

CND
Certified Network Defender

CERTIFIED NETWORK DEFENDER



**TRAIN FOR NEXT GENERATION
NETWORK SECURITY**



Protect



Detect



Respond



Predict

CIND: LA CREDENCIAL QUE ESTABLECE EL ESTÁNDAR GLOBAL PARA LAS HABILIDADES DE SEGURIDAD DE RED Y CONSTRUYE CARRERAS EN SEGURIDAD DE RED Y BLUE TEAM

Las habilidades de seguridad de red están en alta demanda tanto entre las organizaciones como entre los aspirantes a ciberseguridad.

1. ALTAMENTE DEMANDADO POR LAS ORGANIZACIONES:

La creciente frecuencia y sofisticación de los ciberataques ha contribuido a una demanda creciente de profesionales de seguridad de red. La seguridad de red es un aspecto crítico de la ciberseguridad, ya que proteger la integridad, la confidencialidad y la disponibilidad de los datos dentro de las redes es una prioridad principal para las organizaciones.

2. HABILIDAD FUNDAMENTAL ESENCIAL:

Dominar la seguridad de red es una habilidad fundamental esencial para los aspirantes a profesionales de ciberseguridad, ya que implica fortalecer firewalls, implementar protocolos de cifrado sólidos y configurar sistemas de detección de intrusiones —elementos fundamentales vitales para asegurar la compleja red de sistemas interconectados contra amenazas cibernéticas sofisticadas, garantizando la integridad, la confidencialidad y el funcionamiento fluido de la red.



Defensor de Redes Certificado

El programa de capacitación en seguridad de redes más completo y práctico del mundo

La seguridad de red es una de las habilidades de ciberseguridad más demandadas. (TechTarget, LinkedIn, Shiksha, Harvard blog, EC-Council)



QUE ES EL

Defensor de Redes Certificado por EC-Council

(C|ND) PROGRAMA?

Los estudiantes aprenderán las habilidades críticas necesarias para defender sus redes y entornos operativos a través de redes locales, endpoints, infraestructura en la nube, aplicaciones, OT y dispositivos móviles. También adquirirán conocimientos sobre análisis adecuado y efectivo de registros, monitoreo del tráfico de red, investigación y respuesta básicas, así como continuidad del negocio y recuperación ante desastres.

Además, profundizarán en amenazas, analizando la superficie de ataque y estudiando la predicción de amenazas e inteligencia de amenazas en relación con sus responsabilidades de administración y defensa.

Frecuentemente referido como blue-teaming, los C|ND podrán aplicar estrategias de defensa y contramedidas en sus organizaciones, desempeñando un papel fundamental no solo en la prevención de ataques, sino también en la detección, respuesta y remediación mientras configuran redes y sistemas para operar de manera segura.

El programa C|ND cubrirá los conceptos y fortalecerá las habilidades mediante práctica práctica en más de 100 laboratorios ejecutados en máquinas objetivo reales.

El programa C|ND, diseñado por expertos de la industria, prepara a los defensores de redes con capacidades estratégicas, tecnológicas y operativas de seguridad de red, permitiéndoles diseñar, desarrollar y mantener las redes seguras.

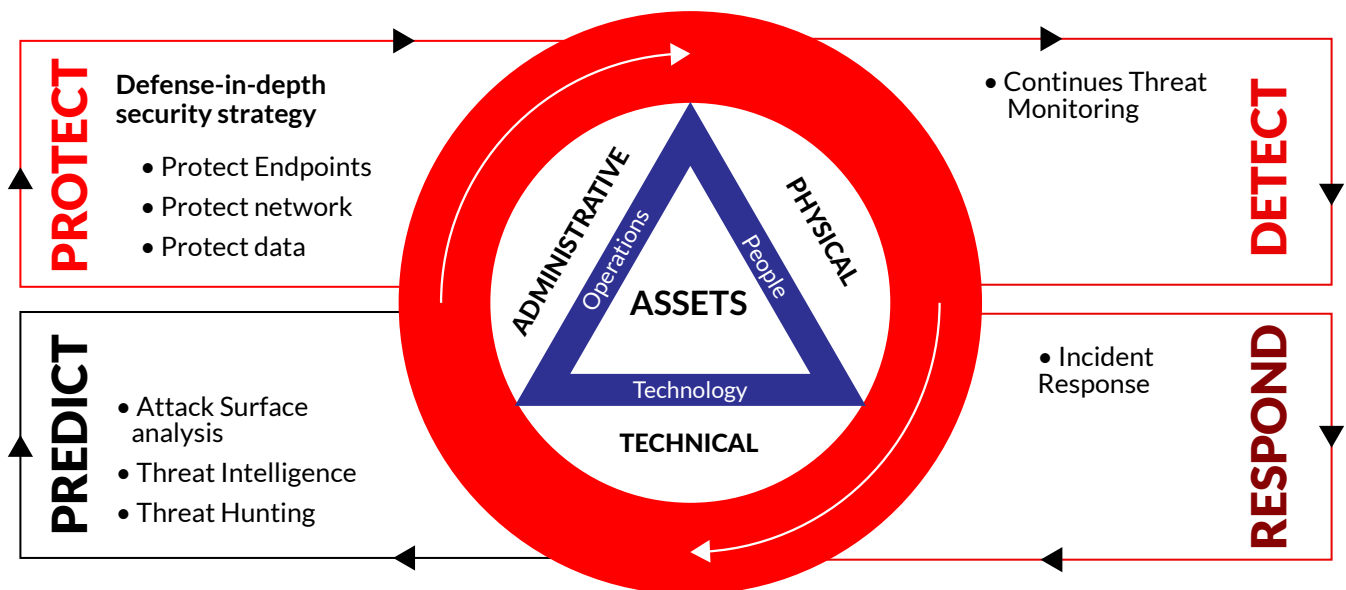
C|ND ES EL PRIMERO DEL MUNDO

PROGRAMA DE SEGURIDAD DE RED

CON UNA ESTRATEGIA DE SEGURIDAD CONTINUA/ADAPTATIVA:

1. Proteger 2. Detectar 3. Responder 4. Predecir

Según Gartner, “los enfoques tradicionales de ‘prevenir y detectar’ son insuficientes”. Por naturaleza oportunista, los actores maliciosos buscan las formas más fáciles de atacar a la mayoría de los usuarios y obtener el máximo beneficio. Desarrollar un Ciclo de Seguridad Adaptativa continuo ayuda a las organizaciones a mantenerse un paso adelante de los ciberdelincuentes mediante la creación y mejora de sistemas de seguridad. Y eso es justamente lo que se aprende en el programa C|ND.



C|ND Course Modules:

1. Network Attacks and Defense Strategies.....	01
2. Administrative Network Security.....	02
3. Technical Network Security.....	04
4. Network Perimeter Security.....	05
5. Endpoint Security - Windows Systems.....	06
6. Endpoint Security - Linux Systems.....	07
7. Endpoint Security - Mobile Devices.....	08
8. Endpoint Security - IoT Devices.....	09
9. Administrative Application Security.....	10
10. Data Security.....	11
11. Enterprise Virtual Network Security.....	12
12. Enterprise Cloud Network Security.....	13
13. Enterprise Wireless Network Security.....	14
14. Network Traffic Monitoring and Analysis.....	15
15. Network Logs Monitoring and Analysis.....	16
16. Incident Response and Forensic Investigation.....	17
17. Business Continuity and Disaster Recovery.....	18
18. Risk Anticipation with Risk Management.....	19
19. Threat Assessment with Attack Surface Analysis.....	20
20. Threat Prediction with Cyber Threat Intelligence.....	21

APPENDIX (Self-Study)

APPENDIX A: Fundamentos de redes computacionales

APPENDIX B: Seguridad física de redes

APPENDIX C: Seguridad de redes privadas virtuales (VPN)

APPENDIX D: Seguridad de endpoints – Sistemas MAC



¿QUÉ APRENDERÁS?

1. Planificar y administrar la seguridad de red para organizaciones
2. Reconocer riesgos, amenazas y vulnerabilidades de seguridad
3. Garantizar el cumplimiento de normas y estándares regulatorios
4. Diseñar e implementar políticas de seguridad de red
5. Aplicar principios de seguridad en entornos de computación distribuida y móvil
6. Implementar Gestión de Identidad y Acceso, cifrado y segmentación de red
7. Administrar la seguridad de Windows y Linux
8. Abordar riesgos de seguridad en dispositivos móviles e IoT
9. Implementar técnicas sólidas de seguridad de datos
10. Gestionar la seguridad en tecnologías de virtualización y plataformas en la nube
11. Implementar seguridad en redes inalámbricas
12. Realizar evaluaciones de riesgo y vulnerabilidad
13. Proporcionar primera respuesta a incidentes de seguridad
14. Identificar Indicadores de Compromiso e Indicadores de Ataque
15. Integrar inteligencia de amenazas para una defensa proactiva
16. Realizar análisis de superficie de ataque
17. Asistir en la planificación de Continuidad del Negocio y Recuperación ante Desastres
18. Monitorear el tráfico de red y realizar gestión de registros (logs)
19. Gestionar proxy, filtrado de contenido y resolución de problemas de red
20. Endurecer la seguridad de endpoints y seleccionar soluciones de firewall
21. Configurar IDS/IPS para mejorar la seguridad
22. Mantener un inventario de dispositivos de red
23. Proporcionar orientación y capacitación en concientización de seguridad
24. Gestionar AAA para dispositivos de red
25. Revisar registros de auditoría y analizar anomalías de seguridad
26. Mantener y configurar plataformas de seguridad
27. Evaluar productos de seguridad y procedimientos operativos
28. Identificar y clasificar los activos de la organización
29. Implementar herramientas de monitoreo de integridad del sistema
30. Comprender soluciones EDR/XDR y UEBA
31. Realizar procesos PIA para evaluación de privacidad
32. Colaborar en actividades de threat hunting y respuesta a incidentes
33. Comprender plataformas SOAR en operaciones de ciberseguridad
34. Integrar principios de Zero Trust en arquitecturas de seguridad
35. Mantenerse actualizado sobre amenazas cibernéticas emergentes
36. Comprender el rol de la IA/ML en la defensa cibernética

4 CARACTERÍSTICAS CLAVE

Y COMPONENTES CRÍTICOS DEL PROGRAMA C|ND

1

El primer programa de seguridad de redes del mundo con una estrategia de seguridad continua/adaptativa:

1. Proteger 2. Detectar 3. Responder 4. Predecir

2

Cubre la estrategia de seguridad de Defensa en Profundidad:

1. Políticas, procedimientos y concientización 2. Físico
3. Perímetro 4. Red interna 5. Host 6. Aplicación 7. Datos

3

Cubre cuatro enfoques de seguridad:

1. Enfoque preventivo 2. Enfoque reactivo
3. Enfoque retrospectivo 4. Enfoque proactivo

4

Cubre las cinco funciones del Marco de Ciberseguridad NIST (CSF):

1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar

CONSTRUYE TU CARRERA EN SEGURIDAD DE REDES CON C|ND

Ventajas del programa C|ND

- Acreditado por el ANSI National Accreditation Board bajo ANSI ISO/IEC 17024
- Aprobado por el Departamento de Defensa de EE. UU. (US DoD) bajo la Directiva 8570/8140
- Reconocido por el National Cyber Security Centre (NCSC), parte del GCHQ (la agencia de inteligencia, seguridad y ciberseguridad del Reino Unido), que aprueba la formación de EC-Council por cumplir con los requisitos de CYBOK.
- Más de 100 laboratorios prácticos: Más laboratorios que cualquier certificación de seguridad de redes reconocida globalmente.
- Programa intensivo en laboratorios (más del 50% es práctica)
- Cubre los requisitos modernos y avanzados de seguridad de redes
- Mapeado al Marco NICE en las siguientes categorías, áreas de especialidad y roles laborales
- Tu camino hacia una carrera en el blue team
- Domina la defensa en dispositivos móviles e IoT
- Aprende defensa táctica de servicios en la nube (AWS, Azure y GCP)
- Aprendizaje más allá de los aspectos técnicos
- Construye habilidades de defensa perimetral
- Desarrolla competencias prácticas listas para el trabajo en entornos reales
- Aprende las tecnologías y conceptos más recientes para cumplir con los requisitos modernos de seguridad de redes
- Desarrolla habilidades prácticas con más de 100 laboratorios que simulan un entorno en tiempo real
- Aprende análisis profundo de la superficie de ataque
- Mapeado con roles y responsabilidades reales de trabajo de los defensores de redes
- Diseñado y desarrollado por expertos en la materia (SMEs) de todo el mundo

CIND CUBRE SEGURIDAD DE REDES MODERNA Y AVANZADA

REQUISITOS DE SEGURIDAD:

- Seguridad de dispositivos móviles empresariales
- Seguridad de dispositivos IoT empresariales
- Seguridad en la nube
- Seguridad de redes virtuales
- Seguridad SDN
- Seguridad NFV
- Seguridad Docker
- Seguridad de contenedores
- Seguridad en Kubernetes
- Inteligencia de amenazas
- Cacería de amenazas (Threat Hunting)
- Detección y respuesta en endpoints (EDR)
- Detección y respuesta extendida (XDR)
- Analítica del comportamiento de usuarios y entidades (UEBA)
- Orquestación, automatización y respuesta de seguridad (SOAR)

DETALLES DE CAPACITACIÓN Y EXAMEN

Detalles de la capacitación:



iLearn (Autoestudio)

Esta solución es un entorno asincrónico de autoestudio en formato de transmisión de video.



iWeek (En vivo online)

Esta solución es un curso de capacitación en línea, en vivo y dirigido por un instructor.



Partner de Capacitación (Presencial)

Esta solución ofrece capacitación “presencial”, lo que le permite beneficiarse de la colaboración con sus compañeros y adquirir experiencia del mundo real guiada por instructores expertos y certificados.

Detalles del Examen:

Código del examen:

312-38

Duración

4 horas

Disponibilidad:

**EC-Council
Exam Portal**

Formato del Test:

Selección múltiple

ROLES LABORALES CON CIND

C|ND es un curso de seguridad de redes diseñado para ayudar a las organizaciones a crear y desplegar el sistema de seguridad de red más completo. C|ND está mapeado a los roles laborales que se indican a continuación, basados en marcos de roles comúnmente reconocidos por organizaciones a nivel mundial. C|ND es un curso de seguridad de redes diseñado para ayudar a las organizaciones a crear y desplegar el sistema de defensa de red más completo.



**Administradores
de red**



**Administradores de
seguridad de redes**



**Ingeniero
redes**



**Operador de
seguridad**



**Analista de
seguridad de
datos**



**Ingeniero de
seguridad de redes**



**Técnico en
defensa de redes**



**Analista de
seguridad**



**Ingeniero en
ciberseguridad**



**Seguridad de
redes**

¿Quiénes pueden postular?

Estudiantes / Profesionales de TI / Cualquier otro profesional de la industria que esté planificando una carrera en ciberseguridad. Cualquier persona que desee iniciar una carrera en el blue team y en la seguridad de redes.

Salarios

El salario promedio de un ingeniero de seguridad de redes en

Estados Unidos es **\$125,014**.

RECONOCIMIENTO / RESPALDO / MAPEAMIENTO

NICE

100% mapping to NICE
Workforce Framework
for Cybersecurity

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION
BODY

United States
Department
of Defense
(DoD)

¿Por qué los mejores profesionales de seguridad de redes de todo el mundo aman el programa CIND?



Robinson Shai

SudAfrica

Profesional de
ciberseguridad

Otros programas enfatizan la comprensión de las redes, pero C|ND muestra las debilidades en una red y cómo cubrirlas para proteger las redes. C|ND es la única certificación que presta tanta atención a la seguridad. Para ingresar a la ciberseguridad, deberías optar por una certificación que te dé una comprensión de una red y te enseñe cómo asegurarla. No hay manera de defender una red sin saber cómo funciona. C|ND te enseña sobre una red y cómo puedes incorporar seguridad dentro de una red. C|ND cubre una amplia variedad de temas, incluidos asegurar el almacenamiento de datos, proteger máquinas, configurar sitios de red e incluso profundiza en medidas de seguridad física como cámaras y sistemas de control de acceso.



Samuel Boateng
USA
**Presidente y Director
Ejecutivo de Slamm
Technologies**

También me ha ayudado a lograr mucho y obtener certificaciones más altas en el campo porque sentó una gran base para mi vida y mi carrera. Una de las cosas buenas de C|ND es que no se puede comparar con ningún otro programa. C|ND viene con un enfoque único hacia las redes, y la forma en que integra la seguridad hace que sea fácil de entender. En C|ND aprendes las siete capas del modelo OSI, comprendes el concepto básico de cómo ensamblar todo y entiendes que tu red es el área clave. C|ND te enseña a monitorear el análisis de registros, lo que muestra cómo los logs pueden analizarse e investigarse. Y esa es mi parte favorita. C|ND proporciona conocimiento sobre cómo asegurar tus sistemas, la infraestructura y cada parte de tu Internet de las Cosas. Te muestra todo lo que necesitas saber sobre seguridad.

C|ND ha mejorado mis conocimientos de tal manera que pude utilizar ese conocimiento en el entorno operativo y estratégico, y aplicarlo para aumentar la seguridad de las redes de la empresa. Hay muchos proveedores de seguridad y programas de capacitación en el mercado. Pero ninguno puede compararse con C|ND. C|ND es el programa más completo que cubre todos los temas necesarios relacionados con la seguridad de redes.

Lo primero que me gusta del programa C|ND es que cubre los principales enfoques de ciberseguridad, como la seguridad preventiva, reactiva, retrospectiva y proactiva. Esto ayuda a planificar, establecer y mantener la seguridad en la red, así como reaccionar correctamente en caso de un incidente.



Ivica Gjorgjevski
USA
**Oficial de Seguridad de la
Información, Stopanska
Banka Macedonia**



ORGANIZACIONES QUE EMPLEAN A MIEMBROS CERTIFICADOS CIND



EC-Council

Building A Culture Of Security

Sobre EC-Council

EC-Council inventó el Certified Ethical Hacker. Fundado en 2001 en respuesta al 11 de septiembre, la misión de EC-Council es proporcionar la capacitación y las certificaciones que los profesionales de ciberseguridad, tanto aprendices como experimentados, necesitan para mantener a salvo de ataques a las corporaciones, agencias gubernamentales y otras entidades que los emplean. Conocido principalmente por su programa Certified Ethical Hacker, hoy EC-Council ofrece 200 programas de capacitación, certificaciones y grados en todo, desde Investigación Forense Computacional y Análisis de Seguridad hasta Inteligencia de Amenazas y Seguridad de la Información. Como organización acreditada ISO/IEC 17024, reconocida bajo la Directiva 8140/8570 del Departamento de Defensa de los Estados Unidos y por muchos otros organismos de ciberseguridad en todo el mundo, la compañía ha certificado a más de 350,000 profesionales a nivel global. Con la confianza de siete de las Fortune 10, la mitad de las Fortune 100 y diversas agencias públicas y privadas en 140 naciones, EC-Council es el estándar de oro en educación y certificación en ciberseguridad. Una verdadera organización global, con una firme convicción en promover la diversidad, la equidad y la inclusión en la fuerza laboral moderna de ciberseguridad, EC-Council mantiene 11 oficinas en EE. UU., el Reino Unido, India, Malasia, Singapur e Indonesia. Si deseas, puedo convertir todo este contenido en un brochure listo para enviar a empresas o para tu OTEC Brainamics.

www.eccouncil.org