Możliwość dofinansowania

SOVERANO

SOVERANO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,6 / 5

121 ocen

Protokoły bezpieczeństwa i reakcja na ataki

Numer usługi 2026/06/10/217200/3617737

800,00 PLN brutto
800,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
175,56 PLN cena rynkowa

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
08:00 h
15.07.2026 do 15.07.2026

Informacje podstawowe

Kategoria	Prawo i administracja / Administracja publiczna
Grupa docelowa usługi	Usługa dedykowana jest wszystkim pracownikom zatrudnionym w Jednostkach Samorządu Terytorialnego oraz instytucjach podległych, bez względu na zajmowane stanowisko urzędnicze (działy finansowe, kadrowe, obsługi mieszkańca, administracyjne, MOPS, oczyszczalnie), dążącym do opanowania technik identyfikacji zagrożeń sieciowych i procedur kryzysowych.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	14-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Usługa prowadzi osobę uczestniczącą do samodzielnego identyfikowania anomalii systemowych wskazujących na atak hakerski, bezbłędnego uruchamiania procedur bezpieczeństwa oraz realizowania specyficznych dobrych praktyk ochrony danych na każdym stanowisku w JST.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. Identyfikuje oznaki i wektory ataków hakerskich specyficzne dla pracy w administracji publicznej.	Osoba szkolona odróżnia fałszywą wiadomość systemową od autentycznej korespondencji urzędowej.	Test teoretyczny z wynikiem generowanym automatycznie
	Osoba szkolona lokalizuje podejrzane zachowania infrastruktury sieciowej na swoim stanowisku pracy.	Test teoretyczny z wynikiem generowanym automatycznie
2. Konfiguruje i wdraża natychmiastowe protokoły bezpieczeństwa w sytuacji wykrycia działania niepożądanego w systemie JST.	Osoba szkolona wykonuje sekwencję kroków odcięcia stacji roboczej od sieci lokalnej zgodnie z procedurą kryzysową.	Test teoretyczny z wynikiem generowanym automatycznie
	Osoba szkolona sporządza prawidłowe zgłoszenie incydentu dla wewnętrznego zespołu IT oraz organów nadzorczych.	Test teoretyczny z wynikiem generowanym automatycznie
3. Analizuje ryzyka operacyjne na swoim stanowisku pracy pod kątem wycieku danych obywateli i tajemnicy służbowej.	Osoba szkolona wdraża zasady czystego biurka i bezpiecznego zarządzania uprawnieniami dostępowymi.	Test teoretyczny z wynikiem generowanym automatycznie
	Osoba szkolona mapuje punkty krytyczne w codziennym przepływie dokumentacji elektronicznej w swoim dziale.	Test teoretyczny z wynikiem generowanym automatycznie

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

Warunki organizacyjne:

- **Czas trwania usługi:** 8 godzin zegarowych (60 min)
- **Przerwy:** wliczone w czas usługi rozwojowej i odbywają się zgodnie z harmonogramem.
- **Klauzula Dostępności:** W oparciu o zasadę racjonalnych usprawnień i dostępności (wynikającą z Ustawy o dostępności) oraz standardy równego traktowania, organizator zapewnia wsparcie dla osób ze szczególnymi potrzebami. W celu skorzystania z racjonalnych usprawnień, uczestnik proszony jest o wcześniejsze zgłoszenie swoich potrzeb organizatorowi szkolenia.
- **Platforma:** Google Meet lub Zoom (obsługa przez przeglądarkę).
- **Wymagania:** Komputer, stabilne łącze internetowe, mikrofon oraz **obowiązkowo włączona kamera** (niezbędna do walidacji tożsamości i aktywności).
- **Dostęp:** Link znajduje się w sekcji karty kody dostępowe.
- **Walidacja:** Walidacja przeprowadzana jest w formie testu teoretycznego generowanego wynikiem automatycznym. W celu zapewnienia obiektywności oceny, proces walidacji jest prowadzony zgodnie z zasadą rozdzielności procesów kształcenia i walidacji.
- **Typy zajęć:** [T] Teoretyczne: Wykłady, prezentacje, analiza koncepcji. [P] Praktyczne: Ćwiczenia, zadania, praca z narzędziami pod okiem trenera. [M] Mieszane: Łączą wprowadzenie teoretyczne z zadaniami praktycznymi.

PROGRAM SZKOLENIA

Merytoryka szkolenia skupia się na budowaniu praktycznych nawyków obronnych wśród pracowników każdego działu JST, eliminując czynnik ludzki jako najczęstsze źródło udanych ataków hakerskich. Program opiera się na analizie rzeczywistych studiów przypadków naruszeń bezpieczeństwa w polskich samorządach i został podzielony na moduły dostosowane do specyfiki poszczególnych stanowisk (od księgowości MOPS po operatorów systemów w oczyszczalniach). Osoby uczestniczące przejdą przez intensywne symulacje sytuacji kryzysowych, ucząc się, jak reagować w pierwszych minutach po wykryciu złośliwego oprogramowania blokującego komputery (ransomware). Warsztaty pozwalają na wdrożenie automatycznych odruchów bezpieczeństwa, co bezpośrednio chroni ciągłość działania urzędu i zapobiega paraliżowi usług publicznych.

HARMONOGRAM SZCZEGÓŁOWY

Dzień 1 (15.07.2026)

- **09:00 – 11:00** Typologia cyberataków na administrację publiczną: jak myślą i działają współcześni hakerzy [M] – Osoba prowadząca: Maciej Cieśla
- **11:00 – 11:15** Przerwa (obowiązkowa, wliczana do czasu usługi)
- **11:15 – 13:00** Dobre praktyki bezpieczeństwa dla poszczególnych działów JST (Kadry, Finanse, Podległe Ośrodki) [P] – Osoba prowadząca: Maciej Cieśla
- **13:00 – 13:30** Przerwa (obowiązkowa, wliczana do czasu usługi)
- **13:30 – 15:30** Warsztaty detekcji: rozpoznawanie zaawansowanego phishingu i złośliwego oprogramowania [P] – Osoba prowadząca: Maciej Cieśla
- **15:30 – 15:45** Przerwa (obowiązkowa, wliczana do czasu usługi)
- **15:45 – 16:45** Zarządzanie incydentem: wdrażanie protokołów awaryjnych i schematy powiadamiania [T] – Osoba prowadząca: Maciej Cieśla
- **16:45 – 17:00** Walidacja efektów uczenia się (Test wiedzy) – Osoba wykonująca walidację: Mateusz Świąder

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Typologia cyberataków na administrację publiczną: jak myślą i działają współcześni hakerzy	Zajęcia	Maciej Cieśla	15-07-2026	09:00	11:00	02:00
2 z 8 -	Przerwa	-	15-07-2026	11:00	11:15	00:15
3 z 8 Dobre praktyki bezpieczeństwa dla poszczególnych działów JST (Kadry, Finanse, Podległe Ośrodki)	Zajęcia	Maciej Cieśla	15-07-2026	11:15	13:00	01:45
4 z 8 -	Przerwa	-	15-07-2026	13:00	13:30	00:30
5 z 8 Warsztaty detekcji: rozpoznawanie zaawansowanego phishingu i złośliwego oprogramowania	Zajęcia	Maciej Cieśla	15-07-2026	13:30	15:30	02:00
6 z 8 -	Przerwa	-	15-07-2026	15:30	15:45	00:15
7 z 8 Zarządzanie incydentem: wdrażanie protokołów awaryjnych i schematy powiadamiania	Zajęcia	Maciej Cieśla	15-07-2026	15:45	16:45	01:00
8 z 8 -	Walidacja	-	15-07-2026	16:45	17:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:45
w tym suma godzin walidacji	00:15
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	800,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Maciej Cieśla

Maciej Cieśla – ceniony ekspert, praktyk oraz doświadczona osoba prowadząca procesy edukacyjne, specjalizująca się w szeroko rozumianym bezpieczeństwie informacji, ochronie danych osobowych oraz przeciwdziałaniu nowoczesnym zagrożeniom cyfrowym. Posiada wieloletnie

doświadczenie zawodowe, które zdobywał realizując zaawansowane projekty z zakresu audytu, wdrażania systemów zarządzania bezpieczeństwem oraz szkolenia kadr administracji publicznej i sektora prywatnego. Jego wiedza merytoryczna jest poparta licznymi certyfikatami o charakterze międzynarodowym, co gwarantuje najwyższy standard merytoryczny prowadzonych zajęć.
Maciej Cieśla Specjalizuje się w analizie ryzyka, projektowaniu bezpiecznych procedur obiegu dokumentacji oraz weryfikacji odporności systemów na próby nieuprawnionego uzyskania dostępu do informacji wrażliwych. Jego unikalne kompetencje pozwalają osobom uczestniczącym na głębokie zrozumienie mechanizmów działania oszustw internetowych oraz naukę skutecznych metod obrony przed nimi w codziennej pracy urzędnika.
W procesie kształcenia stawia na budowanie realnej sprawczości osób szkolonych, ucząc ich nie tylko przepisów Ogólnego Rozporządzenia o Ochronie Danych, ale przede wszystkim krytycznego myślenia w obliczu incydentów bezpieczeństwa.
Posiadane doświadczenie zawodowe i kompetencje spełniają wymagania Bazy Usług Rozwojowych

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Osoba uczestnicząca otrzymuje algorytmy postępowania w sytuacjach kryzysowych w formie grafik, checklistę codziennych dobrych praktyk na stanowisku urzędniczym oraz wzorce formularzy raportowania incydentów.

Warunki uczestnictwa

Aby wziąć udział w szkoleniu, uczestnik powinien być zainteresowany tematem, otwarty na naukę, gotowy do pracy w grupie, posiadać podstawowe umiejętności komunikacyjne oraz mieć dostęp do narzędzi niezbędnych do udziału w szkoleniu. Warunkiem udziału w usłudze jest dokonanie zapisu na usługę co najmniej 1 dzień (do godziny 14.00), przed jej rozpoczęciem i uzyskanie akceptacji ze strony Dostawcy Usługi. Warunkiem uzyskania zaświadczenia/certyfikatu jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej, oraz uzyskanie pozytywnej oceny dla każdego uczestnika na podstawie wyniku walidacji przeprowadzonej przez podmiot walidujący/Walidatora. Odwołanie Usługi rozwojowej możliwe jest do dnia zakończenia usługi w przypadku braku zapisanych uczestników lub w przypadku, gdy wszystkie zapisy uczestników mają status „rezygnacja” lub „odrzucony”. W innych przypadkach odwołanie Usługi rozwojowej możliwe jest na 1 dzień przed rozpoczęciem.

Informacje dodatkowe

Dodatkowo uczestnik zobowiązany jest do okazania się dokumentem potwierdzającym tożsamość ze zdjęciem, przed zespołem monitorującym usługę rozwojową.

Walidacja jest prowadzona w formie testu wiedzy z wynikiem generowanym automatycznie, co zapewnia obiektywną i natychmiastową weryfikację nabytych kompetencji. Proces ten odbywa się w ostatnim bloku szkolenia (godz. 16.45–17:00) pod nadzorem niezależnego walidatora, zgodnie z zasadą rozdzielności funkcji dydaktycznej od oceniającej.

Warunki techniczne

Dla optymalnego udziału w usłudze zdalnej w czasie rzeczywistym, każdy uczestnik powinien dysponować: Stabilnym łączem internetowym o minimalnej przepustowości łącza do pobierania: 10 Mb/s i wysyłania: 5 Mb/s (dla połączeń indywidualnych, w przypadku grupowych zalecane wyższe parametry). Komputerem stacjonarnym lub laptopem z zainstalowanym i aktualnym systemem operacyjnym(Windows 10/11 lub macOS 10.15 i nowsze) oraz przeglądarką internetową (zalecana najnowsza wersja Google Chrome dla pełnej funkcjonalności Meet, akceptowane są również Edge, Firefox lub Safari). Sprawnym mikrofonem i głośnikami/słuchawkami (zalecane słuchawki z mikrofonem dla lepszej jakości dźwięku i eliminacji echa). Sprawną kamerą internetową (wbudowaną lub zewnętrzną)umożliwiającą transmisję obrazu. Brak konieczności instalacji dodatkowej aplikacji – Google Meet działa w pełni poprzez przeglądarkę internetową. Wymagane jest jedynie posiadanie konta Google (Gmail) dołączonego do przeglądarki lub podanie e-maila, na który zostanie wysłane zaproszenie. Platforma Realizacji Usługi Wszystkie sesje usługi będą realizowane zdalnie, w czasie rzeczywistym,

za pośrednictwem platformy Google Meet. Uczestnicy otrzymają unikalny link do dołączenia do dedykowanego spotkania Google Meet przed rozpoczęciem usługi. Link zostanie wysłany drogą elektroniczną (e-mail) lub poprzez udostępniony wcześniej kalendarz (np. GoogleCalendar). Prosimy o punktualne dołączanie do sesji, klikając w otrzymany link.

Kontakt

MATEUSZ ŚWIĄDER

E-mail swiadermateusz@gmail.com

Telefon (+48) 733 058 666