Certified Network Defender version 3

Kód kurzu: CNDv3

V tomto školení Certified Network Defender (CND) v3 sa pripravíš na zloženie skúšky EC-Council CND a naučíš sa taktické zručnosti potrebné na návrh a správu zabezpečenej siete. Získaš pevné porozumenie obrannému zabezpečeniu a praktické schopnosti pre zvládnutie všetkých typov network defense. Naučíš sa, ako zabezpečiť bezpečnosť dát, správne konfigurovať sieťové technológie a inštalovať ochranný software na zvýšenie dôvernosti, integrity a dostupnosti.Školenie EC-Council Certified Network Defender (CND) je komplexný program navrhnutý tak, aby poskytol IT profesionálom zručnosti a znalosti potrebné na efektívnu ochranu, detekciu a reakciu na bezpečnostné hrozby v sieti. Kurz sa zameriava na najnovšie nástroje a techniky pre obranu siete a kladie dôraz na komplexný a proaktívny prístup k zabezpečeniu moderných sieťových prostredí.

Pre koho je kurz určený

Kurz je veľmi vhodný pre správcov bezpečnosti počítačových sietí, systémových administrátorov, absolventov kurzov etického hackingu, ako sú GOC3 – Etický hacking v praxi a CEH – Certified Ethical Hacker, a pre každého, kto hľadá účinnú obranu proti etickému aj neetickému hackingu.

Čo vás naučíme

Počas iba piatich dní sa naučíš používať nástroje, technológie a techniky potrebné na obranu a posilnenie svojej siete proti novej generácii hackerov. Získaš tiež cenné zručnosti, napríklad ako:

- Vytvárať zásady a postupy pre zabezpečenie siete
- Nastavovať zabezpečenie mobilných a IoT zariadení
- Určovať a spravovať zabezpečenie cloudových a bezdrôtových sietí

Požadované vstupné znalosti

Odporúčame vopred absolvovať kurz CompTIA Security+. Pevné znalosti správy operačných systémov a znalosť sieťových protokolov na úrovni kurzov GOC2 a GOC3 sú povinnou požiadavkou.

Metódy výuky

Vysvetlenie princípov zabezpečovacích opatrení je kombinované s praktickými cvičeniami, ktoré obsahujú podrobné ukážky nasadenia a fungovania ochrany proti hackerským útokom.

Študijné materiály

Originálny manuál EC-Council vo forme e-Courseware.

Osnova kurzu

- Modul 1: Útoky na sieť a stratégie obrany
- Modul 2: Administratívne zabezpečenie siete
- Modul 3: Technické zabezpečenie siete
- Modul 4: Zabezpečenie okrajov siete (Network Perimeter Security)
- Modul 5: Zabezpečenie koncových zariadení – Windows systémy
- Modul 6: Zabezpečenie koncových zariadení – Linux zariadenia
- Modul 7: Zabezpečenie koncových zariadení – mobilné zariadenia
- Modul 8: Zabezpečenie koncových zariadení – IoT zariadenia
- Modul 9: Administratívne zabezpečenie aplikácií
- Modul 10: Bezpečnosť dát
- Modul 11: Zabezpečenie virtuálnych sietí v podniku
- Modul 12: Zabezpečenie cloudových sietí v podniku
- Modul 13: Zabezpečenie bezdrôtových sietí v podniku
- Modul 14: Monitorovanie a analýza sieťového prevádzky

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

- Modul 15: Monitorovanie a analýza sieťových logov
- Modul 16: Reakcia na incidenty a forenzné vyšetrovanie
- Modul 17: Zabezpečenie kontinuity prevádzky a obnova po havárii
- Modul 18: Predikcia rizík s využitím riadenia rizík
- Modul 19: Hodnotenie hrozieb pomocou analýzy útokovej plochy
- Modul 20: Predikcia hrozieb 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