Możliwość dofinansowania

Szkolenie z Cyberbezpieczeństwa: Mobile Forensics (analiza śledcza urządzeń mobilnych)

Numer usługi 2026/02/24/148153/3357903

15 362,70 PLN brutto
12 490,00 PLN netto
960,17 PLN brutto/h
780,63 PLN netto/h
261,33 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5

30 ocen

Gdynia
Usługa szkoleniowa
stacjonarna
16:00 h
16.07.2026 do 17.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do osób, których praca ociera się o informatykę śledczą, a więc: • informatyków śledczych pragnących wykonywać analizę urządzeń mobilnych • analityków kryminalistycznych • pracowników SOC-ów i firmowych zespołów reagowania na incydenty • audytorów IT chcących pogłębić swoją wiedzę o możliwości analizy smartofonów • serwisantów GSM potrzebujących odzyskiwać dane z uszkodzonych fizycznie mobilnych urządzeń …ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie “mobile forensics” — dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	6
Data zakończenia rekrutacji	08-07-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Mobile Forensics (analiza śledcza urządzeń mobilnych). Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Podniesiesz poziom bezpieczeństwa w swojej firmie oraz rozwiążesz najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.	Laboratoria przygotowane na symulowanym środowisku kształcenia.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/mobile-forensics-analiza-sledcza-urzadzen-mobilnych/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

I. Omówienie podstaw telefonii komórkowej

– urządzenia mobilne w kontekście dowodu elektronicznego

– procedury zabezpieczania urządzeń mobilnych

– wstęp do GSM

– karty sim ich zastosowanie, identyfikacja i analiza danych

– stacje bazowe BTS

– komponenty urządzeń mobilnych

– procedury badawcze zabezpieczonych urządzeń mobilnych

– biały wywiad

II. Analiza śledcza urządzeń pracujących na systemie Android

– struktura zapisu danych w systemie Android

– ekstrakcja logiczna

– ekstrakcja systemu plików

– ekstrakcja fizyczna

– urządzenia i oprogramowanie do zabezpieczania i analizy danych

– rootowanie telefonów z Androidem

– łamanie zabezpieczeń w systemach Android

– odzyskiwanie danych

– ślady aktywności użytkownika

– kontakty, smsy, rejestr połączeń i inne

– szyfrowanie w systemach Android

III. Analiza śledcza urządzeń pracujących na systemie iOS

– struktura zapisu danych w systemie iOS

– wersje iOS, a możliwości śledcze

– zabezpieczanie urządzeń pracujących w systemie iOS

– odzyskiwanie danych

– łamanie zabezpieczeń w systemach iOS

– śledzenie aktywności użytkownika

– kontakty, smsy, rejestr połączeń i inne

– pliki backupu iTunes

IV. Analiza śledcza urządzeń pracujących na systemie Windows Phone oraz BlackBerry, telefony z przeszłości

– wersje Windows Phone, a możliwości śledcze

– tryb DFU w Windows Phone

– rozwiązania stosowane w telefonach BlackBerry

– zastosowanie boxów w telefonach z przeszłości

V. Odzyskiwanie danych metodą JTAG i ISP

– wymagany sprzęt do JTAG i ISP,

– rozpoznanie modelu płyty głównej i wyszukiwanie pinoutów

– lutowanie pinoutów

– ISP w urządzeniach z zablokowaną możliwością połączenia JTAG

– odczyt zawartości kości pamięci za pomocą boxów serwisowych i porównanie

uzyskanych wyników, w tym prędkości odczytu

VI. Odzyskiwanie danych metodą CHIP-OFF

– diagnozowanie możliwości zastosowania technik chip-off

– rozpoznawanie uszkodzeń urządzeń mobilnych

– opis przebiegu procesu chip-off

– demontaż smartfonów

– identyfikowanie specyfikacji technicznych kości pamięci

– czytniki pamięci, a rozmiary kości

– przygotowanie i wylutowanie kości pamięci

– oczyszczanie kości pamięci

– odczyt danych z wylutowanej kości

– parsowanie zrzutów pamięci za pomocą MOBILedit, Paraben E3 i Autopsy

– wykorzystanie chip-off do wyszukiwania pinout ISP

– podstawa obsługi miernika elektronicznego

VII. Przyszłość analizy urządzeń mobilnych

– szyfrowanie w najnowszych telefonach

– kody blokady, a możliwości analizy

– wpływ factory reset na możliwości odzysku danych

– analiza kryminalna

Harmonogram

Liczba pozycji harmonogramu: 7

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 7 Omówienie podstaw telefonii komórkowej	Witold Sobolewski	16-07-2026	10:00	12:00	02:00
2 z 7 Analiza śledcza urządzeń pracujących na systemie Android	Witold Sobolewski	16-07-2026	12:00	14:00	02:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 7 Analiza śledcza urządzeń pracujących na systemie iOS	Witold Sobolewski	16-07-2026	14:00	16:00	02:00
4 z 7 Analiza śledcza urządzeń pracujących na systemie Windows Phone oraz BlackBerry, telefony z przeszłości	Witold Sobolewski	16-07-2026	16:00	18:00	02:00
5 z 7 Odzyskiwanie danych metodą JTAG i ISP	Witold Sobolewski	17-07-2026	10:00	13:00	03:00
6 z 7 Odzyskiwanie danych metodą CHIP-OFF	Witold Sobolewski	17-07-2026	13:00	16:00	03:00
7 z 7 Przyszłość analizy urządzeń mobilnych	Witold Sobolewski	17-07-2026	16:00	18:00	02:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	15 362,70 PLN
Koszt przypadający na 1 uczestnika netto	12 490,00 PLN
Koszt osobogodziny brutto	960,17 PLN
Koszt osobogodziny netto	780,63 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Witold Sobolewski

Doktor z zakresu informatyki śledczej. Właściciel VS DATA. Łączy funkcje techniczne, managerskie i wykładowe. Posiada ponad 18 letnie praktyczne doświadczenie w wykonywaniu ekspertyz na rzecz organów ścigania, firm prywatnych i instytucji w zakresie odzyskiwania danych, informatyki śledczej oraz analizy powłamaniowej. Wydał ponad 6000 ekspertyz. Biegły sądowy przy Sądzie Okręgowym w Gdańsku z zakresu informatyki śledczej (trzecia kadencja). Posiada międzynarodowe certyfikaty z informatyki śledczej (CFCE, ACE, CCFE), odzyskiwania danych (CDRP) i analizy urządzeń mobilnych (CMFF). Twórca, opiekun merytoryczny i wykładowca na dwóch kierunkach studiów podyplomowych „Cyberbezpieczeństwo oraz Informatyka śledcza" oraz „Zarządzanie cyberbezpieczeństwem" w Centrum Kształcenia Podyplomowego Uczelni Łazarskiego w Warszawie i „Cyberbezpieczeństwo" na Akademii Marynarki Wojennej w Gdyni. Trener firmy niebezpiecznik.pl, w której prowadzi szkolenia „Informatyka śledcza" oraz „Analiza urządzeń mobilnych". Na Krajowej Szkole Sądownictwa i Prokuratury szkoli sędziów i prokuratorów, gdzie w sposób nietechniczny mówi o technicznych aspektach zwalczania i zapobiegania cyberprzestępczości. Częsty gość branżowych prelekcji, konferencji i sympozjów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (zapis prezentacji).

Warunki uczestnictwa

Każdy uczestnik naszych szkoleń **musi** podpisać deklarację, że poznane ataki i narzędzia będzie wykorzystywał wyłącznie w celach zgodnych z prawem.

Szkolenie odbywa się w formule BYOL (Bring Your Own Laptop). Wymagania: 2GB RAM, 5GB HDD oraz zainstalowany darmowy i dostępny na każdy system operacyjny program VirtualBox — trener przed startem szkolenia udostępni obraz maszyny wirtualnej na której będą odbywały się laboratoria.

Informacje dodatkowe

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/mobile-forensics-analiza-sledcza-urzadzen-mobilnych/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Adres

pl. Górnośląski 21
81-509 Gdynia
woj. pomorskie

Szczegóły miejsca realizacji usługi wysyłane są do Uczestników szkolenia na tydzień przed danym terminem.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja

- Wi-fi
- Laboratorium komputerowe
- Lunch oraz przerwy kawowe w trakcie szkoleń stacjonarnych.

Kontakt

Magda Kowalska

E-mail szkolenia@niebezpiecznik.pl

Telefon (+48) 124 420 244