

Kurs CyberSecurity Engineer

Od analizy sieci po zaawansowane testy penetracyjne. Praktyczny kurs dla osób, które chcą chronić infrastrukturę IT, wykrywać podatności i reagować na ataki.

Poznaj kurs CyberSecurity Engineer



8.06.2026
start kursu



66 h
praktycznych zajęć



Certyfikat
dla uczestników



Dostęp do nagrań
z zajęć



Tryb wieczorowy
poniedziałki i środy
(17:30 – 20:30)



4.9/5
9500+ absolwentów

CZEGO SIĘ NAUCZYSZ?

- ✓ Testy penetracyjne – pełny cykl ataku od rekonesansu po raportowanie
- ✓ Bezpieczeństwo chmurowe – testowanie konfiguracji i zagrożeń w AWS, Azure, GCP
- ✓ Narzędzia pentestera – praktyczna praca z Nmap, Metasploit, Burp Suite, Hashcat
- ✓ Wykorzystywanie błędów konfiguracyjnych i luk w systemach Windows/Linux
- ✓ DevSecOps – integracja bezpieczeństwa w pipeline CI/CD i automatyczne skany
- ✓ Cyber Threat Intelligence – analiza zagrożeń z użyciem MITRE ATT&CK, VirusTotal i Shodan
- ✓ Blue Team – wykrywanie i reagowanie na incydenty (SIEM, Sysmon, ELK, EDR)
- ✓ Projekty praktyczne – realizacja kompletnego scenariusza pentestowego w labie
- ✓ Przygotowanie do egzaminu CPTe – trening do praktycznej certyfikacji Mile2



Azure



AWS



Kali Linux



Wireshark



OWASP



Burp Suite



Metasploit



Linux

PROGRAM KURSU

Moduł 0: Prework

Moduł 1: Wprowadzenie do bezpieczeństwa

Moduł 2: Podstawy sieci i systemów

Moduł 3: Narzędzia i metodyka testów penetracyjnych

Moduł 4: Bezpieczeństwo aplikacji webowych

Moduł 5: Bezpieczeństwo chmurowe i DevSecOps

Moduł 6: Cyber Threat Intelligence i nowoczesna obrona

Moduł 7: Projekty praktyczne i przygotowanie do egzaminu CPTe (Mile2)



MASZ PYTANIA? CHĘTNIE POMOGĘ

Sylwia Liedtke

Doradca

sylwia.liedtke@infoshareacademy.com

+48 730 822 825

Skontaktuj się z nami

Oferujemy zniżki dla zespołów
w zależności od liczby uczestników.