticas de seguridad.

Identificar los elementos esenciales de una política de seguridad.

Identificar las funciones y capacidades que mejoran la configuración y la administración de la política de seguridad.

Tareas de laboratorio

- Verificar la política de seguridad
- Modificar las políticas de seguridad
- Instalar la política de seguridad estándar
- Probar la política de seguridad

Módulo 5: Capas de políticas

Demostrar la comprensión del concepto de capas de políticas de Check Point.

Explicar cómo afectan las capas de políticas a la inspección del tráfico.

Tareas de laboratorio

- Agregar una capa ordenada
- Configurar e implementar las reglas de la capa ordenada
- Probar la política de la capa ordenada
- Crear una capa DMZ en línea
- Probar la capa DMZ en línea

Módulo 6: Monitoreo de operaciones de seguridad

Explicar el propósito del monitoreo de operaciones de seguridad.

Ajustar la configuración del servidor de registros.

Utilizar consultas predefinidas y personalizadas para filtrar los resultados de los registros.

Monitorear el estado de los sistemas Check Point.

Tareas de laboratorio

- Configurar la administración de registros
- Mejorar la vista de la base de reglas, las reglas y el registro
- Revisar los registros y buscar datos
- Configurar el módulo de monitoreo
- Monitorear el estado de los sistemas

Módulo 7: Reconocimiento de identidad

Explicar el propósito de la solución de reconocimiento de identidad.

Identificar los elementos esenciales del reconocimiento de identidad. Tareas de laboratorio

- Ajustar la política de seguridad para el reconocimiento de identidad
- Configurar el recopilador de identidades
- Definir el rol de acceso del usuario
- Probar el reconocimiento de identidad

Módulo 8: Inspección HTTPS

Explicar el propósito de la solución de inspección HTTPS.

Identificar los elementos esenciales de la inspección HTTPS.

Tareas de laboratorio

- Habilitar la inspección HTTPS
- Ajustar las reglas de control de acceso
- Implementar el certificado de Security Gateway
- Probar y analizar la política con la inspección HTTPS

Módulo 9: Control de aplicaciones y filtrado de URL

Explicar el propósito de las soluciones de control de aplicaciones y filtrado de URL.

Identificar los elementos esenciales del control de aplicaciones y el filtrado de URL.

Tareas de laboratorio

- Ajustar la política de control de acceso
- Crear y ajustar el control de aplicaciones y URL
- Probar y ajustar las reglas de control de aplicaciones y filtrado de URL
- Módulo 10: Fundamentos de prevención de amenazas
- Explicar el propósito de la solución de prevención de amenazas.
- Identificar los elementos esenciales de la prevención autónoma de amenazas. Tareas de laboratorio
- Habilitar la prevención autónoma de amenazas
- Probar la prevención autónoma de amenazas