Rumos valorizamos profissionais!

# Certified Network Defender (CND)

- **Formato do curso:** Presencial e Live Training
- **Com certificação:** EC-Council Certified Network Defender (CND)
- **Preço:** 1700€
- **Nível:** Intermédio
- **Duração:** 35 horas

**O verdadeiro programa em Network Defender para as blue teams!**

A segurança cibernética agora domina as prioridades de todas as empresas que se esforçam para se adaptar a um mundo pós-COVID. Forçados a se deslocarem remotamente, as identidades e os dispositivos de seus funcionários são o novo perímetro de segurança. Na verdade, a segurança cibernética para as empresas agora é tão crítica quanto o próprio acesso à Internet.

Estudos e relatórios de notícias demonstraram que os hackers são rápidos para atacar o novo, as superfícies de ameaça desprotegidas foram criadas quando milhões de colaboradores começaram a trabalhar em casa. Fornecer segurança de rede a um ecossistema distribuído sem precedentes neste mundo pós-pandémico é um teste para cada equipa de defesa de rede.

O programa Certified Network Defender v2 foi atualizado e munido para ajudar as *blue teams* a defender e vencer a guerra contra violações de rede.

Os profissionais e as empresas que procuram fortalecer as suas competências em defesa de redes consideram o CND v2 um *must-have* por 5 motivos:

- O único programa de defesa de redes que é desenvolvido para incorporar as principais competências críticas na segurança de redes – **Proteger, Detectar, Responder e Prever**
- Alinhado com a NICE 2.0 Framework
- Inclui as **mais recentes** ferramentas, tecnologias e técnicas
- Implementa uma abordagem orientada à **prática para a aprendizagem**
- Projetado para focar na **previsão de ameaças, continuidade do negócio e recuperação de desastres**

**Certificação**

Este curso inclui um voucher para o exame C|ND – *Certified Network Defender* (312-38).

O exame C|ND pode ser realizado após a conclusão do curso completo e oficial C|ND. Os candidatos quem passem no exame receberão o seu certificado C|ND e privilégios associados.

**Exame:**

- Número de perguntas: 100
- Duração: 4 horas
- Formato de teste: Escolha múltipla
- Prefixo do exame: 312-38 (ECC EXAM)

**O que é abordado no curso:**

- Gestão da segurança de redes
- Políticas e procedimentos de segurança de redes
- Administração de segurança em Windows e Linux
- Segurança em dispositivos Mobile e IoT
- Técnicas em Data security
- Tecnologias de segurana em virtualização
- Segurança em Cloud e wireless
- Ferramentas de Risk assessment
- Principios de resposta e técnicas forenses
- Indicadores de compromisso, ataque e exposures (IoC, IoA, IoE)
- Capacidades de inteligência para lidar com ameaças
- Log management
- Endpoint security
- Solções de Firewall
- Tecnologias IDS/IPS
- Autenticação em redes, autorização e gestão – Network Authentication, Authorization, Accounting (AAA)

> While there will be over 1.5 million cyber security jobs that remain unfilled by 2019, millions of IT and Network administrators remain untrained on network defense techniques.
>
> Michael Brown, CEO at Symantec

Este curso também está disponível no formato E-learning. Para mais informações aceda ao link: Certified Network Defender (CND)

## Destinatários

- O CND v2 é direcionado para administradores de redes e segurança cibernética, Engenheiros de Redes, Administradores, Engenheiros de Segurança Cibernética, Analistas de Segurança, Técnicos de Defesa de Rede e Operadores de Segurança.
- O CND v2 é direcionado a todos os profissionais de cibersegurança e para qualquer pessoa que queira construir sua carreira em segurança informática.

---

## Programa

- Network Attacks and Defense Strategies
- Administrative Network Security
- Technical Network Security
- Network Perimeter Security
- Endpoint Security-Windows Systems
- Endpoint Security-Linux Systems
- Endpoint Security- Mobile Devices
- Endpoint Security-IoT Devices
- Administrative Application Security
- Data Security
- Enterprise Virtual Network Security
- Enterprise Cloud Network Security
- Enterprise Wireless Network Security
- Network Traffic Monitoring and Analysis
- Network Logs Monitoring and Analysis
- Incident Response and Forensic Investigation
- Business Continuity and Disaster Recovery
- Risk Anticipation with Risk Management
- Threat Assessment with Attack Surface Analysis
- Threat Prediction with Cyber Threat Intelligence