Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

454 oceny

Cyberbezpieczeństwo 2026 - Strategia bezpieczeństwa dla kadry kierowniczej

Numer usługi 2026/01/20/17164/3271631

Usługa szkoleniowa

zdalna w czasie rzeczywistym

03:00 h

01.06.2026 do 01.06.2026

848,70 PLN brutto

690,00 PLN netto

282,90 PLN brutto/h

230,00 PLN netto/h

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	15
Maksymalna liczba uczestników	100
Data zakończenia rekrutacji	25-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	3
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 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

1. Kto jest atrakcyjnym klientem dla cyberprzestępcy?
2. Administracja i finanse, główny cel atakujących.
3. Jak przestępcy zbierają informację o celu?
4. Sztuczna inteligencja nowy rozdział w informatyce.
5. Przykłady phishingu z wykorzystaniem sztucznej inteligencji.

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

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

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

Prowadzący

Liczba prowadzących: 0

Brak wyników.

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

- Jedna godzina lekcyjna to 45 minut.
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- 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.

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

Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl
Telefon (+48) 327 931 015