AI Ethical Hacker

Kód kurzu: AIEH

Pro koho je kurz určen Inženýři / analytici kybernetické bezpečnostiDržitelé certifikátu EC Council CEH Držitelé certifikátu OSCP Certifikovaní profesionálové SecOps Certifikovaní profesionálové CompTIA Správci sítí a systémoví administrátoři Inženýři a vývojáři dronů a robotiky Operátoři dronů Vyšetřovatelé digitální forenzní analýzy Penetrační testeři Pracovníci v oblasti cloud computing Manažeři projektů v cloudu Podpora provozu se zájmem o kariérní postupCo Vás naučíme Porozumět základům kybernetické bezpečnosti a etickému hackingu Pochopit základní koncepty, principy a významy etického uvažování v praktikách hackingu Identifikace a hodnocení zranitelností sítě Naučit se AI a strojové učení k posílení útočných nástrojů, technik a taktik Naučit se techniky pro odhalení, analýzu a využití zranitelností v sítích a systémech Ovládat různé nástroje a techniky hackingu Získat praktické zkušenosti s oblíbenými nástroji a metodologiemi hackingu Provádět průzkum a shromažďovat informace Rozvoj dovedností v získávání informací o cílech pomocí pasivních i aktivních metod průzkumu Provádění skenování sítě a enumerace Naučit se používat nástroje pro skenování a výčet síťových zařízení, služeb a otevřených portů k mapování potenciálních útočných vektorů Využívat zranitelností systému a sítě Procvičit využívání identifikovaných zranitelností k získání neoprávněného přístupu a ovládání systémů a sítí Implementace technik hackingu webových aplikací Porozumět běžným zranitelnostem webových aplikací jako je SQL injection, XSS a CSRF a naučit se je účinně využívat Rozvoj dovedností v testování bezpečnosti bezdrátové sítě Naučit se, jak testovat a zabezpečit bezdrátové sítě proti běžným útokům jako jsou prolomení Wi-Fi a man-in-the-middle (MITM) Analýza a obrana proti malwaru a exploitům Studium různých typů malwaru, jejich útočných vektorů a obranných strategií pro zmírnění jejich dopadu na systémy Aplikovat etický hacking v reálných scénářích Účast na praktických cvičeních a simulacích, které imitují reálné kybernetické útoky, s využitím technik etického hackingu k zabezpečení systémů a zlepšení obranyNa konci kurzu budou mít účastníci komplexní porozumění principům etického hackingu, praktické dovednosti v různých hackerských technikách a schopnost aplikovat tyto dovednosti k posílení kybernetických opatření ve svých organizacích.
Osnova kurzuDen 1: Úvod do AI v kybernetické bezpečnosti
Den 2: Techniky AI pro ofenzivní bezpečnost
Den 3: Techniky AI pro defenzivní bezpečnost
Den 4: Pokročilé techniky AI a aplikace v bezpečnosti
Den 5: Integrace umělé inteligence a budoucí trendy

Pro koho je kurz určen

- Inženýři / analytici kybernetické bezpečnostiDržitelé certifikátu EC Council CEH
- Držitelé certifikátu OSCP
- Certifikovaní profesionálové SecOps
- Certifikovaní profesionálové CompTIA
- Správci sítí a systémoví administrátoři
- Inženýři a vývojáři dronů a robotiky
- Operátoři dronů
- Vyšetřovatelé digitální forenzní analýzy
- Penetrační testeři
- Pracovníci v oblasti cloud computing
- Manažeři projektů v cloudu
- Podpora provozu se zájmem o kariérní postup

Co Vás naučíme

- Porozumět základům kybernetické bezpečnosti a etickému hackingu
- Pochopit základní koncepty, principy a významy etického uvažování v praktikách hackingu
- Identifikace a hodnocení zranitelností sítě
- Naučit se AI a strojové učení k posílení útočných nástrojů, technik a taktik
- Naučit se techniky pro odhalení, analýzu a využití zranitelností v sítích a systémech
- Ovládat různé nástroje a techniky hackingu

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Copyright © 2020 GOPAS, a.s.,
All rights reserved

- Získat praktické zkušenosti s oblíbenými nástroji a metodologiemi hackingu
- Provádět průzkum a shromažďovat informace
- Rozvoj dovedností v získávání informací o cílech pomocí pasivních i aktivních metod průzkumu
- Provádění skenování sítě a enumerace
- Naučit se používat nástroje pro skenování a výčet síťových zařízení, služeb a otevřených portů k mapování potenciálních útočných vektorů
- Využívat zranitelností systému a sítě
- Procvičit využívání identifikovaných zranitelností k získání neoprávněného přístupu a ovládání systémů a sítí
- Implementace technik hackingu webových aplikací
- Porozumět běžným zranitelnostem webových aplikací jako je SQL injection, XSS a CSRF a naučit se je účinně využívat
- Rozvoj dovedností v testování bezpečnosti bezdrátové sítě
- Naučit se, jak testovat a zabezpečit bezdrátové sítě proti běžným útokům jako jsou prolomení Wi-Fi a man-in-the-middle (MITM)
- Analýza a obrana proti malwaru a exploitům
- Studium různých typů malwaru, jejich útočných vektorů a obranných strategií pro zmírnění jejich dopadu na systémy
- Aplikovat etický hacking v reálných scénářích
- Účast na praktických cvičeních a simulacích, které imitují reálné kybernetické útoky, s využitím technik etického hackingu k zabezpečení systémů a zlepšení obrany

Na konci kurzu budou mít účastníci komplexní porozumění principům etického hackingu, praktické dovednosti v různých hackerských technikách a schopnost aplikovat tyto dovednosti k posílení kybernetických opatření ve svých organizacích.

Osnova kurzu

Den 1: Úvod do AI v kybernetické bezpečnosti

Den 2: Techniky AI pro ofenzivní bezpečnost

Den 3: Techniky AI pro defenzivní bezpečnost

Den 4: Pokročilé techniky AI a aplikace v bezpečnosti

Den 5: Integrace umělé inteligence a budoucí trendy

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Copyright © 2020 GOPAS, a.s.,
All rights reserved