Certified Network Defender (CND)

Der Certified Network Defender von EC-Council ist eine unverzichtbare, herstellerunabhängige Sicherheitszertifizierung.

Seminar	8 Termine verfügbar	Zertifikat
Präsenz / Virtual Classroom	40 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 31772 | Herstellernummer: EC-CND

Stand: 23.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31772

Die Teilnehmer erlernen Fähigkeiten, die erforderlich sind, um ihre Netzwerke und Betriebsumgebungen in lokalen Netzwerken, Endpunkten, Cloud-Infrastrukturen, Anwendungen, OT und Mobilgeräten zu schützen. Darüber hinaus werden auch Kenntnisse über eine effektive, ordnungsgemäße Protokollanalyse, die Überwachung des Netzwerkverkehrs, grundlegende Untersuchungen und Reaktionen sowie Business Continuity und die Wiederherstellung im Katastrophenfall erworben. Weiterhin werden Bedrohungen thematisiert, Angriffsflächen analysiert und Bedrohungsdaten im Hinblick auf Verwaltungsaufgaben untersucht.

Nutzen

CND ist unerlässlicher Schritt für Arbeitgeber, die unangreifbare Cyberverteidigungsverfahren aufbauen wollen. Ziel des Kurses ist es, Unternehmen zu befähigen, sich gegen Netzwerkangriffe zu schützen. Der Kurs ist aus den folgenden Gründen ideal für Cybersecurity geeignet:

- Basierend auf Common Job Role Frameworks, die von Organisationen auf der ganzen Welt anerkannt sind.
- ANSI/ISO/IEC 17024-akkreditiertes Zertifizierungsprogramm.
- Abgestimmt auf den NICE 2.0 Rahmen.
- Der Schwerpunkt liegt auf den neuesten Technologien, darunter Cloud, IoT, Virtualisierung und Bedrohungen durch Remote Worker, Angriffsflächenanalyse, Threat Intelligence, Software Defined Networks (SDN) und Network Function Virtualization (NFV) sowie Docker, Kubernetes und Container-Sicherheit.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Enthält die neuesten Tools, Techniken und Methoden, die von führenden Cybersecurity-Experten auf der ganzen Welt eingesetzt werden.

Zielgruppe

Certified Network Defender richtet sich an Personen, die über grundlegende Kenntnisse im Bereich Netzwerkkonzepte verfügen. Darüber hinaus sind die Inhalte auch für die unten genannten Berufsgruppen geeignet:

- Netzwerk-Administratoren
- IT-Administratoren
- Netzwerk-Ingenieure
- Datenanalysten
- Netzwerktechniker

Abschluss

Zertifikat

EC-Council-Zertifikatsprüfung: Certified Network Defender (CND), Nr. 312-38 Die vierstündige CND-Prüfung besteht aus Multiple Choice Aufgaben und ist in englischer Sprache verfügbar. Wir empfehlen nach dem Seminar eine individuelle Nachbereitung vor der Prüfung. Mehr dazu erklärt Ihnen der CND-zertifizierte Trainer im Seminar.

Aktueller Hinweis zur EC-Council CND-Prüfung: Die Abschlussprüfung findet ausschließlich online proctored und remote statt. Nach dem Seminar und eingereichtem Kursfeedback bekommen Sie direkt von EC-Council einen Examensvoucher mit Informationen zur Prüfungsprozedur.

Der Prüfungsvoucher hat eine Gültigkeit von 12 Monaten.

Inhalte des Seminars

- Modul 01: Netzwerkangriffe und Verteidigungsstrategien
- Modul 02: Administrative Netzwerksicherheit
- Modul 03: Technische Netzsicherheit
- Modul 04: Sicherheit am Netzwerkrand
- Modul 05: Endpunktsicherheit - Windows-Systeme
- Modul 06: Endpunktsicherheit-Linux-Systeme
- Modul 07: Endpunktsicherheit - Mobile Geräte

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Modul 08: Endpunktsicherheit - IoT-Geräte
- Modul 09: Sicherheit von Verwaltungsanwendungen
- Modul 10: Datensicherheit
- Modul 11: Sicherheit im virtuellen Unternehmensnetzwerk
- Modul 12: Netzwerksicherheit in der Unternehmens-Cloud
- Modul 13: Sicherheit von drahtlosen Unternehmensnetzwerken
- Modul 14: Überwachung und Analyse des Netzwerkverkehrs
- Modul 15: Überwachung und Analyse von Netzwerkprotokollen
- Modul 16: Reaktion auf Zwischenfälle und forensische Untersuchungen
- Modul 17: Geschäftskontinuität und Wiederherstellung im Katastrophenfall
- Modul 18: Risikovorwegnahme mit Risikomanagement
- Modul 19: Bedrohungsbewertung mit Angriffsflächenanalyse
- Modul 20: Bedrohungsvorhersage mit Cyber Threat Intelligence

Wichtige Hinweise

- Es wird die aktuelle Kursversion geschult.
- Der Kurs findet in deutscher Sprache statt. Der Kurstrainer spricht sowohl Deutsch als auch Englisch.
- Die Kursunterlagen, Dokumentationen und die Abschlussprüfung sind nur auf Englisch verfügbar.
- Die im Seminar bereitgestellte Übungsumgebung steht Ihnen nach der Aktivierung zu Seminarbeginn für 6 Monate zur Verfügung, sodass Sie auch nach dem Training die Übungen zur Vertiefung des Gelernten nutzen können.
- Wir empfehlen eine individuelle Prüfungsvorbereitung nach dem Lehrgang.
- Der Prüfungsvoucher hat eine Gültigkeit von 12 Monaten.
- Die TÜV Rheinland Akademie ist ein akkreditiertes EC-Council Schulungszentrum (Accredited Training Center).

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31772 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.