# Tytuł szkolenia: Wprowadzenie do informatyki śledczej jako elementu kontroli bezpieczeństwa i audytu wewnętrznego

## Kod szkolenia: INFRA-BEZP-SLED

## Wprowadzenie

Szkolenia jest ukierunkowane na zapoznanie się z obecnymi rozwiązaniami udziału Informatyki Śledczej w systemach bezpieczeństwa organizacji. Podczas szkolenia zapoznasz się jak przygotować zespół reagowania na incydenty teleinformatyczne - CSIRT, jakie są poszczególne etapy podejmowanych działań w środowisku IT. W oparciu o jakie oprogramowanie, standardy i wytyczne przeprowadzić gromadzenia a następnie analizę dowodów elektronicznych, a także jak przygotować raport końcowy.

## Adresaci szkolenia

Szkolenie adresowane jest do osób, które są lub będą odpowiedzialne za bezpieczeństwo systemów IT w organizacji, audytorów wewnętrznych, administratorów bezpieczeństwa informacji, a także odpowiedzialnych za realizację działań w ramach planów ciągłości działania (BCM) i reagowania na sytuacje kryzysowe (DRP).

## Cel szkolenia

Celem szkolenia jest przedstawienie zakresu wiedzy na temat organizacji działań w ramach informatyki śledczej, poszczególnych etapów: od przygotowania, działań „TRIAGE" po realizację zabezpieczenia dowodów elektronicznych w środowisku teleinformatycznym. Ponadto w ramach szkolenia zaprezentowane zostaną aplikacje i metodologie prowadzenia zabezpieczenia danych elektronicznych oraz oceny ich przydatności w postępowaniu dowodowym.

## Czas i forma szkolenia

- 21 godzin (3 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

## Plan szkolenia

1. Wprowadzenie do kontroli, oceny bezpieczeństwa i informatyki śledczej
2. Aspekty prawne oraz wymagania organizacyjne
3. Metodyki organizacji działania zespołu reagowania na incydenty IT oraz rekomendacje
    a. NIST, SANS, ISO/IEC
4. Gromadzenie dowodów cyfrowych.
    a. TRIAGE w informatyce śledczej.
    b. Zabezpieczenie danych z systemu IT.
    c. Odzyskiwanie danych usuniętych.
    d. Gromadzenie i analiza danych w tym danych zaszyfrowanych.
    e. Usuwanie danych.
    f. Ukrywanie danych.
5. Dokumentowanie i oznaczanie dowodów.
6. Śledztwo komputerowe – wyposażenie techniczne i aplikacje.
7. Procedury i postępowanie na miejscu zdarzenia.
8. Raport zespołu CSIRT wraz z ustaleniami z przeprowadzonych działań