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

Warsztaty z Informatyki Śledczej

Warsztaty z informatyki śledczej umożliwiają zdobycie wiedzy zarówno teoretycznej, jak i praktycznej z dziedziny jaką jest infromatyka śledcza.

Dzięki warsztatom poznasz techniki z zakresu identyfikowania, gromadzenia, przejmowania i przechowywania materiału dowodowego. Uzyskasz wiedzę w jaki sposób należy prezentować cyfrowy materiał dowodowy.

Zobacz film: https://youtu.be/3ppnBmrte-8

Dodatkowo zachęcamy do zapoznania się z:

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 przeznaczone jest dla:

- biegłych sądowych,
- specjalistów do spraw cybersecurity,
- osób zajmujących się tematyką cyfrowego materiału dowodowego (dowodu elektronicznego). Wiedza techniczna nie jest wymagana, podczas szkolenia słuchacze poznają jakie informacje można pozyskać podczas analizy zabezpieczonego materiału

Korzyści

Zdobycie wiedzy teoretycznej i praktycznej z zakresu identyfikowania, gromadzenia, przejmowania i przechowywania oraz prezentowania cyfrowego materiału dowodowego (dowodu elektronicznego).

Program szkolenia

1. Definicja, znaczenie i cele informatyki śledczej
2. Umocowanie prawne, dobre praktyki, omówienie norm serii ISO/IEC 27000 oraz standardu NIST
3. Zasady pracy śledczej, cyfrowy materiał dowodowy, metodyka postępowania z materiałem, proces analizy, narzędzia informatyki śledczej
4. Metody prezentowania wyników analizy, tworzenie raportów
5. Przechowywanie cyfrowego materiału dowodowego

Część warsztatowa

1. Symulacja czynności prowadzonych podczas fizycznego zabezpieczania cyfrowego materiału dowodowego
2. Wykonywanie i zabezpieczanie kopii binarnych nośników pamięci w środowisku MS Windows, Linux, macOS
3. Zabezpieczanie cyfrowego materiału dowodowego w środowisku MS Windows, Linux, macOS
4. Analiza systemów plików, dzienników logów, pamięci RAM, odzyskanych usuniętych artefaktów dla systemów MS Windows, Linux, macOS
5. Analiza danych GPS
6. Analiza danych urządzeń elektronicznych, szpiegujących
7. Zaawansowane techniki rekonstrukcji zdarzeń dla systemów MS Windows, Linux, macOS

Oczekiwane przygotowanie uczestnika

- Podstawowa znajomość obsługi komputera

Szkolenie obejmuje

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

Metoda szkolenia

- wykład: 2 dni
- warsztaty: 1 dzień

Czas trwania

3 dni / 21 godzin

Język

- Szkolenie; polski
- Materiały: polski