kod szkolenia: BS.IT 01 / PL DL 3d

Security/Wprowadzenie do zagadnień bezpieczeństwa IT

Zobacz film: https://youtu.be/QvD-S_XordQ

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- **CompTIA CySA+**
- **CompTIA Security+**
- **CompTIA Network+**
- **OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji**
- **CEH - Certified Ethical Hacker**
- **ECIH - Certified Incident Handler**
- **Testy penetracyjne**

Odbiorcy szkolenia

Szkolenie dla osób, które planują zajmowaać się bezpieczeństwem systemów informatycznych w firmie, a w szczególności dla osób, które będą pełniły funkcję Security Managera.

Korzyści

Szkolenie zapoznaje słuchacza z zagadnieniami polityki bezpieczeństwa IT w firmie, w oparciu o światowe standardy i metody sprawdzone w dużych korporacjach. Przedstawione zostaną najnowsze technologie zabezpieczeń, zgodne z wymogami polskiego ustawodawstwa w tym zakresie.

Program szkolenia

1. Wprowadzenie do tematyki bezpieczeństwa
   - Czym jest bezpieczeństwo IT?
   - Terminologia
2. Organizacje i normy
   - Kryteria oceny poziomu bezpieczeństwa
   - AI Act – normy dotyczące AI
   - NIS2 i DORA oraz ECF/NICE
3. Zarządzanie bezpieczeństwem
   - Inicjowanie procesów bezpieczeństwa IT
   - Tworzenie procedur bezpieczeństwa
   - Zagrożenia i zabezpieczenia rozważane przy tworzeniu polityki bezpieczeństwa
4. Kryptografia oraz środowisko PKI
   - Terminologia i organizacje standaryzujące
   - Algorytmy
   - Funkcje skrótu
5. Protokoły i mechanizmy zabezpieczające transmisję danych
   - SSH
   - PGP
   - SSL/TLS
   - Tunelowanie danych
6. Metody autentykacji użytkowników
   - LDAP
   - Kerberos
7. Sieć I TCP/IP
   - Wprowadzenie do TCP/IP
   - Metody uwierzytelniania w sieciach LAN
   - Bezpieczeństwo sieci bezprzewodowych
8. Skanowanie sieci
   - Mapowanie sieci
   - Skanowanie portów

- Wykrywanie systemu operacyjnego

9. Opis typowych i aktualnych trendów ataków
   - Typy ataków
   - Zapobieganie
   - Źródła informacji o nowych typach ataków
10. Systemy wykrywania włamań IDS/IPS
    - Host IDS
    - Network IDS
    - Firewalle
    - Typy firewalli
    - Działanie i implementacje
11. Sieci VPN
    - SSL VPN
    - IPsec VPN
12. Dobre praktyki
    - Sposoby weryfikacji spójności sysytemów
    - Sposoby składowania i ochrona logów
    - Co i jak monitorujemy?

Oczekiwane przygotowanie uczestnika

Wymagana ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.

Szkolenie obejmuje

- 3 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Czas trwania

> 3 dni / 21 godzin

Język

- Szkolenie: polski
- Materiały: polski