Możliwość dofinansowania

Cyberbezpieczeństwo 2026 - Strategia bezpieczeństwa dla kadry kierowniczej

Numer usługi 2026/08/28/17164/3773748

848,70 PLN brutto
690,00 PLN netto
282,90 PLN brutto/h
230,00 PLN netto/h
261,33 PLN cena rynkowa

Dagma sp. z o.o.

4,5 / 5

470 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
03:00 h
09.11.2026 do 09.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**To intensywny kurs z zakresu cyberbezpieczeństwa, stworzony specjalnie dla kadry kierowniczej, menadżerskiej, a także osób zarządzających zespołem.** **Korzyści** • Znajomość najnowszych technik ataków i metod zbierania informacji, • Umiejętność identyfikowania i redukowania ryzyka związanego z atakami phishingowymi, wykorzystaniem zero-day exploit oraz innymi technikami cyberataków, • Wiedza, jak zabezpieczyć firmę oraz jak reagować w przypadku cyberataków, • Umiejętność przekazywania wiedzy i strategii obronnych w środowisku pracy.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Skupiając się na realnych zagrożeniach i strategiach obronnych, szkolenie doskonali umiejętności decyzyjne i przygotowuje liderów do efektywnego zarządzania ryzykiem cybernetycznym przedsiębiorstwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpozna główne cyberzagrożenia i techniki ataków.	Potrafi opisać najczęściej stosowane metody ataków (np. phishing, zero-day exploits) i ich wpływ na organizację.	Wywiad swobodny
Uczestnik zrozumie rolę kadry kierowniczej w cyberbezpieczeństwie.	Zna obowiązki menedżera w budowaniu strategii bezpieczeństwa i reagowaniu na incydenty.	Wywiad swobodny
Uczestnik zastosuje podstawowe strategie minimalizowania ryzyka cybernetycznego.	Potrafi zaproponować działania obronne i procedury zarządcze adekwatne do ryzyka.	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

Moduł 1: Wprowadzenie

1. Kto jest atrakcyjnym klientem dla cyberprzestępcy?
2. Administracja i finanse, główny cel atakujących.
3. Jak przestępcy zbierają informację o celu?

Moduł 2: Sztuczna inteligencja (AI)

1. Sztuczna inteligencja nowy rozdział w informatyce.
2. Przykłady phishingu z wykorzystaniem sztucznej inteligencji.

Moduł 3: Bezpieczeństwo operacyjne

1. OPSEC co to jest i jak działa w praktyce.
2. Klasyczna prawda w nowej odsłonie: najsłabszym ogniwem jest człowiek.
3. Procedury nie obronią firmy – ludzie i praktyka już tak.
4. Sprzęt prywatny vs. sprzęt służbowy,
5. Cyberbezpieczeństwo jako jedne z ryzyk zarządczysz?
6. Najczęstsze pułapki decyzyjne w obszarze IT na poziomie zarządczym.
7. KSeF jako nowy obszar ryzyka strategicznego dla IT.
8. Rola kadry zarządzającej w budowaniu i egzekwowaniu procesów weryfikacji oraz procedur.
9. Rola menedżerów w reakcji na incydenty bezpieczeństwa.
10. Jak zwiększyć odporność na cyberataki,

Moduł 4: Sesja pytań i odpowiedzi.

Harmonogram

Liczba pozycji harmonogramu: 6

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 Moduł 1: Wprowadzenie	Zajęcia	Łukasz Leńdźwa	09-11-2026	09:00	09:30	00:30
2 z 6 Moduł 2: Sztuczna inteligencja (AI)	Zajęcia	Łukasz Leńdźwa	09-11-2026	09:30	10:00	00:30
3 z 6 Moduł 3: Bezpieczeństwo operacyjne	Zajęcia	Łukasz Leńdźwa	09-11-2026	10:00	11:15	01:15
4 z 6 -	Przerwa	-	09-11-2026	11:15	11:30	00:15
5 z 6 Moduł 4: Sesja pytań i odpowiedzi.	Zajęcia	Łukasz Leńdźwa	09-11-2026	11:30	11:45	00:15
6 z 6 -	Walidacja	-	09-11-2026	11:45	12:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	03:00
w tym suma godzin zajęć	02:30
w tym suma godzin walidacji	00:15
w tym suma przerw	00:15
Suma godzin dydaktycznych bez przerw	03:30

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	848,70 PLN
Koszt przypadający na 1 uczestnika netto	690,00 PLN
Koszt osobogodziny brutto	282,90 PLN
Koszt osobogodziny netto	230,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	03:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Łukasz Leńdźwa

Trener IT, prowadzący szkolenia w Dagma Szkolenia IT z dziedziny cyberbezpieczeństwa. Wieloletni administrator sieci systemowych IT oraz audytor wiodący ISO. Certyfikaty: Mikrotik MTCNA (05.02.2025 – 05.02.2028), CSNA (16.09.2024 – 16.09.2027), ISO/IEC 27001:2023 Audytora Wiodącego TUV NORD (05.03.2025 – 04.03.2028) Specjalizacje: cyberbezpieczeństwo, LAN - WAN, Sieci komputerowe, Mikrotik, Active Directory, Architektura sieci, Windows server

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (prezentacja, do której dostęp zostanie udostępniony na adres e-mail uczestnika)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl** w celu rezerwacji miejsca.

Informacje dodatkowe

- - W cenę szkolenia nie wchodzą koszty związane z dojazdem, wyżywieniem oraz noclegiem.
  - Szkolenie nie zawiera egzaminu.
  - Harmonogram ma charakter ramowy i trener może na potrzeby grupy szkoleniowej zmienić długość poszczególnych modułów, przy zachowaniu niezmienionej łącznej liczby godzin usługi szkoleniowej.
  - Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
  - Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA SZKOLENIA IT.
  - Organizator szkolenia zastrzega sobie prawo do zmiany trenera prowadzącego/walidującego jeśli z przyczyn niezależnych od Organizatora (np. zdarzenie losowe) wyznaczony trener nie będzie mógł przeprowadzić szkolenia. Przy czym Organizator zobowiązuje się do zapewnienia w zastępstwie trenera o takich samych/zbliżonych kompetencjach.

Warunki techniczne

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM i/lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: https://szkolenia.dagma.eu/pl/training-list

Kontakt

Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 327 931 015