



Startel

Dé IT-opleider

Certified Network Defender (CND v2) Classroom + examen

De training: “Certified Network Defender (C|ND)” van EC-Council is een uitgebreid lesprogramma dat ontworpen is om cybersecurityprofessionals op te leiden in het beschermen en verdedigen van organisatienetwerken tegen cyberaanvallen.

Algemene omschrijving

De training: “Certified Network Defender (C|ND)” van EC-Council is een uitgebreid lesprogramma dat ontworpen is om cybersecurityprofessionals op te leiden in het beschermen en verdedigen van organisatienetwerken tegen cyberaanvallen. Deze training biedt een diepgaand inzicht in netwerkbeveiligingstechnieken en -praktijken, waardoor deelnemers essentiële vaardigheden verwerven om netwerkinfrastructuren te beschermen tegen potentiële bedreigingen en aanvallen.

Tijdens deze training leer je hoe jij netwerkbeveiligingsstrategieën kunt ontwikkelen, implementeren en onderhouden om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. Door middel van praktische labopdrachten en realistische scenario's word je uitgedaagd om jouw kennis toe te passen en krijg je de gelegenheid om praktische vaardigheden te verkrijgen waarin je gebruikmaakt van de nieuwste hulpmiddelen en technieken op het gebied van netwerkbeveiliging.

Terwijl je werkt met geavanceerde netwerkbeveiligingsapparatuur en -hulpmiddelen, word je begeleid door een ervaren instructeur die zijn expertise deelt vanuit de frontlinie van de industrie. Dit zorgt voor een boeiende en interactieve leerervaring die jou voorbereidt op de uitdagingen van het echte netwerkbeveiligingslandschap.

De training: “Certified Network Defender (C|ND)” bestaat uit verschillende onderwerpen, zoals netwerkverdedigingstechnieken, netwerkbeveiligingsbeheer, netwerkpenetratietesten, het reageren op beveiligingsincidenten en het uitvoeren van forensische onderzoeken. Door deze onderwerpen grondig te verkennen, krijgen jij een diepgaande kennis van netwerkbeveiliging en word jij uitgerust met de benodigde vaardigheden om effectief te reageren op cyberaanvallen en hoe jij jouw organisatie hiertegen kunt beschermen.

Na afloop van de training en het behalen van het afsluitend certificeringsexamen word je beloond met het certificaat: “Certified Network Defender (C|ND)” van EC-Council. Met dit certificaat bewijs jij jouw bekwaamheid in het verdedigen van bedrijfsnetwerken tegen potentiële bedreigingen en ontdek jij nieuwe carrièremogelijkheden en groeipaden binnen het domein van netwerkbeveiliging.

Doelgroep

Deze training is met name geschikt voor de volgende mensen:

- **Netwerkbeheerders**
 - Als netwerkbeheerder ben je verantwoordelijk voor het beheren en onderhouden van de netwerkinfrastructuur van jouw organisatie. De training: "Certified Network Defender (C|ND)" van EC-Council kan jou helpen om jouw kennis en vaardigheden op het gebied van netwerkbeveiliging te versterken.
 - Door deze training te volgen kun je effectiever netwerken beveiligen tegen cyberbedreigingen en potentiële aanvallen identificeren en beperken, waardoor je de algehele veiligheid en betrouwbaarheid van je netwerk verbetert.
- **Cybersecurityprofessionals**
 - Als cybersecurityprofessional ben je belast met het beschermen van organisaties tegen cyberaanvallen en het waarborgen van de integriteit en vertrouwelijkheid van gegevens. De training: "Certified Network Defender (C|ND)" biedt jou gespecialiseerde kennis en vaardigheden op het gebied van netwerkbeveiliging, waardoor je effectiever kunt reageren op en verdedigen tegen potentiële bedreigingen.
 - Met deze training kun jij jezelf positioneren als een waardevolle aanwinst voor jouw organisatie en bijdragen aan het verbeteren van de algehele cyberbeveiliging.
- **Systeembeheerders en beveiligingsanalisten**
 - Als systeembeheerder of beveiligingsanalist ben je verantwoordelijk voor het beheren en monitoren van de ICT-infrastructuur en het identificeren van mogelijke beveiligingsrisico's. De training: "Certified Network Defender (C|ND)" voorziet jou van de benodigde kennis en hulpmiddelen om netwerken te verdedigen tegen cyberaanvallen en proactief beveiligingsmaatregelen te implementeren.
 - Met deze training kun jij jouw bekwaamheid vergroten en een effectievere rol spelen in het beschermen van de organisatie tegen cyberdreigingen.

Leerdoelen CND

Door deze training te volgen zul je de volgende kennis en vaardigheden verkrijgen:

- Netwerkbeveiligingsbeheer.
- Netwerkbeveiligingsbeleid en -procedures.
- Het beheren van de beveiliging van Windows- en Linux-computers.
- Mobiele en IoT-apparaten beveiligen.
- Technieken voor gegevensbeveiliging.
- Beveiliging van virtualisatietechnologie.
- Cloud- en draadloze beveiliging.
- Hulpmiddelen voor het beoordelen van risico's.
- Grondbeginselen van eerste reactie en forensisch onderzoek.
- Indicatoren van compromittering, aanvallen en blootstellingen (IoC, IoA, IoE).
- Mogelijkheden voor dreigingsinformatie.
- Logboekbeheer.
- Beveiliging van eindpunten.
- Firewall-oplossingen.
- IDS/IPS-technologieën.
- Netwerkverificatie, autorisatie, accounting (AAA).

Voorkennis CND

Je hebt geen specifieke voorkennis nodig om deel te mogen nemen aan deze training. Echter zou basiskennis van computernetwerken en netwerkbeveiliging goed van pas komen om deze training zo goed mogelijk te kunnen volgen.

Onderwerpen CND

Course Outline:

- **CND | Module 01:** Network Attacks and Defense Strategies.
- **CND | Module 02:** Administrative Network Security.
- **CND | Module 03:** Technical Network Security.
- **CND | Module 04:** Network Perimeter Security.
- **CND | Module 05:** Endpoint Security - Windows Systems.
- **CND | Module 06:** Endpoint Security - Linux Systems.
- **CND | Module 07:** Endpoint Security - Mobile Devices.
- **CND | Module 08:** Endpoint Security - IoT Devices.
- **CND | Module 09:** Administrative Application Security.
- **CND | Module 10:** Data Security.
- **CND | Module 11:** Enterprise Virtual Network Security.
- **CND | Module 12:** Enterprise Cloud Network Security.
- **CND | Module 13:** Enterprise Wireless Network Security.
- **CND | Module 14:** Network Traffic Monitoring and Analysis.
- **CND | Module 15:** Network Logs Monitoring and Analysis.
- **CND | Module 16:** Incident Response and Forensic Investigation.
- **CND | Module 17:** Business Continuity and Disaster Recovery.
- **CND | Module 18:** Risk Anticipation with Risk Management.
- **CND | Module 19:** Threat Assessment with Attack Surface Analysis.
- **CND | Module 20:** Threat Prediction with Cyber Threat Intelligence.