
cybertrust
INSPIRANDO CONFIANZA
EC-Council
TM
C|ND
Certified Network Defender

# Certified Network Defender (CND)

El Programa de capacitación en certificación de seguridad de redes completo, neutral, práctico y dirigido por un instructor. Es un programa basado en habilidades, intensivo en laboratorio, basado en un análisis de trabajo y tarea y un marco de educación sobre ciberseguridad presentado por la Iniciativa Nacional de Educación Cibernética (NICE). El curso también se ha asignado a las funciones y responsabilidades del trabajo global y a las funciones de trabajo del Departamento de Defensa (DoD) para los administradores del sistema / red. El curso está diseñado y desarrollado después de una extensa investigación de mercado y encuestas.

El programa prepara a los administradores de red sobre las tecnologías y operaciones de seguridad de la red para lograr una preparación de seguridad de la red del tipo "Defense in-Depth"

Cubre el enfoque de protección, detección y respuesta a la seguridad de la red.

El curso contiene laboratorios prácticos, basados en las principales herramientas y técnicas de seguridad de red que proporcionarán a los administradores de redes una experiencia real en las operaciones y tecnologías de seguridad de redes actuales. El kit de estudio le proporciona más de 10 GB de mejores prácticas de seguridad de red, evaluaciones y herramientas de protección. El kit también contiene plantillas para diversas políticas de red y una gran cantidad de documentos técnicos para aprendizaje adicional.

## ¿Qué aprenderás?

1. El alumno aprenderá sobre diversos controles de seguridad de red, protocolos y dispositivos
2. El alumno podrá determinar la ubicación adecuada para los sensores IDS / IPS, ajustar IDS para falsos positivos y falsos negativos, y configuraciones para reforzar la seguridad a través de las tecnologías IDPS
3. Los estudiantes podrán solucionar fallos de su red por diversos problemas de red que se estudiarán en el curso.

C|ND Certified Network Defender

4. Los estudiantes podrán aprenderan a configurar una implementación segura de VPN para su organización

5. El alumno podrá identificar varias amenazas en la red de la organización

6. El alumno podrá identificar diversas amenazas a la red inalámbrica y aprender a mitigarlas

7. El alumno aprenderá cómo diseñar e implementar diversas políticas de seguridad para sus organizaciones

8. El alumno podrá supervisar y realizar análisis de firmas para detectar varios tipos de ataques y actividades de infracción de políticas.

9. El alumno aprenderá la importancia de la seguridad física y podrá determinar e implementar diversos controles de seguridad física para sus organizaciones

10. El alumno podrá realizar evaluaciones de riesgos, evaluaciones / escaneos de vulnerabilidades a través de varias herramientas y generar informes detallados sobre el mismo

11. El alumno podrá reforzar la seguridad de varios hosts individualmente en la red de la organización

12. El alumno podrá identificar los datos críticos, elegir el método de copia de seguridad adecuado, los medios y la técnica para realizar copias de seguridad de los datos de la organización con regularidad.

13. El alumno podrá elegir la solución de firewall adecuada, la topología y las configuraciones para reforzar la seguridad a través del firewall

14. El alumno podrá proporcionar la primera respuesta al incidente de seguridad de la red y ayudar al equipo de investigación del equipo IRT y al equipo de investigación forense a manejar un incidente.

El enfoque organizacional en la defensa cibernética es más importante que nunca, ya que las infracciones cibernéticas tienen un impacto financiero mucho mayor y pueden causar un gran daño a la reputación.

A pesar de los mejores esfuerzos para evitar infracciones, muchas organizaciones aún se ven comprometidas. Por lo tanto, las organizaciones deben tener, como parte de sus mecanismos de defensa, ingenieros de red capacitados que se centren en proteger, detectar y responder a las amenazas en sus redes.

Los administradores de red pasan mucho tiempo con entornos de red y están familiarizados con los componentes de red, el tráfico, el rendimiento y la utilización, la topología de red, la ubicación de cada sistema, la política de seguridad, etc.

Por lo tanto, las organizaciones pueden ser mucho mejores para defenderse de ataques feroces si los administradores de TI y red cuentan con habilidades de seguridad de red adecuadas. De esta forma, el administrador de red puede desempeñar un papel importante en la defensa de la red y convertirse en la primera línea de defensa de cualquier organización.

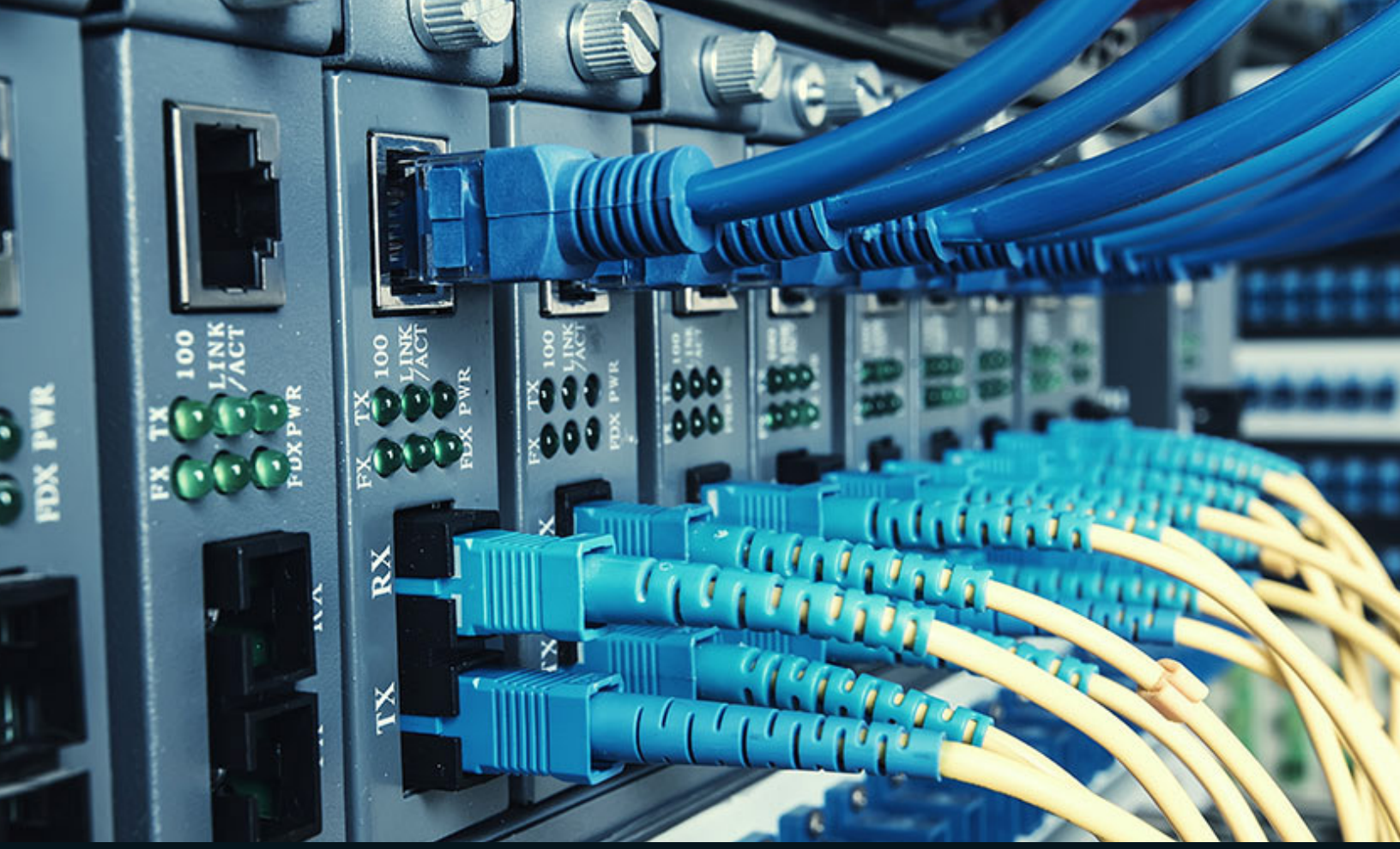
No existe una capacitación de seguridad de red táctica adecuada que esté disponible para los administradores de red, que les proporciona las habilidades básicas de seguridad de la red.
Los estudiantes inscriptos en el curso Certified Network Defender obtendrán una comprensión detallada y la capacidad práctica para funcionar en situaciones de la vida real que involucren defensa de red. Ganarán la profundidad técnica requerida para diseñar activamente una red segura en su organización. Este programa será similar a aprender matemáticas en lugar de simplemente usar una calculadora. Este curso le proporciona la comprensión fundamental de la verdadera construcción de la transferencia de datos, las tecnologías de red y las tecnologías de software para que comprenda cómo funcionan las redes, comprenda qué software se está automatizando y cómo analizar el material de la asignatura.

Aprenderá cómo proteger, detectar y responder a los ataques de la red. Aprenderá los fundamentos de defensa de red, la aplicación de controles de seguridad de red, protocolos, dispositivos perimetrales, IDS seguro, VPN y configuración de firewall. A continuación, aprenderá las complejidades de la firma del tráfico de red, el análisis y la exploración de vulnerabilidades, que lo ayudarán cuando diseñe mejores políticas de seguridad de red y planes de respuesta a incidentes exitosos. Estas habilidades te ayudarán a fomentar la resiliencia y la continuidad de las operaciones durante los ataques.

# Modulos

1. Fundamentos de defensa de la red
2. Amenazas, vulnerabilidades y ataques a la seguridad de la red
3. Controles de seguridad de red, protocolos y dispositivos
4. Diseño e implementación de políticas de seguridad de red
5. Seguridad física
6. Seguridad de host
7. Configuración y administración segura de firewall
8. Configuración y gestión seguras de VPN
9. Defensa de red inalámbrica
10. Monitoreo y análisis de tráfico de red
11. Gestión de vulnerabilidades y riesgos de red
12. Copia de seguridad y recuperación de datos
13. Respuesta y gestión de incidentes de red

CND Certified Network Defender




## ¿Para quién va dirigido el curso?

Administradores de red

Administradores de seguridad de red

Ingeniero de seguridad de red

Técnicos de defensa de red

Analista de CND

Analista de seguridad

Operador de seguridad

Cualquiera que participe en operaciones de red

C|ND Certified Network Defender


www.cybertrust.cl

Av. Apoquindo 4775, Piso 3 - Las Condes, Santiago de Chile. Teléfono: +562 3224 3551 | +562 3224 3552 Email: contacto@cybertrust.cl