Możliwość dofinansowania

Cyberbezpieczeństwo: Szkolenie z Informatyki Śledczej (computer forensics)

Numer usługi 2026/02/04/148153/3307026

7 734,24 PLN brutto
6 288,00 PLN netto
552,45 PLN brutto/h
449,14 PLN netto/h
261,33 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5

30 ocen

Kraków
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
14:00 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: • biegłych sądowych, • administratorów sieci LAN w których dochodzi do incydentów, • pracowników firmowych zespołów reagowania na incydenty, • policjantów i pracowników służb mundurowych, • audytorów i pentesterów, ...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie “IT forensics” — dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	08-07-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	14
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 Informatyki Śledczej (computer forensics). 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
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.	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/szkolenia/szkolenie-z-informatyki-sledczej-computer-forensics/?zai

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

ŚWIADOMOŚĆ INFORMATYKI ŚLEDCZEJ

-informatyka śledcza, a cyberprzestępczość

-informatyka śledcza na potrzeby osób prywatnych, biznesu, organów ścigania, wojska, rządu

-cyfrowy dowód informacji: źródła, rodzaje, cechy, podatność, integralność

-aspekty prawne informatyki śledczej

-procesy w informatyce śledczej

-najlepsze praktyki informatyki śledczej

-narzędzia do informatyki śledczej i ich możliwości

-zawód – informatyk śledczy

-zarządzanie pracą informatyka śledczego

-dziedziny pokrewne informatyki śledczej

PROCES PRZYGOTOWANIA

-biały wywiad w informatyce śledczej

-opracowanie procedury zabezpieczenia

-budowanie zaplecza narzędziowego-programowego

IDENTYFIKACJA DOWODÓW

-zasady dokumentowania

-opis miejsca zdarzenia

-opis dowodów rzeczowych

-łańcuch dowodowy w informatyce śledczej

-przykłady dowodów cyfrowych

-selekcja dowodów, a zakres zlecenia

PROCES ZABEZPIECZANIA

-dokumentowanie procesu zabezpieczania danych

-proces klonowania i obrazowania nośników

-sterylność nośnika docelowego

-zabezpieczanie post-mortem

-obrazowanie do różnych formatów plików

-funkcje skrótu i ich cechy

-oprogramowanie i narzędzia do wykonywania kopii binarnych

-porównanie urządzeń blokujących zapis

-prezentacja różnych scenariuszy zabezpieczeń

-reakcja na incydenty, a zabezpieczanie danych

-zabezpieczenie LIVE

-akwizycja pamięci RAM

-zabezpieczanie danych metodą Triage

-praca z nośnikami szyfrowanymi

-różnice w zabezpieczaniu dysków HDD i SSD

-zabezpieczanie danych w chmurze

-transport i przechowywanie dowodów cyfrowych

PROCES ANALIZY

- Przygotowanie do analizy:

-ustalanie metodyki badań

-ekstrakcja i przetwarzanie, interpretacja danych

-struktura warstwowa systemu plików

-fizyczna budowa dysku HDD

-zasady działania dysków

-formatowanie i partycjonowanie dysków

-blok danych

-struktury systemów plików

-systemy plików FAT i NTFS

-dane i ich metadane

- Analiza rejestru:

-analiza rejestru w trybie online oraz offline

-zbieranie informacji o użytkowniku

-badanie konfiguracji systemu

-ewidencjonowanie działań użytkownika

-analiza podłączanych urządzeń do USB

- Odzyskiwanie danych:

-„proste” odzyskiwanie danych

-odzyskiwanie danych ze strukturą

-odzyskiwanie danych bez struktury

-odzyskiwanie danych vs. Odzyskiwanie plików

-zastosowanie wyszukiwania GREP

- Analiza artefaktów Windows:

-identyfikacja danych systemowych

-ostatnio używane pliki

-ostatnio uruchamiane aplikacje

-wiedza o plikach i folderach

- Analiza przeglądarek WWW:

-analiza przeglądarki IE/Edge, Firefox oraz Chrome

-historia, zakładki, autouzupełnianie

-ciasteczka, cache i pobrane pliki

-bazodanowa struktura plików przeglądarek

-Portable Web Browsing

-tryb prywatny w przeglądarkach

- Analiza komunikatorów internetowych:

-sprawdzanie konfiguracji komunikatorów

-ujawnianie historii komunikacji głosowej

-odzyskiwanie treści wiadomości komunikatorów

- Analiza e-mail:

-analiza wiadomości email

-webmail, a możliwości śledcze

-identyfikacja nadawców wiadomości

- Analiza logów zdarzeń:

-logowanie do systemu Windows

-podłączanie urządzeń pod USB

-manipulacja czasem systemowym

-uruchamianie złośliwego oprogramowania

- Linia czasu:

-tworzenie linii czasu

-filtrowanie i wyszukiwanie zdarzeń

-wizualizacja linii czasu

PROCES RAPORTOWANIA

-zasady raportowania

-layout raportu

-prezentacja dla zleceniodawcy

Harmonogram

Liczba pozycji harmonogramu: 6

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 ŚWIADOMOŚĆ INFORMATYKI ŚLEDCZEJ	Witold Sobolewski	16-07-2026	10:00	12:00	02:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 6 PROCES PRZYGOTOWANIA	Witold Sobolewski	16-07-2026	12:00	14:00	02:00
3 z 6 IDENTYFIKACJA DOWODÓW	Witold Sobolewski	16-07-2026	14:00	17:00	03:00
4 z 6 PROCES ZABEZPIECZANIA	Witold Sobolewski	17-07-2026	10:00	12:00	02:00
5 z 6 PROCES ANALIZY	Witold Sobolewski	17-07-2026	12:00	15:00	03:00
6 z 6 PROCES RAPORTOWANIA	Witold Sobolewski	17-07-2026	15:00	17:00	02:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 734,24 PLN
Koszt przypadający na 1 uczestnika netto	6 288,00 PLN
Koszt osobogodziny brutto	552,45 PLN
Koszt osobogodziny netto	449,14 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 (podręcznik – 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/szkolenia/szkolenie-z-informatyki-sledczej-computer-forensics/?zai

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

Adres

ul. Armii Krajowej 11
30-150 Kraków
woj. małopolskie

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

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Magda Kowalska

E-mail szkolenia@niebezpiecznik.pl
Telefon (+48) 124 420 244