Cybersecurity od podstaw

w CODE:ME

program kursu

1. Wprowadzenie do Cyberbezpieczeństwa

- Podstawowe zagrożenia i pojęcia
- Wprowadzenie do rozpoznania w cyberprzestrzeni

2. Systemy operacyjne – podstawy

- Podstawy systemów operacyjnych
- Instalacja i konfiguracja zabezpieczeń
- Zarządzanie uprawnieniami użytkowników

3. Zarządzanie ryzykiem i politykami

- Analiza ryzyka w cyberbezpieczeństwie
- Tworzenie polityk bezpieczeństwa
- Zarządzanie incydentami i audyty bezpieczeństwa

4. Bezpieczeństwo danych i urządzeń

- Klasyfikacja danych, szyfrowanie, zarządzanie urządzeniami
- Zabezpieczanie danych z użyciem np. BitLocker, VeraCrypt, EFS
- Procedury backupu oraz zarządzanie urządzeniami mobilnymi

5. Architektura bezpieczeństwa sieci

- Zasady projektowania bezpiecznej sieci
- Konfiguracja firewall i segmentacja sieci

6. Bezpieczeństwo komunikacji i ruchu sieciowego

- Protokoły komunikacyjne i zabezpieczenia
- Konfiguracja VPN i zabezpieczeń sieciowych
- Konfiguracja IDS/IPS oraz analiza logów

7. Zarządzanie Tożsamością i Dostępem (IAM)

- Zarządzanie dostępem, SSO, MFA
- Implementacja Single Sign-On, federacja tożsamości oraz Multi-Factor Authentication
- Audyt i analiza aktywności użytkowników

Cybersecurity od podstaw

w CODE:ME

program kursu

8. Analiza i Weryfikacja bezpieczeństwa systemów

- Metody testowania, testy penetracyjne
- OSINT
- Praktyczne testy penetracyjne
- Zastosowanie technik OSINT w praktyce

9. Cyberbezpieczeństwo – kluczowe regulacje i standardy

- Różnice między **standardami**, **dyrektywami**, **rozporządzeniami** i **strategiami** w zakresie cyberbezpieczeństwa. Kluczowe regulacje wpływające na organizacje w Polsce i Europie
- zgłaszanie incydentów, testowanie systemów, zarządzanie ryzykiem IT. Wskazanie, które przepisy mają charakter **dobrowolny (np. ISO**), a które są **obowiązkowe (np. NIS2, DORA)**

10. Bezpieczeństwo w Tworzeniu Oprogramowania

- Secure coding, secure scripting, DevSecOps
- Analiza bezpieczeństwa kodu aplikacji

11. Techniki Obrony w Cyberprzestrzeni

- Zarządzanie incydentami
- Ćwiczenia praktyczne w zakresie obrony/ataku przed zaawansowanymi atakami
- Skanowanie podatności oraz raportowanie
- Implementacja SIEM oraz analiza incydentów bezpieczeństwa

Bądźmy w kontakcie!
kontakt@codeme.pl
tel: +48 724 379 836
codeme.pl