Możliwość dofinansowania

Cybersecurity & AI - Future Collars

Numer usługi 2026/04/16/44546/3491339

11 500,00 PLN brutto
11 500,00 PLN netto
176,92 PLN brutto/h
176,92 PLN netto/h
332,00 PLN cena rynkowa

iCode Trust Sp. z o.o.

4,5 / 5

65 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
65:00 h
27.07.2026 do 17.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	Kurs Cybersecurity jest sierowany do osób, które pasjonują się światem technologii i chcą nauczyć się, jak rozpoznawać cyberataki, skutecznie im zapobiegać i odpowiednio reagować, gdy wystąpią w organizacji. Bootcamp online Cybersecurity to kurs dla osób początkujących, które chcą się dowiedzieć, jak skutecznie ochronić firmę przed rosnącym zagrożeniem ze strony cyberprzestępców Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój Usługa rozwojowa adresowana również dla Uczestników projektu Zachodniopomorskie Bony Szkoleniowe
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	26-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	65
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest przygotwanie Kuranta do samodzielnej pracy na stanowisku Cybersecurity

1.Kursant będzie wiedzieć, jak oszacować wagę bezpieczeństwa informatycznego w Twojej organizacji.
2. Kursant dowie się jakie elementy środowiska informatycznego są kluczowe w utrzymaniu bezpieczeństwa na właściwym poziomie.
3.Kursant będzie wiedzieć, jak pisać polityki bezpieczeństwa.
4. Kursant dowie się, jak reagować na incydenty informatyczne i jak zapobiegać atakom.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Kursant potrafi rozróżnić podstawowe pojęcia związane z bezpieczeństwem IT.	Wymienia i charakteryzuje triadę CIA (poufność, integralność, dostępność). Opisuje standardy bezpieczeństwa (ISO/IEC 27001, CIS controls). Wyjaśnia rolę systemów operacyjnych w zapewnianiu bezpieczeństwa.	Test teoretyczny
Kursant analizuje i identyfikuje ataki phishingowe.	Rozpoznaje różne typy e-maili phishingowych. Analizuje artefakty wiadomości e-mail (nagłówki, adresy URL). Tworzy raport z analizy incydentu phishingowego.	Obserwacja w warunkach symulowanych
Kursant wdraża procedury reagowania na incydenty.	Omawia fazy reagowania na incydenty (przygotowanie, detekcja, reakcja, odzyskiwanie). Korzysta z narzędzi do monitoringu (Wireshark, Splunk). Opracowuje plan ograniczenia i eliminacji skutków incydentu.	Obserwacja w warunkach symulowanych
Kursant tworzy i wdraża polityki bezpieczeństwa.	kreśla kluczowe elementy polityki bezpieczeństwa IT. Tworzy dokumentację polityki zgodnie ze standardami. Dostosowuje polityki do wymagań organizacji.	Obserwacja w warunkach symulowanych
Kursant przeprowadza analizę powłamaniową.	Wyjaśnia podstawy analizy forensycznej. Korzysta z narzędzi forensycznych (Autopsy, Splunk). Identyfikuje i dokumentuje ślady włamania.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Kursant wykorzystuje analizę Threat Intelligence w ocenie zagrożeń.	harakteryzuje pojęcia Tactical, Strategic i Operational Threat Intelligence. Analizuje dane OSINT (Shodan, YARA). Tworzy raporty oceny ryzyka na podstawie danych o zagrożeniach.	Obserwacja w warunkach symulowanych

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

Program kursu Cybersecurity

1. Podstawy cyberbezpieczeństwa

Kursanci nauczyą się zasad zarządzania (Managment Principles), poznają umiejętności miękkie potrzebne w pracy. Kursanci nauczą się podstaw sieci i podstaw systemów operacyjnych. Zostanie także wyjaśnione Security Controls.

2. Threat Intelligence

Kursanci zaznajomią się z pojęciami Threat, Tactical Strategic i Operational Intelligence. Uczestnicy kursu poznają kim są Threat Actors I grupy APT.

W ramach zajęć zostanie przedstawiony wstęp do OSINT.

3. Analiza phishingu

Kursanci zostaną wprowadzeni w tematykę analizy phishingu, zapoznają się z typami e-maili phishingowych, badaniem e-maili, analizą artefaktów i pisaniem raportów z przeprowadzonych prac.

4. Analiza powłamaniowa

Uczestnicy zostaną wprowadzeni w tematykę analizy powłamaniowej, poznają Forensics Fundamentals, zostaną zaznajomieni z pojęciem dowodów cyfrowych, Windows i Linux Forensics.

5. Monitoring i SIEM

Kursanci zostaną wprowadzeni w tematykę monitoringu oraz systemów SIEM i różnicy między nimi. Uczestnicy kursu poznają logi i ich potęgę w cyberbezpieczeństwie, nauczą się także ich agregacji i korelacji. Zostanie przeprowadzony przegląd dostępnych na rynku narzędzi.

6. Zarządzanie incydentem

Podczas tego modułu zostanie przedstawiony kursantom wstęp do Incident Response, omówiona zostanie faza przygotowawcza, analiza i detekcja. Kursanci zostaną zapoznani z pojęciami Containment, Eradication i Recovery.

7. Rozwój

Kursanci dowiedzą się, jakie certyfikacje wybrać, jakich platform używać oraz w którą ścieżką podążać. Porozmawiamy szczegółowo i rolach w obszarze bezpieczeństwa i podstawowych wymaganiach, by zmienić swoją profesjonalną ścieżkę zawodową.

8. Warsztat online

Kursanci wezmą udział w praktycznych zajęciach symulujące incydent bezpieczeństwa w przedsiębiorstwie. Nauczą się, jak odpowiednio reagować, komunikować i mitygować z wykorzystaniem posiadanej wiedzy.

9. Warsztat AI

Kursanci poznają i oswoją się z tematyka sztucznej inteligencji w cyberbezpieczeństwie.

Kursanci dowiedzą się na co zwracać uwagę w wykorzystaniu sztucznej inteligencji patrząc przez pryzmat cyberbezpieczeństwa.

Czas trwania : 12 tygodni

Czas dostępu do platformy: 3 miesięcy od zakończenia kursu

Kluczową przewagą szkolenia jest nauka zdalna, elastyczna, dostosowana do zajęć podopiecznych, bez względu na miejscezamieszkania czy harmonogram dnia. Fakt, że nauka odbywa się w sposób zdalny, a osoby biorące udział w szkoleniu nie muszązwychodzić z domu, daje szansę osobą, które pomimo swoich wysokich możliwości nie mogą podjąć zatrudnienia bądź są wykluczone zprzyczyn niezależnych od nich.

Użytkownik indywidualny dostaje dostęp do autorskiej platformy Future Collars, na której znajdzie kurs składający się z materiałówstworzonych przez mentorów prowadzących. Platforma jest czynna 24/7 więc kursant może z niej korzystać w dowolnym momencie. Materiały dostępne są w formie prezentacji, materiałów poglądowych, wideotutorialów oraz fi lmów z lekcji na żywo.

W trakcie kursu każdemu z użytkowników przysługuje:

2x w tyg lekcje z mentorem po 1.5h na zoomie (grupowa)

1h tygodniowo indywidualnego wsparcia mentora, które można wykorzystać na czacie (RocketChat) lub również na zoomie (lekcjana żywo)

Wsparcie mentora na czacie oraz kontakt z innymi uczestnikami grupy na slacku

Szkoła przez cały czas monitoruje prace kursanta na platformie.

Sprawdzamy:

obecność na zajęciach

zaangażowanie poprzez oddawanie prac domowych

czy kursant zalicza projekty końcowe

godziny i terminy konsultacji z mentorem

Kurs obejmuje 65h lekcyjnych (45 min) = w przeliczeniu 49h zegarowe (60 min)

Kurs obejmuje 36 godz. zegarowych na żywo w czasie rzeczywistym - spotkania z Mentorem

Kurs obejmuje dodatkowo 12 godz. zegarowych indywidualnych konsultacji z Mentorem 1:1 (1 godz. na każdy tydzień kursu spotkania na żywo w czasie rzeczywistym)

Walidacja - 1 godz. zegarowa wliczone do godziny kursu

Wszystkie lekcje są nagrywne i można z nich korzystać i wielkokrotnie odtwarzać

Kurs uczy praktycznych umiejętności, zakłada wykonywanie zadań i projektów oraz przyswajanie teoretycznej wiedzy umieszczonejna platformie.

Harmonogram

Liczba pozycji harmonogramu: 2

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 lekcja organizacyjna (wykład)	Daniel Ziółkowski	27-07-2026	18:00	19:30	01:30
2 z 2 szczegółowy harmonogram kursu będzie dodany w tygodniu poprzedzającym rozpoczęcie kursu	Daniel Ziółkowski	29-07-2026	18:00	19:30	01:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	11 500,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	11 500,00 PLN
Koszt osobogodziny brutto	176,92 PLN
Koszt osobogodziny netto	176,92 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Ziółkowski

Mentor przeprowadzjący walidację kursu Cybersecurity.
Wieloletnik prakty w dziedzinie Cyberbezpieczeństwa:
1.Stryker
Cybersecurity Manager
kwi 2024 –obecnie
2.Securitas Polska
Global CERT Security Engineer
sty 2022 – paź 2022
3.Sage
Senior Security Specialist
lut 2020 – gru 2020 · 11 mies.
posiada certyfikat
GIAC Certified Incident Handler (GCIH)
Wydany lis 2019 · Wygasa lis 2027
wykształcenie:
Wyższa Szkoła Technologii Informatycznych w Warszawie
IT Network Engineer
2013 – 2017

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały opracowane są przez mentorów z wieloletnim doświadczeniem na rynku pracy w branży IT. Kursant otrzymuje dostęp doplatformy edukacyjnej, na której zamieszczone są wszystkie niezbędne materiały i może uczyć się w dowolnym momencie. Materiały sądostępne na platformie Future Collars w formie:

prezentacji, materiałów poglądowych, wideotutorialów, slajdów, plików pdf, filmów z lekcji na żywo.

Użytkownik otrzymuje dostęp do platformy, na której odbywać się będą lekcje online w czasie rzeczywistym. Platforma jest dostępna24/7, więc kursant może z niej korzystać w dowolnym momencie.

Kursant ma dostęp do tych materiałów i lekcji, które są zapisywane na platformie po lekcji online i może z nich korzystać jeszcze przez 3 miesięcy po zakończeniu kursu.

Usługa rozwojowa adresowana również dla Uczestników projektu Zachodniopomorskie Bony Szkoleniowe

Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój

Informacje dodatkowe

Jako firma szkoleniowa jesteśmy kreatorem innowacyjnej edukacji. Zapewniamy rozwój i bezpieczną przyszłość każdemu człowiekowi wświecie nowych technologii. Dzięki autorskim rozwią zaniom dopasowujemy sposób nauczania przez Internet do indywidualnych potrzeb,a nasi Mentorzy i Mentorki są niezawodnym wsparciem w zdobywaniu umieję tnoś ci poż ą danych na współczesnym rynku pracy.

Kursant otrzymuje dostęp do platformy, na której są zamieszczone wszystkie niezbędne materiały dzięki czemu może uczyć się wdowolnym dla siebie momencie. Kluczową przewagą szkolenia jest nauka zdalna, elastyczna, dopasowana do zajęć podopiecznych, bezwzględu na miejsce zamieszkania.

Mentorzy, bazując na wieloletnim doświadczeniu w branży, wprowadzają w świat pracy w IT oraz zapewniają kursantom wsparciepodczas lekcji na żywo, prowadzonych dwa razy w tygodniu, w formie: videochatu live i codziennych konsultacji na chacie pisanym.

Warunki techniczne

własny komputer z dostępem do internetu i aktulną przeglądarką internetową

Dwurdzeniowy procesor 2 GHz lub więcej (i3/i5/i7 lub odpowiednik AMD)

4GB pamięci RAM DDR3

Dysk HDD 250GB +

Łącze o mocy przynajmniej 4Mbps pobierania i 0.5Mbps wysyłania

System operacyjny Windows 8.1 lub nowszy, macOS Yosemite, aktualny Linux

Kontakt

Edyta Warda

E-mail hello@futurecollars.com
Telefon (+48) 691 950 343