

Kod szkolenia: **SEC/IOT**

Tytuł szkolenia: **Testowanie bezpieczeństwa rozwiązań IoT**

Dni: 2

## Opis:

### Adresaci szkolenia:

Szkolenie jest adresowane do programistów i testerów zainteresowanych zapewnieniem bezpieczeństwa rozwiązań IoT

### Cel szkolenia:

Przedstawienie praktycznych zagadnień związanych z testowaniem bezpieczeństwa rozwiązań IoT

### Mocne strony szkolenia:

Mocną stroną szkolenia jest przedstawienie praktycznych zagadnień związanych z testowaniem

### Wymagania:

Biegłe posługiwanie się komputerem, znajomość podstaw pracy w systemie Windows i Linux

### Parametry szkolenia

2\*8 godzin (2\*7 godzin netto) wykładów i warsztatów (z wyraźną przewagą warsztatów).

### Program szkolenia:

- Typy urządzeń IoT (Consumer, M2M)
- SDR (Software Defined Radio)
  - sniffowanie i dekodowanie komunikacji z użyciem urządzeń typu SDR
- Protokoły komunikacji i ich bezpieczeństwo
  - typowe ataki na protokoły komunikacji: sniffing (podsluchiwanie), relay (przekazywanie), replay (odtworzenie)
  - NFC, RFID
  - Bluetooth Low Energy
  - WiFi, Zigbee
- Elektronika



- JTAG, interfejsy testowe
- ekstrakcja pamięci firmware
- Analiza firmware
  - typowe błędy w firmware
  - dekompilacja i dezasemblacja firmware
- Analiza zabezpieczeń kryptograficznych
  - side-channel
- Backend IoT
  - testowanie API, typowe błędy w API

Warsztaty z użyciem Ubertooth, Adafruit BLE Sniffer, HackRF, Hydra NFC, SDR

