# Certified Network Defender version 3

Kód kurzu: CNDv3

V tomto školení Certified Network Defender (CND) v3 se připravíš na složení zkoušky EC-Council CND a naučíš se taktické dovednosti potřebné k návrhu a správě zabezpečené sítě. Získáš pevné porozumění obranné bezpečnosti a praktické schopnosti pro zvládnutí všech typů network defense. Naučíš se, jak zajistit bezpečnost dat, správně konfigurovat síťové technologie a instalovat ochranný software pro zvýšení důvěrnosti, integrity a dostupnosti.Školení EC-Council Certified Network Defender (CND) je komplexní program navržený tak, aby poskytl IT profesionálům dovednosti a znalosti potřebné k efektivní ochraně, detekci a reakci na bezpečnostní hrozby v síti. Kurz se zaměřuje na nejnovější nástroje a techniky pro obranu sítě a klade důraz na komplexní a proaktivní přístup k zajištění bezpečnosti moderních síťových prostředí.

## Pro koho je kurz určen

Kurz je velmi vhodný pro správce bezpečnosti počítačových sítí, systémové administrátory, absolventy kurzů etického hackingu, jako jsou GOC3 – Etický hacking v praxi a CEH – Certified Ethical Hacker, a pro každého, kdo hledá účinnou obranu proti jak etickému, tak neetickému hackingu.

## Co vás naučíme

Během pouhých pěti dnů se naučíš používat nástroje, technologie a techniky potřebné k obraně a posílení své sítě proti nové generaci hackerů. Získáš také cenné dovednosti, například jak:

- Vytvářet zásady a postupy pro zabezpečení sítě
- Nastavovat zabezpečení mobilních a IoT zařízení
- Určovat a spravovat zabezpečení cloudových a bezdrátových sítí

## Požadované vstupní znalosti

Doporučujeme předem absolvovat kurz CompTIA Security+. Pevné znalosti správy operačních systémů a znalost síťových protokolů na úrovni kurzů GOC2 a GOC3 jsou povinným požadavkem.

## Osnova kurzu

- Modul 1: Útoky na síť a strategie obrany
- Modul 2: Administrativní zabezpečení sítě
- Modul 3: Technické zabezpečení sítě
- Modul 4: Zabezpečení okrajů sítě (Network Perimeter Security)
- Modul 5: Zabezpečení koncových zařízení – Windows systémy
- Modul 6: Zabezpečení koncových zařízení – Linux zařízení
- Modul 7: Zabezpečení koncových zařízení – mobilní zařízení
- Modul 8: Zabezpečení koncových zařízení – IoT zařízení
- Modul 9: Administrativní zabezpečení aplikací
- Modul 10: Bezpečnost dat
- Modul 11: Zabezpečení virtuálních sítí v podniku
- Modul 12: Zabezpečení cloudových sítí v podniku
- Modul 13: Zabezpečení bezdrátových sítí v podniku
- Modul 14: Monitorování a analýza síťového provozu
- Modul 15: Monitorování a analýza síťových logů
- Modul 16: Reakce na incidenty a forenzní vyšetřování
- Modul 17: Zajištění kontinuity provozu a obnova po havárii
- Modul 18: Predikce rizik s využitím řízení rizik
- Modul 19: Hodnocení hrozeb pomocí analýzy útokové plochy
- Modul 20: Predikce hrozeb s využitím Cyber Threat Intelligence

**GOPAS Praha**
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

**GOPAS Brno**
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

**GOPAS Bratislava**
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk