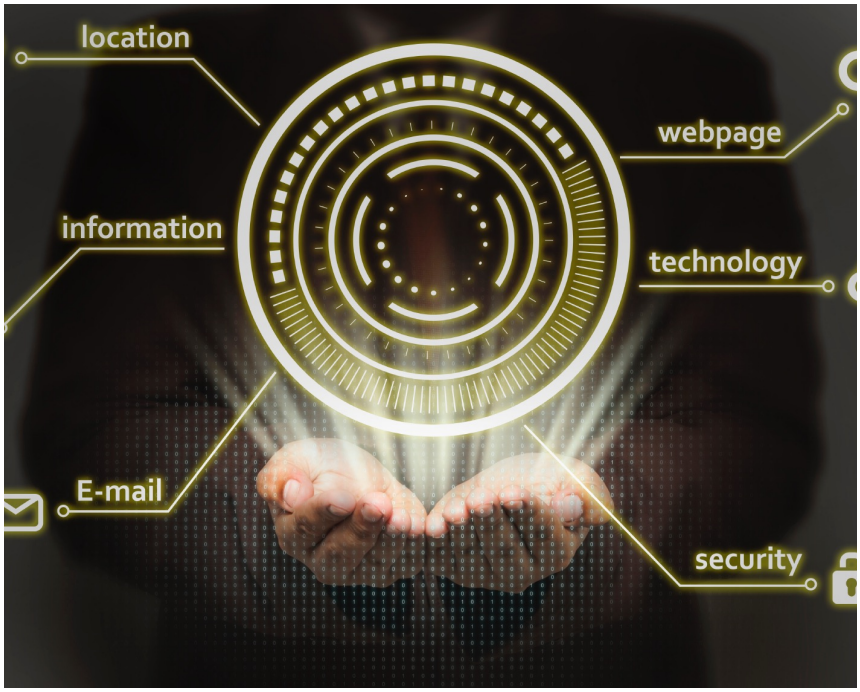
Informatyka Śledcza

Poziom Ekspercki



Agenda:

- Wykonywane kopii binarnych w środowisku lokalnym
- Wykonywane kopii binarnych w środowisku sieciowym
- Analiza i zabezpieczanie danych z Volume Shadow Copy
- Ręczna analiza tablicy MFT
- Różnice w analizie koszta systemowego w systemach operacyjnych
- Analiza zawartości pagefile.sys oraz hiberfile
- Analiza zawartości bufora wydruku
- Analiza nagłówków pliku poczty elektron.
- Ukrywanie danych w Alternatywnych strumieniach danych
- Wyszukiwanie plików w Alternatywnych strumieniach danych
- Informacje zawarte w listach szybkiego dostępu
- Znaczenie i analiza logów w systemach UNIX
- Zabezpieczanie informacji ulotnych - TRIGE
- Analiza Prefetch
- Zabezpieczanie obrazu pamięci RAM
- Analiza zawartości pamięci RAM
- Zaawansowana analiza RAM
- Analiza ZEUS-a na podstawie RAM
- Steganografia plików
- Ruch sieciowy jako źródło istotnych danych
- Lokalizacje sieciowe - wyszukiwanie i analiza
- Wyszukiwanie plików po sygnaturach czasowych
- Wyodrębnianie istotnych informacji z rejestru systemu Windows
- Automatyzacja pracy - budowa własnego narzędzia

Gdzie: **ForSec Sp. z o.o.**
ul. 73 Pułku Piechoty 7A
40-496 Katowice

Czas: **2 dni (8:30 - 15:30)**

FOR SEC
Forensics&Security