Możliwość dofinansowania

Szkolenie z Cyberbezpieczeństwa: Szkolenie Cyber Ratownik: First Incident Responder

Numer usługi 2026/02/24/148153/3357872

4 907,70 PLN brutto
3 990,00 PLN netto
701,10 PLN brutto/h
570,00 PLN netto/h
261,33 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5

30 ocen

Kraków
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
07:00 h
17.07.2026 do 17.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do: • pracowników działów bezpieczeństwa; • inspektorów ochrony danych osobowych; • pracowników komórek zarządzania bezpieczeństwem (SOC) oraz zespołów reagowania na incydenty (CERT) • pracowników organów ścigania: policjantów i pracowników służb mundurowych; • pracowników wymiaru sprawiedliwości; • ekspertów działów IT, audytorów i pentesterów ...ale tak naprawdę, to z przyjemnością powitamy każdego, kto chce rozwijać się w obszarze reagowania na incydenty. Wymagamy jedynie podstawowej świadomości branży bezpieczeństwa, cała potrzebna wiedza w temacie zostanie przekazana podczas szkolenia. Jeśli dopiero zaczynasz swoją przygodę z cyberbezpieczeństwem, to szkolenie będzie dla Ciebie idealne.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	09-07-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	7

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 “incident response“. Po zakończonym szkoleniu uczestnik wie jakie czynności wykonać w pierwszej kolejności, a jakich pod żadnym pozorem nie przeprowadzać. Podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże 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 wie jakie czynności wykonać w pierwszej kolejności, a jakich pod żadnym pozorem nie przeprowadzać. Podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże 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/cyberratownik-first-incident-responder/?zai

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

Agenda szkolenia:

- **Ataki na organizacje:**– cele ataku
  - – etapy klasycznego ataku
  - – działania post exploitacyjne atakujących
  - – techniki, taktyki procedury
  - – reakcja na incydent
  - **Analiza powłamaniowa:**– cele analizy
  - – metodyka
  - – sprzęt i oprogramowanie
  - – dokumentowanie procesów
  - – zakres incydentu
  - – RFC 3227
  - – czego szuka DFIR?
  - – raportowanie
  - **Zabezpieczanie danych:**-dane ulotne
  - -pamięć RAM
  - -kopia binarna vs klon dysku
  - -szyfrowanie danych
  - -kopia logiczna
  - -metodyka TRIAGE
  - -dane z sieci
  - -logi zdarzeń
  - -serwery i macierze RAID
  - -maszyny wirtualne (Hyper-V, VMware)
- Ciekawe przypadki zabezpieczeń i analiz powłamaniowych – case studies.

Harmonogram

Liczba pozycji harmonogramu: 4

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Ataki na organizacje	Witold Sobolewski	17-07-2026	10:00	12:00	02:00
2 z 4 Analiza powłamaniowa	Witold Sobolewski	17-07-2026	12:00	14:00	02:00
3 z 4 Zabezpieczanie danych	Witold Sobolewski	17-07-2026	14:00	16:00	02:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 4 Ciekawe przypadki zabezpieczeń i analiz powłamaniowych – case studies	Witold Sobolewski	17-07-2026	16:00	17:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 907,70 PLN
Koszt przypadający na 1 uczestnika netto	3 990,00 PLN
Koszt osobogodziny brutto	701,10 PLN
Koszt osobogodziny netto	570,00 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: uprawnienia administratorskie, 4GB RAM, 20GB HDD oraz zainstalowany darmowy i dostępny na każdy system operacyjny program VirtualBox.

Informacje dodatkowe

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

https://niebezpiecznik.pl/szkolenia/cyberratownik-first-incident-responder/?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