

CAPACITACIÓN



El programa de certificación de **Certified Network Defender (CND)** se enfoca en crear **Network Administrators** capacitados para proteger, detectar y responder ante las amenazas en la red. Los **Network administrators** generalmente están familiarizados con los componentes de la red, el tráfico, el rendimiento y la utilización, la topología de la red, la ubicación de cada sistema, la política de seguridad, etc. Un **CND** tendrá la comprensión fundamental de la verdadera construcción de transferencia de datos, tecnologías de red y tecnologías de software para entender cómo operan las redes, que software está automatizando y cómo analizar la materia. Además, entenderá los fundamentos de defensa de red, la aplicación de controles de seguridad de red, protocolos, dispositivos perimetrales, a asegurar **IDS, VPN y configuración de firewall, complejidad de firmas de tráfico de red, análisis y Vulnerability Scanning**, lo que ayudará al **Network Administrator** a diseñar mejores políticas de seguridad de redes y exitosos programas de respuesta a incidentes.

OBJETIVOS:

- Preparar al participante en tecnologías de seguridad y operación de redes para alcanzar un grado de Defensa en profundidad.
- **Certified Network Defender** es un curso de nivel Intermedio, no es tan especializado como **CEH**, incluso podría ser un paso antes en el plan de carrera del profesional de seguridad, por lo que solo es necesario contar con conocimiento básico en redes.

CAPACITACIÓN



DIRIGIDO A:

- Administradores de Red
- Administradores de Seguridad en Red
- Técnicos de defensa de red
- Operador de seguridad Analista de **CND**
- Ingeniero de seguridad de red Analista de seguridad

DURACIÓN: 40 Hrs.

REQUISITOS:

- Conocimientos en **Networking**

INCLUYE:

- Instalaciones adecuadas
- Material y manuales de cursos
- Instructores Certificados
- Examen de Certificación **Certified Network Defender (CND)**

Reconocimientos



CAPACITACIÓN



Temario:

- Fundamentos de las redes computacionales y la defensa
- Amenazas, Vulnerabilidades y Ataques a la Seguridad de las Redes
- Controles, Protocolos y Dispositivos de Seguridad de las Redes
- Diseño e Implementación de la Política de Seguridad de las Redes
- Seguridad Física
- Seguridad del Host
- Configuración y Administración del **Firewall** Seguro
- Configuración y Administración de **IDS** Seguro
- Configuración y Administración de **VPNs** Seguros
- Defensa de Redes Inalámbricas
- Monitoreo y Análisis del Tráfico de las Redes
- Gestión de Riesgos y Vulnerabilidades de las Redes
- Respaldo y Recuperación de Datos
- Respuesta y Administración de Incidentes de las Redes