Możliwość dofinansowania

Logo C4Y KATARZYNA ZASIECZNA

C4Y KATARZYNA ZASIECZNA

Brak ocen dla tego dostawcy

Szkolenie: Zabezpiecz firmę od środka – cyberbezpieczeństwo i ochrona danych w produkcji (IT/OT) – Warsztat praktyczny

Numer usługi 2026/04/22/203083/3505333

2 300,00 PLN brutto
1 869,92 PLN netto
143,75 PLN brutto/h
116,87 PLN netto/h
261,33 PLN cena rynkowa

Usługa szkoleniowa
zdalna w czasie rzeczywistym
16:00 h
23.05.2026 do 24.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do osób pracujących w środowisku zakładu produkcyjnego, które w codziennej pracy mają styczność z informacją firmową, dokumentacją techniczną lub systemami/urządzeniami wykorzystywanymi w produkcji i utrzymaniu ruchu, w tym w szczególności: • biuro produkcji, • utrzymanie ruchu, • mistrzowie zmian, • logistyka wewnętrzna, • administracja, • kierownicy Grupę docelową stanowią również wszystkie zainteresowanych osób podniesieniem kompetencji w zakresie cyberbezpieczeństwa, ochrony danych oraz stosowania bezpiecznych praktyk cyfrowych w codziennej pracy.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	22-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Usługa "Szkolenie: Zabezpiecz firmę od środka – cyberbezpieczeństwo i ochrona danych w produkcji (IT/OT) – Warsztat praktyczny" przygotowuje do bezpiecznej pracy z danymi i informacją w środowisku zakładu produkcyjnego poprzez nabycie praktycznych kompetencji z zakresu ochrony danych (osobowych i firmowych) oraz cyberbezpieczeństwa ze szczególnym uwzględnieniem rozpoznawanie zagrożeń, bezpieczna praca z informacją, wzmocnienie bezpieczeństwa kont i urządzeń oraz prawidłowa reakcja na incydenty.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje i wyjaśnia zagrożenia cybernetyczne w środowisku produkcyjnym (w tym phishing/BEC) oraz ich skutki dla ciągłości działania	-wskazuje min. 3 typowe zagrożenia (np. phishing, BEC, ransomware)	Test teoretyczny
	-opisuje min. 2 możliwe skutki dla organizacji/produkcji (np. przestój, utrata danych, straty finansowe)	Test teoretyczny
Wyjaśnia zasady ochrony danych i informacji firmowej (w tym dokumentacji technicznej) oraz reguły ograniczania dostępu (need-to-know)	-rozróżnia dane osobowe vs dane firmowe/techniczne	Test teoretyczny
	-wskazuje właściwe zasady postępowania dla min. 3 przykładów informacji/dokumentów	Test teoretyczny
Opisuje podstawowe różnice IT/OT oraz typowe ryzyka związane z dostępem serwisowym, stanowiskami współdzielonymi i nośnikami	-poprawnie przypisuje min. 4 przykłady do IT/OT	Test teoretyczny
	-wskazuje min. 2 ryzyka i 2 działania ograniczające ryzyko (serwis/USB/stanowisko współdzielone)	Test teoretyczny
Identyfikuje cechy phishingu/BEC i dobiera właściwe działanie (nie otwiera/ weryfikuje/ zgłasza)	-wskazuje prawidłową reakcję w każdym scenariuszu (np. weryfikacja kanałem niezależnym, zgłoszenie)	Test teoretyczny
Dobiera bezpieczny sposób udostępnienia dokumentu lub informacji (kanał + uprawnienia + zabezpieczenia)	-wskazuje właściwy kanał (mail/chmura/link/druk)	Test teoretyczny
	-dobiera adekwatne zabezpieczenia (uprawnienia, hasło, ograniczenie czasu dostępu)	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykazuje odpowiedzialność za bezpieczeństwo informacji: stosuje zasady poufności i reaguje na nieprawidłowości	-w scenariuszach wskazuje zachowanie zgodne z zasadami poufności i minimalizacji dostępu	Test teoretyczny
	-deklaruje i uzasadnia działania ograniczające ryzyko w swoim obszarze pracy	Test teoretyczny
Współpracuje w zespole w sytuacji incydentu: komunikuje się rzeczowo, nie eskaluje błędnie, przekazuje komplet informacji	-w scenariuszu wskazuje poprawny sposób komunikacji i eskalacji (kogo, kiedy, co przekazać)	Test teoretyczny
	unika działań ryzykownych (np. „samodzielne naprawy”, przekazywanie danych nieuprawnionym)	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

Szkolenie przygotowuje do bezpiecznej pracy z informacją i dokumentacją w zakładzie produkcyjnym poprzez rozwój kompetencji z zakresu ochrony danych i cyberbezpieczeństwa. Uczestnicy uczą się rozpoznawać phishing oraz oszustwa „na dostawcę”, bezpiecznie udostępniać i przetwarzać dokumentację techniczną (np. instrukcje, rysunki, receptury), stosować zasady nadawania dostępów i pracy na stanowiskach współdzielonych, a także ograniczać ryzyka związane z dostępem serwisowym. Program uwzględnia specyfikę środowisk IT i OT oraz podstawowe zasady cyberhigieny (m.in. nośniki USB) i prawidłową reakcję na incydent.

Otwarcie szkolenia: cele, zasady pracy, kontekst IT/OT, omówienie walidacji.

Moduł 1. Dane i dokumentacja w produkcji – klasyfikacja informacji i zasady poufności

1. Rodzaje informacji w środowisku produkcyjnym: dane osobowe, dane firmowe, dane produkcyjne, dokumentacja techniczna (instrukcje, rysunki, receptury).
2. **Klasyfikacja informacji** – jak ocenić wrażliwość danych i przypisać poziom poufności.
3. Zasada **minimalizacji dostępu (need-to-know)** – role i odpowiedzialności, typowe błędy organizacyjne, konsekwencje dla ciągłości działania.
4. Przechowywanie i obieg dokumentacji: wersje robocze, kopie, wydruki, dostęp na zmianie.
5. **Ćwiczenie praktyczne:** przypisanie poziomu poufności do przykładowych dokumentów i określenie minimalnego dostępu dla ról (np. mistrz zmiany, UR, logistyka, administracja).

Moduł 2. Bezpieczne udostępnianie dokumentacji i ochrona tajemnic firmy

1. Zasady bezpiecznego udostępniania: **mail / chmura / link / druk** – ryzyka i dobre praktyki.
2. Uprawnienia i kontrola dostępu: odbiorca, zakres, czas, wersjonowanie, ograniczenie dalszego przekazywania.
3. Zabezpieczenia: hasła, szyfrowanie (jeśli stosowane), bezpieczne linki, ograniczenia pobrań, kontrola wydruków.
4. Ochrona tajemnicy przedsiębiorstwa: co jest tajemnicą firmy i jak jej nie ujawnić „przy okazji" (w korespondencji, w załącznikach, w rozmowach).
5. **Ćwiczenie praktyczne:** dobór sposobu udostępnienia dokumentu dla 3–4 scenariuszy (np. wysyłka instrukcji do podwykonawcy, przekazanie receptury, konsultacja serwisowa).

Podsumowanie

Podsumowanie dnia 1 - wnioski, pytania oraz wprowadzenie do kolejnego dnia szkolenia.

Moduł 3. Phishing i BEC w łańcuchu dostaw – rozpoznawanie i reakcja

1. Phishing w praktyce produkcyjnej: najczęstsze mechanizmy (podszycie pod dostawcę, „pilne zamówienie", „zmiana konta bankowego", „wezwanie do zapłaty").
2. BEC (Business Email Compromise) w łańcuchu dostaw – jak wygląda atak, jak oszuści budują wiarygodność.
3. Cechy ostrzegawcze w wiadomościach: domeny, linki, załączniki, język presji czasu, nietypowe prośby, zmiana danych kontaktowych/płatniczych.
4. Procedura bezpiecznej weryfikacji: niezależny kanał kontaktu, zasady potwierdzania danych, eskalacja.
5. **Ćwiczenia na scenariuszach:** analiza wiadomości / sytuacji i wybór poprawnej reakcji (nie otwiera, weryfikuje, zgłasza).

Moduł 4. Konta i dostępy oraz cyberhigiena stanowiska – IT/OT, dostęp serwisowy, minimum zasad

1. Podstawowe rozróżnienie środowisk **IT i OT** – co to oznacza dla bezpieczeństwa w produkcji.
2. Konta i dostępy: hasła, zasady ich tworzenia i przechowywania, **MFA (tam gdzie możliwe)**, dostęp czasowy.
3. Konta serwisowe i dostęp zewnętrzny: ryzyka, zasada ograniczonego dostępu, logowanie działań, odpowiedzialność.
4. Stanowiska współdzielone: blokada ekranu, wylogowanie, praca na kontach imiennych vs współdzielonych (zgodnie z zasadami firmy).
5. Nośniki i urządzenia: **USB**, skanowanie, ograniczenia, aktualizacje, minimalne zasady na zmianie.
6. **Ćwiczenie praktyczne:** „szybki audyt stanowiska" – checklista nawyków i korekta błędów.

Moduł 5. Incydent i ciągłość działania – procedura „pierwszych 15 minut" + plan wdrożenia

1. Co uznajemy za incydent w realiach produkcji (podejrzany mail/załącznik, nietypowe zachowanie systemu, blokada dostępu, wyciek danych).
2. Decyzje, które mają znaczenie: co robić, czego nie robić (np. nie „naprawiać na własną rękę", nie przekazywać dalej podejrzanych plików).
3. **Procedura pierwszych 15 minut:** rozpoznanie → zabezpieczenie → zgłoszenie → ograniczenie skutków.
4. Minimalny zakres informacji do zgłoszenia: co, kiedy, gdzie, na jakim stanowisku, jakie objawy, jakie działania podjęto.
5. **Checklista wdrożeniowa na 30 dni:** dopasowanie do działu/zmiany – wybór 3–5 działań do wdrożenia, odpowiedzialność, termin, sposób weryfikacji.

Walidacja (test teoretyczny)

Szkolenie realizowane jest w godzinach dydaktycznych.

Przerwy nie są wliczone w czas trwania usługi szkoleniowej.

Szkolenie prowadzone w godzinach dydaktycznych w formie zajęć teoretyczno-praktycznych, tzn. Szkolenie w formie zajęć teoretyczno-praktycznych łączy przekazywanie wiedzy teoretycznej z praktycznym jej zastosowaniem. Wykłady na żywo, współdzielenie ekranu, chat, dyskusja.

Uczestnicy zdobywają informacje poprzez wykłady i prezentacje, a następnie wykorzystują je w praktyce podczas warsztatów (scenariuszy branżowych, checklisty).

Rozdzielność szkolenia od walidacji - rozdzielność osobowa. Osoba szkoląca nie ocenia wiedzy i umiejętności swoich kursantów w zakresie, w którym nauczała. Końcową walidację prowadzi odrębna osoba.

Walidacja odbywa się w formie testu końcowego (15-25 pytań, w tym pytania scenariuszowe). Kryterium zaliczenia: minimum 70% poprawnych odpowiedzi. Test weryfikuje rozpoznawanie zagrożeń, zasady ochrony danych i bezpiecznej komunikacji, poprawne decyzje w scenariuszach oraz podstawy reakcji na incydent.

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej
- 1 godzina rozliczeniowa = 45 minut
- przerwy nie wliczają się do czasu szkolenia
- Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych

Harmonogram

Liczba pozycji harmonogramu: 20

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 20 Dzień 1: Otwarcie szkolenia: cele, zasady pracy, kontekst IT/OT (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	08:00	08:45	00:45
2 z 20 Moduł 1. Dane i dokumentacja w produkcji – rodzaje informacji i klasyfikacja (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	08:45	09:30	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 20 Moduł 1. Klasyfikacja informacji i zasady poufności (need-to-know, role i odpowiedzialności) (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	09:30	10:15	00:45
4 z 20 Przerwa	Beata Lewandowska	23-05-2026	10:15	10:30	00:15
5 z 20 Moduł 1. Przechowywanie i obieg dokumentacji w środowisku produkcyjnym (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	10:30	11:15	00:45
6 z 20 Moduł 1. Ćwiczenie praktyczne – klasyfikacja dokumentów i przypisanie dostępów (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	11:15	12:00	00:45
7 z 20 Przerwa	Beata Lewandowska	23-05-2026	12:00	12:30	00:30
8 z 20 Moduł 2. Bezpieczne udostępnianie dokumentacji – kanały i ryzyka. (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	12:30	13:15	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 20 Moduł 2. Zabezpieczenia i ochrona tajemnicy przedsiębiorstwa (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	13:15	14:00	00:45
10 z 20 Moduł 2. Ćwiczenie praktyczne – dobór sposobu udostępniania dokumentacji (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	23-05-2026	14:00	14:45	00:45
11 z 20 Moduł 3. Phishing i BEC w łańcuchu dostaw – mechanizmy ataków (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	08:00	08:45	00:45
12 z 20 Moduł 3. Cechy ostrzegawcze i procedury weryfikacji (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	08:45	09:30	00:45
13 z 20 Moduł 3. Ćwiczenia praktyczne – analiza scenariuszy i reakcja (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	09:30	10:15	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 20 Przerwa	Beata Lewandowska	24-05-2026	10:15	10:30	00:15
15 z 20 Moduł 4. Konta i dostępy w środowisku IT/OT – zasady i ryzyka (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	10:30	11:15	00:45
16 z 20 Moduł 4. Stanowiska współdzielone, dostęp serwisowy, cyberhigiena (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	11:15	12:00	00:45
17 z 20 Przerwa	Beata Lewandowska	24-05-2026	12:00	12:30	00:30
18 z 20 Moduł 4. Ćwiczenie praktyczne – audyt stanowiska pracy (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	12:30	13:15	00:45
19 z 20 Moduł 5. Incydent i ciągłość działania – procedura „pierwszych 15 minut”, Plan wdrożenia + podsumowanie szkolenia. (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Beata Lewandowska	24-05-2026	13:15	14:00	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 20 Walidacja - test teoretyczny. (test, chat, współdzielenie ekranu)	-	24-05-2026	14:00	14:45	00:45

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 300,00 PLN
Koszt przypadający na 1 uczestnika netto	1 869,92 PLN
Koszt osobogodziny brutto	143,75 PLN
Koszt osobogodziny netto	116,87 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Beata Lewandowska

Specjalistka w obszarze ochrony danych osobowych z wieloletnim doświadczeniem począwszy od 2009 r. i w dalszym ciągu świadczy kompleksowe usługi doradcze, szkoleniowe i audytorskie dla urzędów powiatowych i gminnych oraz jednostek im podległych. Współpracuje także z przedsiębiorstwami, spółdzielniami mieszkaniowymi, stowarzyszeniami oraz podmiotami służby zdrowia.
W 2015 r. ukończyła studia podyplomowe z zakresu ochrony danych oraz uzyskaniu certyfikatu audytora wiodącego ISO/IEC 27001. W ostatnuch 5 latach przed publikacją oferty zrealizowała na dużą skalę szkolenia, konferencje oraz wdrożenia dokumentacji Systemów Zarządzania Bezpieczeństwem Informacji zgodnych z RODO, Krajowymi Ramami Interoperacyjności (KRI) oraz ISO/IEC 27001 na terenie całego kraju. W tym okresie przeprowadziła ponad 1000 audytów KRI i RODO, identyfikując kluczowe ryzyka, weryfikując zgodność z przepisami oraz rekomendując praktyczne działania korygujące. Opracowała kompleksową dokumentację i procedury dostosowane do specyfiki różnych sektorów i jednostek.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypt/kompendium szkoleniowe – podsumowanie kluczowych zasad ochrony danych i cyberbezpieczeństwa w środowisku produkcyjnym.

Informacje dodatkowe

Zapisując się na usługę wyrażasz zgodę na rejestrowanie/nagrywanie swojego wizerunku na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów uczenia się.

Usługa może być zwolniona z VAT dla Uczestników, których poziom dofinansowania wynosi co najmniej 70% na podstawie § 3 ust. 1 pkt. 14 Rozporządzenia Ministrów Finansów z 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

Warunki techniczne

Platforma: MS Teams

iOS: iOS 11

Windows: Windows 10 kompilacja 14393

Android: Android OS 5.0

Funkcje sieci Web. Najnowsza wersja przeglądarki Safari, Internet Explorer 11, Chrome, Edge lub Firefox

Komputer Mac: MacOS 10.13

Połączenie internetowe: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach:

- dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie).

- dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie).

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Link: będzie udostępniony i umieszczony w karcie na 5 dni roboczych przed szkoleniem.

Kontakt

KATARZYNA ZASIECZNA

E-mail katarzynazasieczna@gmail.com

Telefon (+48) 668 163 580