EC-COUNCIL



EC-COUNCIL · PROGRAMA DE DEFENSA DE REDES

Certified Network Defender (C|ND) v3

Proteja, detecte, responda y anticipe: la certificación de referencia mundial en seguridad de redes y Blue Team

¿Por qué debería asistir?

El Certified Network Defender (C|ND) de EC-Council es una certificación de seguridad de redes, independiente de fabricantes, para todo administrador de TI y de sistemas que necesita operar con una mentalidad segura. Los participantes aprenden a defender redes y entornos operativos en redes locales, endpoints, infraestructura en la nube, aplicaciones, OT y dispositivos móviles, además de análisis de logs, monitoreo de tráfico, investigación y respuesta básica, y continuidad del negocio.

C|ND es el primer programa de seguridad de redes con una estrategia de seguridad continua y adaptativa (Proteger, Detectar, Responder y Predecir), que cubre la defensa en profundidad y las cinco funciones del NIST CSF. Es un programa intensivo en laboratorios, con más de 100 prácticas sobre máquinas reales, mapeado al 100 % con el marco NICE.

5 días	20	100+	+50 %	Blue Team
DURACIÓN	MÓDULOS	LABORATORIOS	PRÁCTICA	ENFOQUE



¿Quién debería participar?

Administración de redes
Administradores de red y de seguridad de red, e ingenieros de red responsables de operar la infraestructura de forma segura.

Ingeniería y análisis
Ingenieros de seguridad de red, ingenieros de ciberseguridad y analistas de seguridad de datos.

Operación de la defensa
Técnicos de defensa de red, operadores de seguridad y analistas de seguridad que monitorean y responden a incidentes.

Inicio de carrera
Estudiantes y profesionales de TI o de otras industrias que desean iniciar una carrera en ciberseguridad y Blue Team.

Objetivos de aprendizaje

- Planificar y administrar la seguridad de la red, y reconocer riesgos, amenazas y vulnerabilidades
- Diseñar e implementar políticas de seguridad de red y asegurar el cumplimiento de estándares regulatorios
- Implementar gestión de identidades y accesos, cifrado y segmentación de red, integrando principios Zero Trust
- Administrar la seguridad de Windows y Linux, y atender los riesgos de dispositivos móviles e IoT
- Gestionar la seguridad en tecnologías de virtualización y en plataformas en la nube (AWS, Azure y GCP)
- Monitorear el tráfico de red, gestionar logs y configurar IDS/IPS para identificar indicadores de compromiso
- Brindar la primera respuesta a incidentes y apoyar la planificación de continuidad y recuperación ante desastres
- Integrar inteligencia de amenazas, análisis de superficie de ataque y comprender EDR/XDR, UEBA, SOAR e IA/ML en la defensa

Áreas de habilidad del programa

Proteger · defensa en profundidad | Detectar · monitoreo continuo | Responder · respuesta a incidentes | Predecir · inteligencia de amenazas | Cinco funciones del NIST CSF | Nube: AWS, Azure y GCP | Contenedores, SDN y NFV | EDR, XDR, UEBA y SOAR

Programa del curso

Duración: 5 días

Módulo	Contenido
Módulos 1–4 Día 1	01 **Ataques de red y estrategias de defensa:** terminología, tipos de ataques, IoC/IoA y estrategias de defensa. 02 **Seguridad administrativa de la red:** cumplimiento normativo, políticas de seguridad y concienciación. 03 **Seguridad técnica de la red:** controles de acceso, IAM, criptografía y segmentación de red. 04 **Seguridad del perímetro de la red:** firewalls, IDS/IPS, proxies y filtrado de contenido.
Módulos 5–8 Día 2	05 **Seguridad de endpoints – Sistemas Windows:** hardening, parches, cuentas y Active Directory. 06 **Seguridad de endpoints – Sistemas Linux:** hardening, usuarios, servicios y parches. 07 **Seguridad de endpoints – Dispositivos móviles:** políticas BYOD/COPE, MDM y seguridad Android e iOS. 08 **Seguridad de endpoints – Dispositivos IoT:** riesgos, controles y entornos conectados.
Módulos 9–12 Día 3	09 **Seguridad administrativa de aplicaciones:** listas blancas, sandboxing, WAF y gestión de parches. 10 **Seguridad de datos:** cifrado, respaldo, prevención de pérdida de datos (DLP) y retención. 11 **Seguridad de redes virtuales empresariales:** virtualización, SDN, NFV, Docker y Kubernetes. 12 **Seguridad de redes en la nube empresariales:** responsabilidad compartida y seguridad en AWS, Azure y GCP.
Módulos 13–16 Día 4	13 **Seguridad de redes inalámbricas empresariales:** estándares, cifrado WPA2/WPA3 y WIDS/WIPS. 14 **Monitoreo y análisis del tráfico de red:** captura de paquetes, firmas y detección de anomalías. 15 **Monitoreo y análisis de logs de red:** logs de sistemas y dispositivos, SIEM y gestión centralizada. 16 **Respuesta a incidentes e investigación forense:** primera respuesta, proceso IH&R y fundamentos forenses.
Módulos 17–20 Día 5	17 **Continuidad del negocio y recuperación ante desastres:** conceptos BC/DR, alta disponibilidad y planes. 18 **Anticipación de riesgos con gestión de riesgos:** marcos de riesgo y gestión de vulnerabilidades. 19 **Evaluación de amenazas con análisis de superficie de ataque:** superficie de ataque y threat hunting. 20 **Predicción de amenazas con inteligencia de amenazas cibernéticas:** fuentes, plataformas y uso proactivo.

Apéndices de autoestudio:

A. Fundamentos de redes de computadoras ·
B. Seguridad física de la red ·
C. Seguridad de VPN ·
D. Seguridad de endpoints – Sistemas Mac.



Examen

Duración: 4 horas

Título	EC-Council Certified Network Defender (C|ND) – Versión 3		
Código	312-38	**N.º de preguntas**	100
Formato	Opción múltiple	**Duración**	4 horas
Aprobación	60 % – 85 %, según la forma del examen	**Plataforma**	EC-Council Exam Portal

Requisitos de elegibilidad

- **Con capacitación oficial de EC-Council:** puede presentar el examen sin proceso de elegibilidad.
- **Sin capacitación oficial:** al menos dos años de experiencia en el dominio de seguridad de la información, solicitud de elegibilidad aprobada y una cuota de US$100.

Estrategia de seguridad continua y adaptativa

C|ND es el primer programa de seguridad de redes con una estrategia continua y adaptativa en cuatro fases: **Proteger** (defensa en profundidad de endpoints, red y datos), **Detectar** (monitoreo continuo de amenazas), **Responder** (respuesta a incidentes) y **Predecir** (análisis de superficie de ataque, inteligencia y cacería de amenazas).

Información general

- Material oficial de EC-Council y más de 100 laboratorios en entornos en vivo
- Credencial acreditada por ANAB (ISO/IEC 17024) y reconocida por el DoD 8570/8140, y aprobada por el NCSC (GCHQ) del Reino Unido
- La certificación es válida por tres años y se mantiene con créditos de educación continua (ECE)

EC-Council Accredited Training Center

C|ND Certified Network Defender

C|EI Certified EC-Council Instructor