Możliwość dofinansowania

MIC centre Liliia Sles

Brak ocen dla tego dostawcy

Specjalistyczny język angielski w cyberbezpieczeństwie: zarządzanie incydentami bezpieczeństwa IT i komunikacja kryzysowa (Kurs indywidualny).

Numer usługi 2026/08/13/227222/3745361

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia indywidualne
81:00 h
17.11.2026 do 23.11.2027

16 000,00 PLN brutto
16 000,00 PLN netto
197,53 PLN brutto/h
197,53 PLN netto/h
166,67 PLN cena rynkowa

Informacje podstawowe

Kategoria	Języki / Angielski
Grupa docelowa usługi	**Szkolenie jest skierowane do osób, dla których specjalistyczna znajomość języka angielskiego stanowi niezbędne narzędzie pracy przy wdrażaniu nowych technologii oraz zarządzaniu bezpieczeństwem informacji. Odbiorcami wsparcia są:** 1. **Pracodawcy oraz kadra zarządzająca** (w tym osoby prowadzące jednoosobową działalność gospodarczą zatrudniające pracowników), odpowiedzialni za nadzór nad infrastrukturą IT, wdrażanie polityk bezpieczeństwa, zarządzanie ryzykiem operacyjnym oraz komunikację kryzysową z partnerami biznesowymi w sytuacjach zagrożeń cyfrowych. 2. **Specjaliści ds. IT, programiści, administratorzy sieci i systemów**, którzy w codziennej pracy wykorzystują zaawansowane narzędzia diagnostyczne, oprogramowanie monitorujące zagrożenia oraz międzynarodowe bazy wiedzy o podatnościach (np. CVE, standardy NIST, OWASP), dostępne wyłącznie w języku angielskim. 3. **Pracownicy wyznaczeni do reagowania na incydenty bezpieczeństwa**, którzy potrzebują precyzyjnych kompetencji język.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1
Data zakończenia rekrutacji	16-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do samodzielnego posługiwania się specjalistycznym językiem angielskim w obszarze cyberbezpieczeństwa i technologii informatycznych. Po zakończeniu usługi uczestnik samodzielnie analizuje anglojęzyczną dokumentację techniczną, skutecznie zarządza incydentami bezpieczeństwa IT zgodnie z międzynarodowymi standardami NIST i OWASP, a także sprawnie prowadzi komunikację kryzysową z zagranicznymi partnerami oraz zespołami Incident Response (reagowania na incydenty).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Posługuje się specjalistyczną terminologią z zakresu cyberbezpieczeństwa i systemów IT w języku angielskim.	Definiuje kluczowe pojęcia techniczne w języku angielskim z obszaru zagrożeń sieciowych (np. phishing, ransomware, DDoS, malware, social engineering).	Test teoretyczny z wynikiem generowanym automatycznie
	Rozróżnia rodzaje podatności systemów IT na podstawie anglojęzycznych opisów i klasyfikacji.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje dokumentację techniczną oraz standardy bezpieczeństwa IT w języku angielskim.	Charakteryzuje strukturę anglojęzycznego raportu z audytu bezpieczeństwa IT.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje właściwe procedury reagowania na incydenty na podstawie anglojęzycznych wytycznych technicznych.	Test teoretyczny z wynikiem generowanym automatycznie
Komunikuje się w sytuacjach kryzysowych związanych z incydentami IT w języky angielskim.	Charakteryzuje etapy procesu obsługi incydentu (Incident Response) w komunikacji z międzynarodowym zespołem technicznym.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera właściwe zwroty i techniki komunikacji kryzysowej w języku angielskim do kontaktu z klientem biznesowym (B2B) po wystąpieniu incydentu (np. wycieku danych).	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

Moduł I: Zaawansowana terminologia cyberbezpieczeństwa i systemów IT

- **Czas trwania:** 10 spotkań (15 godzin zegarowych).
- **Tematyka:** Szczegółowa terminologia techniczna i słownictwo branżowe. Rodzaje zagrożeń sieciowych w języku angielskim (phishing, ransomware, DDoS, malware, social engineering, brute-force, SQL injection, man-in-the-middle). Architektura systemów IT i nazewnictwo zaawansowanych zabezpieczeń (firewalls, SIEM, SOAR, EDR, szyfrowanie, MFA, protokoły sieciowe).
- **Metody pracy:** Ćwiczenia leksykalne, praca z tekstami technicznymi, tworzenie słowników pojęciowych, analiza case studies dotyczących architektur bezpieczeństwa.

Moduł II: Analiza dokumentacji technicznej, norm prawnych i standardów bezpieczeństwa IT

- **Czas trwania:** 14 spotkań (21 godzin zegarowych).
- **Tematyka:** Struktura, interpretacja i praktyczne zastosowanie anglojęzycznych standardów bezpieczeństwa informacji (szczegółowe wytyczne NIST - National Institute of Standards and Technology, ISO/IEC 27001 oraz OWASP Top 10). Praca z międzynarodowymi bazami danych o podatnościach i zagrożeniach (CVE - Common Vulnerabilities and Exposures). Analiza i interpretacja logów systemowych, alertów bezpieczeństwa oraz raportów podatności generowanych przez systemy skanujące w języku angielskim.
- **Metody pracy:** Analiza dokumentów źródłowych (standardy NIST, OWASP), symulacje identyfikacji podatności w bazach CVE, ćwiczenia z tłumaczenia i interpretacji logów i alertów systemowych, redagowanie notatek technicznych.

Moduł III: Zarządzanie incydentami bezpieczeństwa IT (Incident Response) w języku angielskim

- **Czas trwania:** 14 spotkań (21 godzin zegarowych).
- **Tematyka:** Fazy obsługi incydentów bezpieczeństwa (Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-Incident Activity) według metodologii NIST w środowisku anglojęzycznym. Sporządzanie szczegółowej dokumentacji powypadkowej i raportów z incydentów (Incident Reports) w języku angielskim. Formułowanie procedur operacyjnych (SOP - Standard Operating Procedures) oraz polityk bezpieczeństwa. Komunikacja techniczna wewnątrz zespołów Incident Response oraz koordynacja działań naprawczych z międzynarodowymi specjalistami.
- **Metody pracy:** Symulacje procesów Incident Response (scenariusze typu role-play), redagowanie raportów z symulowanych naruszeń, tworzenie procedur SOP, ćwiczenia komunikacyjne w sytuacjach presji czasu.

Moduł IV: Komunikacja kryzysowa i relacje biznesowe B2B w cyberbezpieczeństwie

- **Czas trwania:** 14 spotkań (21 godzin zegarowych).
- **Tematyka:** Przygotowywanie oficjalnych komunikatów zewnętrznych (dla klientów, partnerów biznesowych, organów nadzorczych, mediów) w języku angielskim w przypadku wystąpienia incydentów bezpieczeństwa i wycieków danych. Strategie komunikacji kryzysowej w relacjach B2B. Prowadzenie negocjacji, ustaleń technicznych oraz audytów z międzynarodowymi partnerami, zagranicznymi ubezpieczycielami ryzyka cybernetycznego oraz zewnętrznymi dostawcami technologii IT.
- **Metody pracy:** Tworzenie szablonów oświadczeń kryzysowych (data breach notifications), symulacje rozmów kryzysowych i negocjacji z partnerami zagranicznymi, odgrywanie ról audytora i audytowanego.

Moduł V: Walidacja i ewaluacja efektów uczenia się

- **Czas trwania:** 2 spotkania (3 godziny zegarowe).

- **Tematyka:** Podsumowanie całego cyklu szkoleniowego, powtórzenie i utrwalenie kluczowych zagadnień leksykalnych oraz struktur komunikacyjnych. Przeprowadzenie walidacji efektów uczenia się. Ewaluacja szkolenia i omówienie wyników.
- **Metody pracy:**
  - *Spotkanie 53 (1,5 godz. zegarowej):* Walidacja w formie testu teoretycznego z wynikiem generowanym automatycznie na platformie szkoleniowej.
  - *Spotkanie 54 (1,5 godz. zegarowej):* Indywidualna informacja zwrotna, szczegółowe omówienie błędów oraz określenie obszarów do dalszego rozwoju.

Harmonogram

Liczba pozycji harmonogramu: 54

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 54 Moduł I:Wprowadzenie do terminologii bezpieczeństwa informacji i systemów IT. Podstawowe pojęcia techniczne.	Zajęcia	LILIIA SLES	17-11-2026	18:00	19:30	01:30
2 z 54 Słownictwo związane z architekturą sieciową, protokołami bezpiecznymi (HTTPS, SSH, SFTP) i infrastrukturą IT.	Zajęcia	LILIIA SLES	23-11-2026	18:00	19:30	01:30
3 z 54 Rodzaje zagrożeń cyfrowych i wektorów ataków: Socjotechnika (Social Engineering) i Phishing w języku angielskim.	Zajęcia	LILIIA SLES	30-11-2026	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 54 Zagrożenia typu Malware: Ransomware, Spyware, Adware – analizowanie opisów technicznych.	Zajęcia	LILIIA SLES	07-12-2026	18:00	19:30	01:30
5 z 54 Ataki sieciowe: DDoS (Distributed Denial of Service) oraz Brute-Force – słownictwo techniczne.	Zajęcia	LILIIA SLES	14-12-2026	18:00	19:30	01:30
6 z 54 Zaawansowane podatności aplikacji webowych: SQL Injection oraz Man-in-the-Middle (MitM) – terminologia.	Zajęcia	LILIIA SLES	21-12-2026	18:00	19:30	01:30
7 z 54 Narzędzia i systemy ochrony: Zapory sieciowe (Firewalls), EDR (Endpoint Detection and Response) – terminologia wdrożeniowa.	Zajęcia	LILIIA SLES	28-12-2026	18:00	19:30	01:30
8 z 54 Systemy monitorowania bezpieczeństwa: Narzędzia SIEM (Security Information and Event Management) oraz SOAR.	Zajęcia	LILIIA SLES	04-01-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 54 Słownictwo z zakresu uwierzytelniania (MFA - Multi-Factor Authentication, biometria) oraz mechanizmów szyfrowania danych.	Zajęcia	LILIIA SLES	11-01-2027	18:00	19:30	01:30
10 z 54 Podsumowanie Modułu I. Ćwiczenia leksykalne, powtórzenie słownictwa technicznego i analiza case studies.	Zajęcia	LILIIA SLES	18-01-2027	18:00	19:30	01:30
11 z 54 Moduł II:Wprowadzenie do międzynarodowych standardów bezpieczeństwa IT. Struktura dokumentacji w języku angielskim.	Zajęcia	LILIIA SLES	25-01-2027	18:00	19:30	01:30
12 z 54 Standardy NIST (National Institute of Standards and Technology) CSF – fazy Identify (Identyfikacja) oraz Protect (Ochrona).	Zajęcia	LILIIA SLES	01-02-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 54 Standardy NIST (National Institute of Standards and Technology) CSF – fazy Identify (Identyfikacja) oraz Protect (Ochrona).	Zajęcia	LILIIA SLES	08-02-2027	18:00	19:30	01:30
14 z 54 Standardy NIST CSF – fazy Detect (Wykrywanie) oraz Respond (Reagowanie) w dokumentacji technicznej.	Zajęcia	LILIIA SLES	15-02-2027	18:00	19:30	01:30
15 z 54 Czytanie, interpretacja i tłumaczenie logów systemów operacyjnych oraz logów sieciowych w języku angielskim.	Zajęcia	LILIIA SLES	22-02-2027	18:00	19:30	01:30
16 z 54 Standard OWASP Top 10 (Open Web Application Security Project) – analiza najczęstszych podatności aplikacji.	Zajęcia	LILIIA SLES	01-03-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 54 Analiza alertów bezpieczeństwa i praca z bazami danych o podatnościach CVE	Zajęcia	LILIIA SLES	08-03-2027	18:00	19:30	01:30
18 z 54 Analiza alertów bezpieczeństwa i praca z bazami danych o podatnościach CVE	Zajęcia	LILIIA SLES	15-03-2027	18:00	19:30	01:30
19 z 54 Analiza alertów bezpieczeństwa i praca z bazami danych o podatnościach CVE	Zajęcia	LILIIA SLES	22-03-2027	18:00	19:30	01:30
20 z 54 Słownictwo i analiza raportów z audytów bezpieczeństwa IT	Zajęcia	LILIIA SLES	29-03-2027	18:00	19:30	01:30
21 z 54 Słownictwo i analiza raportów z audytów bezpieczeństwa IT	Zajęcia	LILIIA SLES	05-04-2027	18:00	19:30	01:30
22 z 54 Redagowanie notatek technicznych i dokumentacji konfiguracji sieci	Zajęcia	LILIIA SLES	12-04-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 54 Redagowanie notatek technicznych i dokumentacji konfiguracji sieci	Zajęcia	LILIIA SLES	19-04-2027	18:00	19:30	01:30
24 z 54 Podsumowanie modułu, ćwiczenia leksykalne i powtórzenie materiału	Zajęcia	LILIIA SLES	26-04-2027	18:00	19:30	01:30
25 z 54 Moduł III: Cykl życia incydentu oraz faza przygotowania planów reagowania (Incident Response)	Zajęcia	LILIIA SLES	03-05-2027	18:00	19:30	01:30
26 z 54 Cykl życia incydentu oraz faza przygotowania planów reagowania (Incident Response)	Zajęcia	LILIIA SLES	10-05-2027	18:00	19:30	01:30
27 z 54 Faza wykrywania, analizy oraz powstrzymywania incydentów IT	Zajęcia	LILIIA SLES	17-05-2027	18:00	19:30	01:30
28 z 54 Faza wykrywania, analizy oraz powstrzymywania incydentów IT	Zajęcia	LILIIA SLES	24-05-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
29 z 54 Faza eliminacji zagrożeń, odzyskiwania danych oraz analiza lessons learned	Zajęcia	LILIIA SLES	31-05-2027	18:00	19:30	01:30
30 z 54 Faza eliminacji zagrożeń, odzyskiwania danych oraz analiza lessons learned	Zajęcia	LILIIA SLES	07-06-2027	18:00	19:30	01:30
31 z 54 Sporządzanie raportów powypadkowych (Ransomware, Data Breach Report)	Zajęcia	LILIIA SLES	14-06-2027	18:00	19:30	01:30
32 z 54 Sporządzanie raportów powypadkowych (Ransomware, Data Breach Report)	Zajęcia	LILIIA SLES	21-06-2027	18:00	19:30	01:30
33 z 54 Sporządzanie raportów powypadkowych (Ransomware, Data Breach Report)	Zajęcia	LILIIA SLES	28-06-2027	18:00	19:30	01:30
34 z 54 Opracowywanie Standardowych Procedur Operacyjnych (SOP) oraz komunikacja pod presją czasu	Zajęcia	LILIIA SLES	05-07-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
35 z 54 Opracowywanie Standardowych Procedur Operacyjnych (SOP) oraz komunikacja pod presją czasu	Zajęcia	LILIIA SLES	12-07-2027	18:00	19:30	01:30
36 z 54 Koordynacja działań naprawczych i komunikacja z międzynarodowymi zespołami	Zajęcia	LILIIA SLES	19-07-2027	18:00	19:30	01:30
37 z 54 Koordynacja działań naprawczych i komunikacja z międzynarodowymi zespołami	Zajęcia	LILIIA SLES	26-07-2027	18:00	19:30	01:30
38 z 54 Praktyczna symulacja obsługi incydentu i podsumowanie modułu	Zajęcia	LILIIA SLES	02-08-2027	18:00	19:30	01:30
39 z 54 Moduł IV: Wprowadzenie do komunikacji kryzysowej oraz przygotowywanie powiadomień dla klientów	Zajęcia	LILIIA SLES	09-08-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
40 z 54 Wprowadzenie do komunikacji kryzysowej oraz przygotowywanie powiadomień dla klientów	Zajęcia	LILIIA SLES	16-08-2027	18:00	19:30	01:30
41 z 54 Opracowywanie komunikatów o naruszeniu danych dla organów nadzorczych i mediów	Zajęcia	LILIIA SLES	23-08-2027	18:00	19:30	01:30
42 z 54 Opracowywanie komunikatów o naruszeniu danych dla organów nadzorczych i mediów	Zajęcia	LILIIA SLES	30-08-2027	18:00	19:30	01:30
43 z 54 Zarządzanie kryzysem wizerunkowym B2B oraz prowadzenie rozmów z partnerami	Zajęcia	LILIIA SLES	06-09-2027	18:00	19:30	01:30
44 z 54 Zarządzanie kryzysem wizerunkowym B2B oraz prowadzenie rozmów z partnerami	Zajęcia	LILIIA SLES	13-09-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
45 z 54 Słownictwo w relacjach z ubezpieczycielami oraz przygotowanie do audytu bezpieczeństwa	Zajęcia	LILIIA SLES	20-09-2027	18:00	19:30	01:30
46 z 54 Słownictwo w relacjach z ubezpieczycielami oraz przygotowanie do audytu bezpieczeństwa	Zajęcia	LILIIA SLES	27-09-2027	18:00	19:30	01:30
47 z 54 Symulacja audytu językowego - odgrywanie roli audytora oraz audytowanego	Zajęcia	LILIIA SLES	04-10-2027	18:00	19:30	01:30
48 z 54 Symulacja audytu językowego - odgrywanie roli audytora oraz audytowanego	Zajęcia	LILIIA SLES	11-10-2027	18:00	19:30	01:30
49 z 54 Komunikacja z dostawcami usług IT oraz zarządem (C-level) podczas incydentów	Zajęcia	LILIIA SLES	18-10-2027	18:00	19:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
50 z 54 Komunikacja z dostawcami usług IT oraz zarządem (C-level) podczas incydentów	Zajęcia	LILIIA SLES	25-10-2027	18:00	19:30	01:30
51 z 54 Prezentowanie raportów technicznych dla krytycznych odbiorców i podsumowanie	Zajęcia	LILIIA SLES	01-11-2027	18:00	19:30	01:30
52 z 54 Prezentowanie raportów technicznych dla krytycznych odbiorców i podsumowanie	Zajęcia	LILIIA SLES	08-11-2027	18:00	19:30	01:30
53 z 54 -	Walidacja	LILIIA SLES	15-11-2027	18:00	19:30	01:30
54 z 54 Moduł V: Ewaluacja końcowa szkolenia, indywidualna informacja zwrotna i podsumowanie	Zajęcia	LILIIA SLES	22-11-2027	18:00	19:30	01:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	81:00
w tym suma godzin zajęć	79:30
w tym suma godzin walidacji	01:30
Suma godzin dydaktycznych bez przerw	108:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	16 000,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	16 000,00 PLN
Koszt osobogodziny brutto	197,53 PLN
Koszt osobogodziny netto	197,53 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	81:00

Prowadzący

Liczba prowadzących: 1

1 z 1

LILIIA SLES

Dyplomowany lektor języka angielskiego z wieloletnim doświadczeniem w nauczaniu osób dorosłych oraz klientów biznesowych. Specjalizuje się w prowadzeniu szkoleń z zakresu Business English oraz specjalistycznego języka dla branży IT (English for IT). Posiada bogate, praktyczne doświadczenie we współpracy ze specjalistami z sektora technologicznego. Doskonale rozumie specyfikę pracy w projektach IT oraz zna branżową terminologię techniczną, niezbędną do czytania dokumentacji, komunikacji z klientem zagranicznym. W swojej pracy szkoleniowej kładzie największy nacisk na przełamywanie bariery komunikacyjnej, rozwijanie płynności wypowiedzi oraz praktyczne zastosowanie języka w realnych sytuacjach zawodowych. Posiada doświadczenie w samodzielnym opracowywaniu materiałów dydaktycznych. Charakteryzuje się wysokimi umiejętnościami interpersonalnymi oraz indywidualnym podejściem do każdego uczestnika.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzymuje kompletny, autorski zestaw materiałów dydaktycznych w wersji elektronicznej (pliki PDF) lub drukowanej, wspierających proces nabywania kompetencji językowych w obszarze cyberbezpieczeństwa. W skład pakietu wchodzą:

1. Autorski skrypt szkoleniowy zawierający kompendium specjalistycznego słownictwa angielskiego, zwrotów oraz struktur stosowanych w analizie zagrożeń IT i komunikacji kryzysowej.
2. Praktyczne szablony dokumentacji w języku angielskim: wzory raportów z incydentów (Incident Reports), powiadomień o wycieku danych (Data Breach Notifications) oraz procedur operacyjnych (SOP).
3. Wyciągi z anglojęzycznych standardów NIST i wytycznych OWASP, dostosowane do celów dydaktycznych.

Warunki techniczne

Aby wziąć udział w szkoleniu realizowanym w formie zdalnej, uczestnik musi spełniać następujące warunki techniczne:

- **Sprzęt:** Komputer stacjonarny lub laptop wyposażony w sprawną kamerę internetową oraz mikrofon (zalecane jest korzystanie z zestawu słuchawkowego z mikrofonem w celu zapewnienia optymalnej jakości dźwięku i eliminacji szumów z otoczenia).
- **Połączenie internetowe:** Stabilne, szerokopasmowe połączenie z internetem (zalecana minimalna prędkość pobierania/wysyłania to 10 Mbps), pozwalające na płynną transmisję audio i wideo.
- **Oprogramowanie:** Zaktualizowana przeglądarka internetowa (np. Google Chrome, Mozilla Firefox, Microsoft Edge) oraz darmowa aplikacja / dostęp przeglądarkowy do platformy komunikacyjnej **np. MS Teams / Zoom / Google Meet**, na której będą odbywać się zajęcia.
- **Materiały:** Oprogramowanie umożliwiające otwieranie i odczytywanie plików w formacie PDF (np. Adobe Acrobat Reader) oraz podstawowy edytor tekstu.

Kontakt

LILIIA SLES

E-mail slesliliia@gmail.com
Telefon (+48) 786 588 749