TEK
DIGITAL BUSINESS

EC-Council

C|ND v2
Certified Network Defender

DEFENSOR DE LA RED

CERTIFICADO

Proteger. Detectar. Responder. Predecir.

DEFENSOR DE LA RED CERTIFICADO V2

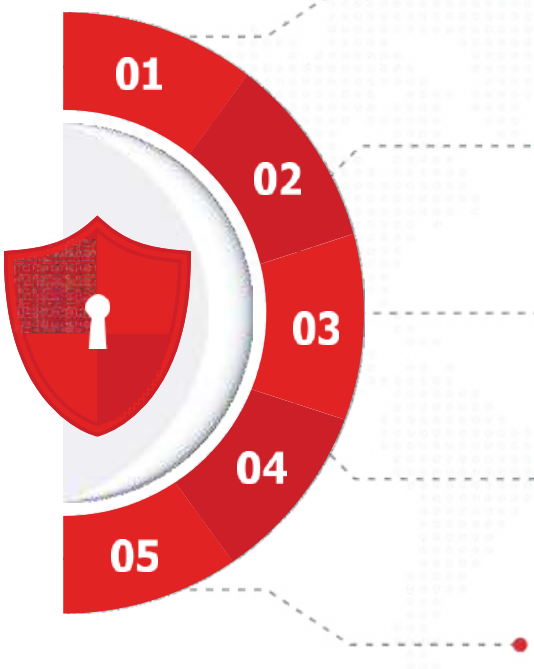
¡El único verdadero programa de defensa de la red del equipo azul!

La ciberseguridad ahora domina las prioridades de todas las empresas que se esfuerzan por adaptarse a un mundo posterior a COVID. Obligados a trabajar de forma remota, las identidades y los dispositivos de sus trabajadores son el nuevo perímetro de seguridad. De hecho, la ciberseguridad para las empresas es ahora tan crítica como el propio acceso a Internet.

¡El único programa creado para el experimento de trabajo desde casa más grande del mundo!

Los estudios y los informes de noticias han demostrado que los atacantes cibernéticos atacan rápidamente las nuevas superficies de amenazas desprotegidas creadas cuando millones de empleados comenzaron a trabajar desde casa. Brindar seguridad de red a un ecosistema distribuido sin precedentes en este mundo pospandémico es la prueba de fuego de cada equipo de defensa de la red.

El programa Certified Network Defender v2 se actualizó y se cargó con munición lista para la batalla para ayudar a los equipos azules a defender y ganar la guerra contra las violaciones de la red. Las personas y corporaciones que buscan fortalecer sus habilidades de defensa de la red encontrarán que CND v2 es imprescindible por 5 razones:



01 El único programa integral de defensa de la red creado para incorporar habilidades críticas de redes seguras: proteger, detectar, responder y predecir

02 Mapas para NICE 2.0 Framework

03 Viene repleto de las últimas herramientas, tecnologías y técnicas.

04 Implementa un enfoque práctico para el aprendizaje.

05 Diseñado con un enfoque mejorado en la predicción de amenazas, la continuidad del negocio y la recuperación ante desastres

Una estrategia de seguridad adaptativa: proteger, detectar, responder y predecir

La ciberseguridad es un proceso continuo, no lineal. Por lo tanto, su enfoque para mitigar los riesgos cibernéticos no puede ser estático. Esto es particularmente importante cuando la nueva "normalidad" tiene millones de empleados que trabajan desde ubicaciones remotas en redes WiFi frágiles en el hogar y dispositivos personales no desinfectados.

Según Gartner, los enfoques tradicionales de "prevenir y detectar" son inadecuados. Oportunistas por naturaleza, los actores maliciosos buscan las formas más fáciles de atacar a la mayoría de los usuarios y desviar las ganancias máximas. El desarrollo de un ciclo de seguridad adaptativo continuo ayuda a las organizaciones a adelantarse a los ciberdelincuentes mediante la creación y mejora de sistemas de seguridad. Introduzca CND v2.

Tan práctico como puede ser la defensa de redes.

Creado en base a un análisis exhaustivo de tareas laborales

CND v2 se basa en el marco de educación en seguridad cibernética y el análisis de tareas de roles de trabajo presentado por el Marco Nacional de Competencias de Infocomm (NICF). El programa también está asignado a las funciones del Departamento de Defensa (DoD) para los administradores de sistemas/redes, así como a las funciones y responsabilidades de trabajo global establecidas por el NICE Framework 2.0 revisado.

Estrategia de Seguridad Adaptativa

CND v2 incluye la Estrategia de Seguridad Adaptativa, aumentando así el alcance deProteger - Detectar - Responder a Proteger - Detectar - Responder - Predecir.

Mayor tiempo de laboratorio y enfoque práctico

Más del 50% del programa CND v2 está dedicado a habilidades prácticas en rangos en vivo a través de laboratorios del Consejo de la CE que cubren dominios como Gestión de defensa de red, Protección perimetral de red, Protección de puntos finales, Protección de aplicaciones y datos, Enterprise Virtual, Cloud y Protección de redes inalámbricas , detección y respuesta a incidentes y predicción de amenazas.

Un Módulo dedicado a la seguridad de LoT

La seguridad de IoT, antes ignorada, ahora es un tema de gran preocupación. Los dispositivos IoT noestán diseñados principalmente teniendo en cuenta la seguridad. Esto deja serias vulnerabilidades alconfigurar dispositivos IoT en una red. CND v2 presenta a los candidatos los diversos desafíos que plantean los dispositivos IoT y las medidas necesarias para mitigarlos.

Prácticas de visualización de red para la fuerza laboral remota

El seguimiento de las aplicaciones de seguridad y las configuraciones de los entornos de trabajo remotosa medida que la fuerza de trabajo se extiende por los servidores es muy difícil. El programa CND v2 enseña a los candidatos a implementar y administrar la seguridad de las tecnologías de virtualización Virtualización de red (NV), Red definida por software (SDN), Virtualización de función de red (NFV), Virtualización de SO, Contenedores, Dockers, Kubernetes utilizados en las redes modernas .

Incluye la última tecnología

CND v2 cubre las últimas tecnologías, como seguridad de red definida por software (SDN), seguridad de virtualización de funciones de red (NFV), seguridad de contenedores, seguridad de Docker y seguridad de Kubernetes.

Una actualización de las medidas de seguridad móvil

La firma de investigación Gartner predice que para 2021, el 27 % del tráfico de datos corporativos pasará por alto la seguridad del perímetro y fluirá directamente desde dispositivos móviles y portátiles a la nube. Con CND v2, aprenderá seguridad de dispositivos móviles empresariales, redefinición de seguridad de control de acceso y otras plataformas para garantizar que este punto final permanezca seguro.

Enfoque mejorado en la seguridad de la nube

Si bien la adopción de la computación en la nube en las organizaciones ha aumentado, también lo han hecho los desafíos. Los candidatos aprenderán diferentes formas de garantizar la seguridad en varias plataformas en la nube: AWS, Microsoft Azure Cloud y Google Cloud Platform.

Una introducción a la inteligencia de amenazas

Tener un enfoque proactivo de la seguridad es el nuevo requisito de todas las organizaciones. Sin inteligencia de amenazas, su postura de ciberseguridad es solo reactiva. CND v2 lo ayuda a adoptar unenfoque más efectivo y proactivo utilizando inteligencia de amenazas.

Análisis de superficie de ataque en profundidad

La clave para la gestión del riesgo cibernético es un análisis profundo de la superficie de ataque. CND v2 lo capacita para identificar qué partes de su organización deben revisarse y probarse para detectar vulnerabilidades de seguridad y cómo reducir, prevenir y mitigar los riesgos de la red.

Sobre el examen

Numero de preguntas: **100**	Duración del exámen: **4 horas**
Formato de prueba: **Opción multiple**	Entrega de prueba: **EXAMEN ECC**
Prefijo de examen: **312-38 (EXAMEN ECC)**	

Puntaje de aprobación

Para mantener la alta integridad de nuestros exámenes de certificación, los exámenes del EC-Council se proporcionan en múltiples formas (es decir, diferentes bancos de preguntas). Cada formulario se analiza cuidadosamente a través de pruebas beta con un grupo de muestra apropiado bajo la guía de un comité de expertos en la materia. Este enfoque garantiza que nuestros exámenes ofrezcan dificultad académica, así como aplicaciones del "mundo real". También tenemos un proceso para determinar la calificación de dificultadde cada pregunta. La calificación individual contribuye entonces a una "puntuación de corte" general para cada formulario de examen. Para garantizar que cada formulario cumpla con los estándares de evaluación, los puntajes de corte se establecen "por formulario de examen". Según el formulario de examen que se cuestione, las puntuaciones de corte pueden oscilar entre el 60 % y el 85 %

Esquema del curso

Module 01	Ataques de red y estrategias de defensa
Module 02	Seguridad de red administrativa
Module 03	Seguridad técnica de la red
Module 04	Seguridad perimetral de la red
Module 05	Endpoint Security-Sistemas Windows
Module 06	Endpoint Security-Sistemas Linux

Módulo07	Seguridad de punto final: dispositivos móviles
Módulo08	Dispositivos IoT de seguridad de punto final
Módulo09	Datos de seguridad de aplicaciones administrativas
Módulo10	Seguridad
Módulo11	Seguridad de red virtual empresarial
Módulo12	Seguridad de red en la nube empresarial
Módulo13	Seguridad de redes inalámbricas empresariales
Módulo14	Supervisión y análisis de tráfico de red
Módulo15	Supervisión y análisis de registros de red
Módulo 16	Respuesta a incidentes e investigación forense
Módulo17	Continuidad del negocio y recuperación ante desastres
Módulo18	Anticipación de riesgos con gestión de riesgos
Módulo19	Evaluación de amenazas con análisis de superficie de ataque
Módulo20	Predicción de amenazas con Cyber Threat Intelligence

¿Qué aprenderás?

- Comprender la seguridad de la red gestión
- Aprenda los conceptos básicos de la primera respuesta y forense
- Establecimiento de la seguridad de la red: Policías y procedimientos
- Entender los indicadores de Compromiso, ataque y Exposures (IoC, IoA, IoE)
- Seguridad Windows y Linux administración
- Creación de inteligencia de amenazas capacidades
- Configuración de dispositivos móviles e IoT seguridad
- Registro de establecimiento y seguimiento gestión
- Implementación de seguridad de datos y técnicas en redes
- Implementación de seguridad de punto final
- Integración de virtualización seguridad tecnológica
- Configurar un firewall con soluciones óptimas
- Determinación de la nube y la tecnología inalámbrica seguridad
- Comprensión y uso de IDS/IPS tecnologías
- Implementación y uso del riesgo herramientas de evaluación
- Establecimiento de red Autorización de autenticación, Contabilidad (AAA)

¿Para quién?

CND v2 es para aquellos que trabajan en el dominio de administración de redes/seguridad cibernética en la capacidad de administrador/ingeniero de redes, administrador/ingeniero/analista de seguridad de redes, ingeniero de seguridad cibernética,analista de seguridad, técnico de defensa de redes, operador de seguridad. CND v2 es para todas las operaciones y roles de ciberseguridad y para cualquier persona que busque desarrollar una carrera en ciberseguridad.

Duración sugerida: 5 días (9:00 a. m. a 5:00 p. m.)

Criterio de elegibilidad

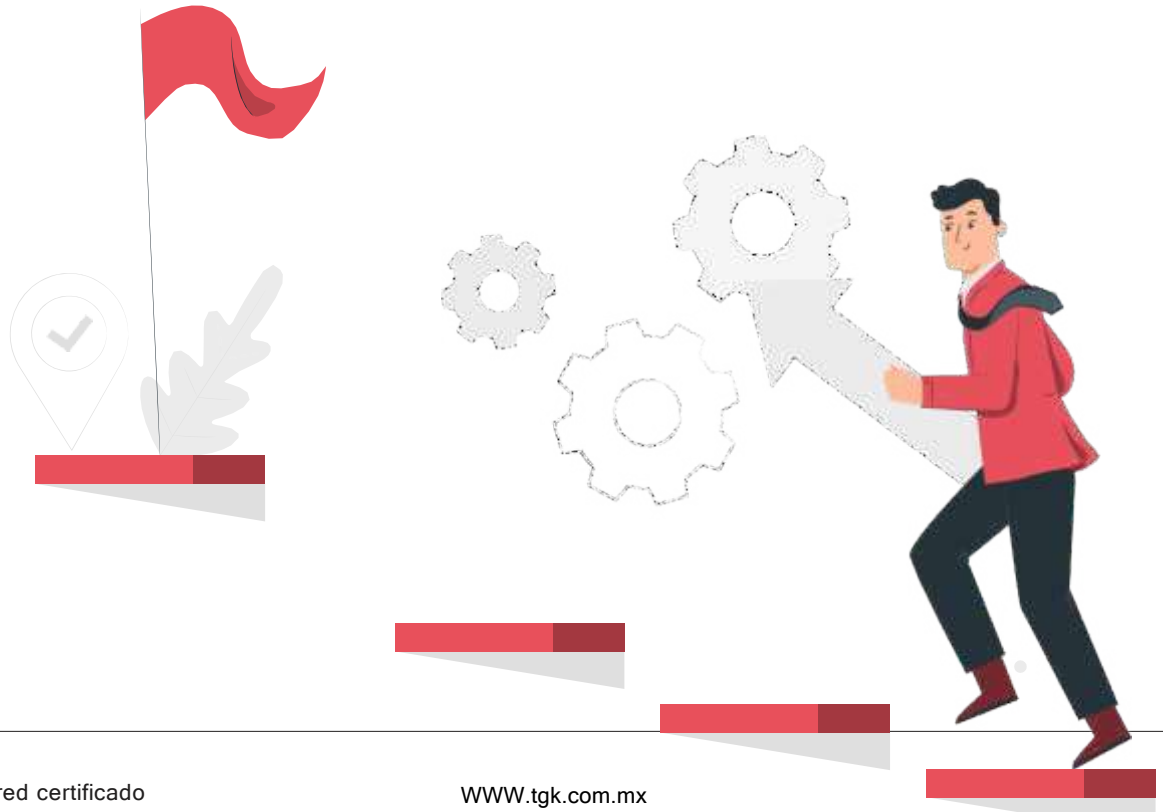
Para ser elegible para impugnar el examen de certificación EC-Council CND, el candidato tiene dosopciones:

Asista a la capacitación oficial de seguridad de redes del Consejo de la CE:

Si un candidato completó una capacitación oficial del EC-Council en un centro de capacitación acreditado, a través de la plataforma iClass o en una institución académica aprobada, el candidato es elegible para desafiar el examen EC-Council correspondiente sin pasar por el proceso de solicitud.

Intentar el examen sin capacitación oficial del EC-Council:

Para ser considerado para el examen EC-Council CND v2 sin asistir a la capacitación oficial en seguridad de redes, el candidato debe tener al menos 2 años de experiencia laboral en el dominio de seguridad de la información. Si el candidato tiene la experiencia laboral requerida, puede enviar un formulario de solicitud de elegibilidad junto con USD 100.00, una tarifa no reembolsable.



Ilearn (Autoaprendizaje)

Esta solución es un entorno de estudio autodirigido para ofrecer el CND v2 de EC-Council programa en un formato de transmisión de video.

iWeek (en vivo en línea)

Esta solución proporciona capacitación CND v2 en vivo, en línea y dirigida por un instructor. Puedes asistir desde cualquier lugar, siempre y cuando tenga

Capacitación dirigida por un instructor de capacitación

CND v2 está disponible en todo el mundo a través de los socios decapacitación autorizados de EC-Council y está convenientemente ubicado en su área y le ofrece el beneficio de aprender a través de EC-Council certificado . experimentado. instructores junto con sus compañeros, . ganando las habilidades del mundo real juntos.

Socio educativo

This solution offers CND v2 through EC-Council Instituciones académicas asociadas y es para enrolled in the applicable college or university degree programs.

Clase maestra

Esta solución le ofrece la oportunidad de aprender Certified Network Defender de los instructores de clase mundial en colaboración con los mejores profesionales de la seguridad de la información.

Acreditaciones, Reconocimientos y Avales

Estándares Nacionales Americanos Instituto (ANSI)

Comunicaciones Gubernamentales Sede (GCHQ)

Departamento de los Estados Unidos de Defensa (DoD)

Infocomunicación Nacional Marco de competencias

Testimonios

"EC-Council ofrece programas exhaustivos con un elaborado contenido de formación. Mi aprendizaje del programa Certified Network Defender (C|ND) me ayudó en mi vida profesional. Con este conocimiento obtenido, pude analizar las vulnerabilidades en la seguridad de la red de nuestra organización. También contribuí con mis insumos para fortalecer la infraestructura de seguridad existente en mi lugar de trabajo.

Raimundo Felipe Gamboa

Subgerente - Operaciones de servicio, Daimler Mobility AG, Singapur

---

"Para mí, el programa Certified Network Defender (C|ND) de EC-Council cubría todo el dominio de seguridad de la red. Es un programa integral e independiente del proveedor que se enfoca en protocolos de red, controles, vulnerabilidades, dispositivos y mucho más. El programa incluye laboratorios prácticos para ofrecer una mejor comprensión de todas las principales herramientas y técnicas de seguridad de red.

George L.S.

Endpoint Protection/Administrador de ACAS, Jacobs, EE. UU.

"Para todos aquellos apasionados por aprender seguridad de redes, su primera parada debe ser Defensor de red certificado por el EC-Council (C|ND). El material didáctico de C|ND me ayudó a comprender los diferentes módulos del programa. Además, no existe ningún otro programa de capacitación que pueda cubrir este dominio con dicha información. No habría podido obtener la credencial C|ND sin pasar por esta capacitación avanzada. Mi experiencia incluye laboratorios de alta calidad, entrega de contenido brillante por parte de un instructor experimentado y conocimiento enciclopédico del dominio. También cubrió varios temas importantes de redes que hicieron que toda esta experiencia de aprendizaje se relacionara con escenarios del mundo real. Después de esto, estoy planeando progresar más a través del camino de

Geoffrey Chisnal

Administrador de seguridad de redes, Experian, Sudáfrica

"Mi experiencia con EC-Council desde la primera capacitación en 2015 hasta ahora ha sido una excelente oportunidad. El software del curso y el material de capacitación, en comparación con los cursos de capacitación de otros proveedores, son mucho mejores y mejoran a lo largo de los años con cada nueva actualización de versión y lanzamiento de credenciales.

Ivica Gjorgjevski

Jefe del Departamento de Acreditación de Seguridad de Información Clasificada y soporte de TIC, Dirección de Seguridad de Información Clasificada, Macedonia del Norte

---

"Después de terminar mi contrato con el Ejército, New Horizons Computer Learning Centers me ofreció capacitación profesional en Ciberseguridad. Quería tomar el Defensor de red certificado (C|ND) de EC-Council debido a su gran cantidad de material de capacitación. Me emocionó poder aprender y probar mis habilidades en diferentes conceptos de seguridad de redes. Encontré su material de origen bien escrito y lleno de nueva información. El entrenamiento de C|ND me recordó siempre estar alerta. Nunca dejes de aprender porque siempre hay algo nuevo por descubrir.

Kenneth P.

Investigador, IEEE, España

EC-Council

Envia un Correo a:
academiaciber@tgk.com.mx
Siguenos en nuestras redes