Możliwość dofinansowania

DFIR-201 Informatyka śledcza i reagowanie na incydenty (Digital Forensics & Incident Response) - szkolenie

Numer usługi 2026/07/30/18395/3719041

3 900,00 PLN brutto
3 900,00 PLN netto
177,27 PLN brutto/h
177,27 PLN netto/h
261,33 PLN cena rynkowa

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

4,6 / 5

45 ocen

Kraków
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
22:00 h
13.10.2026 do 15.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Członkowie zespołów reagowania na incydenty, analitycy SOC wyższego szczebla, administratorzy systemów i sieci pełniący rolę First Responders, a także specjaliści ds. bezpieczeństwa i audytorzy zaangażowani w wyjaśnianie naruszeń danych w organizacjach komercyjnych.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	08-10-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	kształcenie w innych formachkształcenia prowadzonych przez uczelnie

Cel

Cel edukacyjny

Usługa prowadzi do uzyskania zaawansowanych kompetencji praktycznych w zakresie integrowania procedur reagowania na incydenty (Incident Response) z technikami cyfrowej informatyki śledczej (Digital Forensics), w tym

prawidłowego zabezpieczania dowodów elektronicznych oraz prowadzenia analizy przyczyn źródłowych na potrzeby mitygacji zagrożeń i postępowań prawno-regulacyjnych (RODO/NIS2).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Planuje działania w ramach cyklu reagowania na incydent (IR) i zabezpiecza materiał dowodowy zgodnie z zasadą Chain of Custody	omawia fazy cyklu reagowania na incydent (PICERL wg NIST/SANS) i zasady organizacji pracy kryzysowej, rozróżnia działania dozwolone i zabronione dla First Respondera (np. niszczenie dowodów), uzasadnia wymogi zachowania łańcucha dowodowego dla postępowań sądowych i ubezpieczycieli, wykonuje zrzut pamięci RAM i binarną kopię dysku zgodnie z zasadą Order of Volatility	Test teoretyczny
Analizuje artefakty systemu Windows w celu rekonstrukcji aktywności użytkownika i śladów uruchomienia złośliwego oprogramowania	identyfikuje ślady wykonania programów w, ekstrahuje i analizuje logi w poszukiwaniu ruchu bocznego (lateral movement), rekonstruuje aktywność użytkownika na podstawie rejestru Windows i historii podłączanych urządzeń USB	Test teoretyczny
Przeprowadza podstawową analizę pamięci RAM i triage złośliwego oprogramowania	identyfikuje ukryte procesy i wstrzyknięty kod (process injection) w zrzucie pamięci, rozróżnia analizę statyczną od dynamicznej malware, ekstrahuje z pamięci wskaźniki kompromitacji takie jak domeny i adresy IP	Test teoretyczny
Prowadzi podstawowe śledztwo sieciowe w celu identyfikacji skompromitowanych hostów	analizuje zrzuty ruchu sieciowego (PCAP) w poszukiwaniu oznak incydentu, identyfikuje skompromitowane hosty na podstawie analizy przepływów sieciowych, dobiera strategię izolacji hosta tak aby nie utrudniać działania firmy	Test teoretyczny
Koordynuje działania containment/eradication/recovery oraz opracowuje raport DFIR z analizą przyczyn źródłowych	dobiera działania izolacji atakującego przy zachowaniu ciągłości działania firmy, opisuje proces bezpiecznej odbudowy infrastruktury i resetowania poświadczeń, przeprowadza root cause analysis i opracowuje raport DFIR wraz z rekomendacjami dla zarządu	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Metodyka reagowania na incydenty: ramy NIST i SANS, triage incydentu, organizacja pracy kryzysowej.
2. Rola First Respondera i aspekty prawne: zasada Chain of Custody, błędy niszczące materiał dowodowy, wymogi dla postępowań i ubezpieczycieli.
3. Zabezpieczanie dowodów cyfrowych: order of volatility, wykonywanie zrzutów pamięci RAM i kopii binarnych dysków.
4. Informatyka śledcza systemów Windows: artefakty NTFS, Prefetch, Amcache, Shimcache, analiza logów EVTX i rejestru Windows.
5. Analiza pamięci RAM i malware triage: Volatility, identyfikacja ukrytych procesów, process injection, ekstrakcja IoC.
6. Śledztwa sieciowe i odbudowa: analiza PCAP i NetFlow, containment, eradication, recovery.
7. Raportowanie i lessons learned: root cause analysis, raport DFIR oraz rekomendacje naprawcze i inwestycyjne.

Zajęcia odbywają się w jednej grupie szkoleniowej. Na jednego uczestnika przypada jedno stanowisko komputerowe wraz z niezbędnym sprzętem i oprogramowaniem.

Walidacja będzie realizowana na ostatnich zajęciach w postaci testu teoretycznego.

Zgodnie z proporcją 30/70% przyjętą w programie szkolenia zajęcia obejmują ok. 7 godzin dydaktycznych (ok. 5,25 godziny zegarowej) części teoretycznej (wykład metodyczny) oraz ok. 17 godzin dydaktycznych (ok. 12,75 godziny zegarowej) części praktycznej (intensywne warsztaty śledcze i symulacje incydentów).

Szkolenie realizowane jest stacjonarnie w dniach 13–15.10.2026, z jedną godzinną przerwą każdego dnia oraz 30-minutowym testem teoretycznym kończącym szkolenie w dniu 15.10.2026.

Harmonogram

Liczba pozycji harmonogramu: 17

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 17 Moduł 1: Cykl Reagowania na Incydenty – ramy NIST i SANS (PICERL), triage incydentu, organizacja pracy War Roomu. Wykład metodyczny.	Zajęcia	Piotr Waryszak	13-10-2026	08:00	09:30	01:30
2 z 17 Moduł 2: Rola First Respondera i Prawo – czego nie robić po wykryciu włamania, zasada Chain of Custody, wymogi dla sądów i ubezpieczycieli. Wykład metodyczny, dyskusja moderowana.	Zajęcia	Piotr Waryszak	13-10-2026	09:30	11:00	01:30
3 z 17 -	Przerwa	-	13-10-2026	11:00	12:00	01:00
4 z 17 Moduł 3: Zabezpieczanie Ulotnych Dowodów – Order of Volatility, zrzuty pamięci RAM, kopie binarne dysku (FTK Imager, dd). Warsztat lab.	Zajęcia	Piotr Waryszak	13-10-2026	12:00	13:30	01:30
5 z 17 -	Przerwa	-	13-10-2026	13:30	13:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 17 Moduł 4: Artefakty Systemu Windows – NTFS/MFT, Prefetch, Amcache, Shimcache, analiza logów EVTX (lateral movement). Wykład, warsztat lab.	Zajęcia	Piotr Waryszak	13-10-2026	13:45	16:00	02:15
7 z 17 Moduł.5. Rejestr Windows jako Kopalnia Wiedzy– klucze autostartu,urządzenia USB,historia przeglądania, rekonstrukcja aktywności użytkownika na podst. NTUSER.DAT. Wykład, warsztat lab.	Zajęcia	Piotr Waryszak	14-10-2026	08:00	10:15	02:15
8 z 17 -	Przerwa	-	14-10-2026	10:15	11:15	01:00
9 z 17 Moduł 6: Memory Forensics (Pamięć RAM) – wprowadzenie do Volatility, ukryte procesy, malware bezplikowy, process injection. Wykład, warsztat lab.	Zajęcia	Piotr Waryszak	14-10-2026	11:15	13:30	02:15
10 z 17 -	Przerwa	-	14-10-2026	13:30	13:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 17 Moduł 7: Triage Złośliwego Oprogramowania – analiza statyczna i dynamiczna, praca w bezpiecznym środowisku (sandbox), ekstrakcja IoC ze zrzutu pamięci. Wykład, warsztat lab.	Zajęcia	Piotr Waryszak	14-10-2026	13:45	16:00	02:15
12 z 17 Moduł 8: Network Forensics (Ślady w Sieci) – analiza zrzutów ruchu (PCAP), tunelowanie DNS, eksfiltracja bazy danych. Wykład, warsztat lab.	Zajęcia	Piotr Waryszak	15-10-2026	08:00	09:30	01:30
13 z 17 -	Przerwa	-	15-10-2026	09:30	09:45	00:15
14 z 17 Moduł 9: Containment, Eradication & Recovery – izolacja vs. ciągłość działania, bezpieczna odbudowa infrastruktury i resetowanie poświadczeń. Wykład metodyczny, dyskusja moderowana.	Zajęcia	Piotr Waryszak	15-10-2026	09:45	11:15	01:30
15 z 17 -	Przerwa	-	15-10-2026	11:15	12:15	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 17 Moduł 10: Raportowanie i Lessons Learned – Root Cause Analysis, struktura raportu DFIR. Warsztat opracowania raportu zamykającego o przypadek laboratoryjny.	Zajęcia	Piotr Waryszak	15-10-2026	12:15	13:15	01:00
17 z 17 -	Walidacja	-	15-10-2026	13:15	14:00	00:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	22:00
w tym suma godzin zajęć	17:30
w tym suma godzin walidacji	00:45
w tym suma przerw	03:45
Suma godzin dydaktycznych bez przerw	24:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 900,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	3 900,00 PLN
Koszt osobogodziny brutto	177,27 PLN

Koszt osobogodziny netto	177,27 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	22:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Waryszak

Biegły sądowy z zakresu informatyki wpisany na listę Prezesa Sądu Okręgowego w Lublinie, ekspert informatyki śledczej i cyberbezpieczeństwa z blisko dziesięcioletnim doświadczeniem praktycznym. Autor ponad czterystu ekspertyz sądowych sporządzonych na potrzeby postępowań karnych i cywilnych. Doktorant na kierunku Informatyka, specjalizujący się w analizie dowodów cyfrowych, bezpieczeństwie systemów teleinformatycznych oraz badaniu incydentów cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały bezpośrednio związane z realizowaną usługą oraz dokument potwierdzający udział/ukończenie szkolenia po zdaniu testu teoretycznego.

Adres

Kraków 23/D-8
30-055 Kraków
woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Agata Rzepka

E-mail szkolenia@informatyka.agh.edu.pl
Telefon (+48) 12 3283 414