Szkolenie: CompTIA
CompTIA SecAI+ Prep Course

DOSTĘPNE TERMINY

2026-12-14 | 5 dni | Warszawa / Wirtualna sala

Cel szkolenia:

Szkolenie CompTIA SecAI+ przygotowuje uczestników do skutecznego zabezpieczania, nadzorowania i odpowiedzialnej integracji sztucznej inteligencji z operacjami cyberbezpieczeństwa. Program koncentruje się na praktycznym przygotowaniu do uzyskania certyfikacji oraz wykształceniu kompetencji niezbędnych do obrony systemów AI. Uczestnicy nauczą się spełniać globalne wymogi zgodności oraz wykorzystywać potencjał AI do optymalizacji wykrywania zagrożeń, automatyzacji procesów i wdrażania innowacji, co realnie wzmacnia odporność organizacji na nowoczesne ataki.

Umiejętności, które zdobędziesz:

- Podnoszenie poziomu cyberbezpieczeństwa poprzez praktyczne zastosowanie koncepcji AI w strukturach organizacji.
- Skuteczne zabezpieczanie systemów AI, w tym ochrona danych, modeli oraz powiązanej infrastruktury przy użyciu zaawansowanych mechanizmów kontrolnych.
- Automatyzacja przepływów pracy i przyspieszanie reakcji na incydenty dzięki wykorzystaniu technologii AI w operacjach bezpieczeństwa.
- Wdrażanie AI zgodnie z globalnymi ramami GRC, zapewniając etykę i zgodność z przepisami w różnych branżach.
- Przeciwdziałanie zagrożeniom napędzanym przez AI, takim jak ataki adversarial, zautomatyzowane złośliwe oprogramowanie czy nadużycia generatywnej sztucznej inteligencji.
- Bezpieczna integracja rozwiązań AI z potokami DevSecOps oraz ogólną strategią bezpieczeństwa organizacji.

Role zawodowe, które skorzystają na kompetencjach SecAI+

- Analityk bezpieczeństwa (Security Analyst) – dzięki szkoleniu z zakresu AI analityk zyska umiejętność wykorzystywania nowoczesnych narzędzi AI do szybszego i bardziej precyzyjnego wykrywania zagrożeń, analizowania wzorców ataków oraz podejmowania trafnych decyzji w reakcji na incydenty. Rozwinie kompetencje w modelowaniu działań atakujących i wspieraniu procesu decyzyjnego za pomocą automatyzacji oraz innowacyjnych technik, co usprawni jego

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

codzienną pracę.

- Inżynier chmurowy (Cloud Engineer) – szkolenie pozwoli inżynierowi chmurowemu lepiej projektować i utrzymywać środowiska chmurowe z wykorzystaniem AI, co przełoży się na zwiększenie bezpieczeństwa, zgodności oraz efektywności zarządzania obciążeniami i danymi. Pozna zaawansowane mechanizmy kontrolne dla systemów AI, co umożliwi skuteczniejsze zabezpieczanie infrastruktury oraz ochronę informacji.
- Analityk SOC (SOC Analyst) – uczestnictwo w szkoleniu umożliwi analitykowi SOC wykorzystanie AI do automatyzacji wykrywania anomalii, redukcji „zmęczenia alertami" (alert fatigue) oraz usprawnienia obsługi zdarzeń bezpieczeństwa. Dzięki nabytym kompetencjom będzie mógł efektywniej zarządzać codziennymi operacjami SOC oraz wdrażać innowacyjne rozwiązania zwiększające bezpieczeństwo.
- Tester penetracyjny / konsultant ds. bezpieczeństwa (Penetration Tester / Security Consultant) – szkolenie pozwoli na rozszerzenie testów penetracyjnych o systemy AI, ocenę modeli oraz potoków danych pod kątem specyficznych podatności. Dzięki zdobytej wiedzy tester/konsultant będzie mógł formułować precyzyjne rekomendacje ryzyka dla interesariuszy oraz skuteczniej wykrywać i neutralizować zagrożenia związane z AI.
- Starszy administrator systemów (Senior Systems Administrator) – szkolenie umożliwi administratorowi wspieranie projektów AI na zarządzanej infrastrukturze poprzez wdrożenie praktyk ładu, ryzyka i zgodności. Pozna techniki ochrony systemów AI/ML, co pozwoli mu lepiej zabezpieczać zasoby oraz zapewniać zgodność z regulacjami i wymaganiami branżowymi.
- Naukowiec danych / inżynier uczenia maszynowego (Data Scientist / ML Engineer) – szkolenie zapewni wiedzę z zakresu zabezpieczania danych treningowych, potoków danych i wyników modeli AI. Pozwoli na budowę i wdrażanie rozwiązań AI z zachowaniem wysokiego poziomu bezpieczeństwa oraz efektywną współpracę z zespołami cyberbezpieczeństwa.
- Inżynier DevSecOps/CI/CD (DevSecOps/CI/CD Engineer) – szkolenie umożliwi rozwijanie praktyk DevOps o zaawansowane kontrole bezpieczeństwa dla AI oraz automatyczne testy przed wdrożeniem kodu lub modeli. Pozyskane umiejętności pozwolą na bezpieczną integrację AI z potokami DevSecOps i skuteczne zarządzanie bezpieczeństwem w cyklu życia oprogramowania.
- Specjalista ds. ryzyka i zgodności (Risk & Compliance Officer) – szkolenie umożliwi stosowanie globalnych ram, takich jak GDPR czy NIST AI RMF, do rzeczywistych przypadków użycia AI. Dzięki temu specjalista będzie wspierać organizację w spełnianiu wymogów prawnych i regulacyjnych oraz wdrażać AI w sposób etyczny i zgodny z przepisami.
- Specjalista ds. wojskowych operacji cybernetycznych (Military Cyber Operations Specialist) – szkolenie pozwoli na ochronę krytycznych systemów AI/ML oraz analizę sposobów ich wykorzystania przez przeciwników. Zdobyte kompetencje pomogą w identyfikacji zagrożeń i wdrażaniu skutecznych strategii bezpieczeństwa w środowiskach o podwyższonym ryzyku.

Każdy uczestnik autoryzowanego szkolenia CompTIA SecAI+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA SecAI+ CY0-001.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Plan szkolenia:

- Podsumowanie pojęć z zakresu AI i danych na potrzeby cyberbezpieczeństwa
  - Wyjaśnienie podstawowych koncepcji AI w kontekście cyberbezpieczeństwa
    - Podstawowe typy AI
    - Rodzaje AI
    - Generatywna AI
    - Uczenie maszynowe i uczenie statystyczne
    - Wykrywanie podejrzanej aktywności z użyciem ML
    - Ćwiczenie: porównanie typów AI
    - Transformery
    - Uczenie głębokie
    - Przetwarzanie języka naturalnego (NLP)
    - Laboratorium: poznanie środowiska laboratoryjnego SecAI+
  - Omówienie trenowania modeli AI oraz inżynierii promptów
    - Trening modelu AI
    - Uczenie nadzorowane
    - Uczenie nienadzorowane
    - Uczenie ze wzmocnieniem
    - Uczenie federacyjne
    - Techniki uczenia modeli
    - Wprowadzenie do inżynierii promptów
    - Ćwiczenie: inżynieria promptów
    - Laboratorium: inżynieria promptów i wykrywanie stronniczości
    - Role systemowe i prompty systemowe
    - Prompty użytkownika
    - Zero-shot, one-shot, multi-shot oraz szablony
    - Zabezpieczanie modelu
    - Laboratorium: projektowanie i optymalizacja promptów
  - Zabezpieczanie danych wykorzystywanych przez AI
    - Bezpieczeństwo danych w kontekście AI
    - Aspekty bezpieczeństwa danych dla AI
    - Typy danych AI
    - Laboratorium: analiza rozwiązań RAG
    - Techniki przetwarzania danych
    - Ćwiczenie: przetwarzanie danych

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Laboratorium: weryfikacja integralności danych

- Wdrażanie modelowania zagrożeń i zabezpieczanie systemów AI
  - Wykorzystanie modelowania zagrożeń dla AI
    - Wprowadzenie do modelowania zagrożeń dla AI
    - Modelowanie zagrożeń dla AI
    - Wykorzystanie zasobów dotyczących zagrożeń AI
    - Laboratorium: analiza zagrożeń z użyciem publicznych źródeł
    - Wymagania wstępne do przeprowadzenia modelowania zagrożeń AI
    - Proces modelowania zagrożeń AI
    - Ćwiczenie: analiza modelu zagrożeń
    - Ramy modelowania zagrożeń AI
    - Laboratorium: zastosowanie frameworku modelowania zagrożeń do AI
    - Laboratorium: utworzenie i wdrożenie LLM w Azure OpenAI
  - Wdrożenie mechanizmów kontroli bezpieczeństwa dla systemów AI
    - Przegląd mechanizmów kontroli bezpieczeństwa AI
    - Mechanizmy kontroli specyficzne dla modelu
    - Zabezpieczenia, ograniczniki modelu
    - Szablony promptów
    - Mechanizmy kontroli bramy oraz interfejsu
    - Kontrole i zabezpieczenia/ograniczniki na poziomie bramy
    - Ograniczenia użycia i limity
    - Testowanie mechanizmów kontroli bezpieczeństwa
    - Ćwiczenie: budowa polityki obronnej
    - Laboratorium: zastosowanie ustrukturyzowanych szablonów promptów
    - Laboratorium: zabezpieczenie LLM w Azure OpenAI
- Wdrażanie mechanizmów kontroli dostępu dla AI
  - Wdrażanie mechanizmów kontroli dostępu dla AI
    - Zasady kontroli dostępu w systemach AI
    - Modele kontroli dostępu dla AI
    - Ćwiczenie: wdrożenie wniosku o dostęp
    - Krajobraz zagrożeń dla systemów AI
    - Dostęp do modelu
    - Kontrola dostępu do systemów AI
    - Dostęp do danych i agentów
    - Dostęp do sieci i API
  - Zastosowanie mechanizmów ochrony danych na potrzeby bezpieczeństwa AI

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Przegląd mechanizmów ochrony danych dla AI
- Szyfrowanie danych AI
- Środki bezpieczeństwa danych
- Ćwiczenie: maskowanie, anonimizacja danych
- Laboratorium: sanityzacja danych do analizy AI

- Monitoring i audyt systemów AI
  - Monitoring promptów i logów
  - Monitoring wydajności i kosztów
  - Monitoring kosztów AI
  - Audyt jakości i zgodności
  - Ćwiczenie: audyt AI
  - Laboratorium: analiza logów z użyciem AI

- Rozróżnianie zagrożeń związanych z AI i stosowanie mechanizmów kompensacyjnych
  - Znaczenie bezpieczeństwa w cyklu życia AI
    - Omówienie cyklu życia AI
    - Ćwiczenie: klasyfikacja etapów cyklu życia AI dla przypadku użycia
    - Aspekty bezpieczeństwa danych
    - Aspekty bezpieczeństwa w cyklu życia AI
    - Rola człowieka w bezpieczeństwie AI
    - Aspekty etyczne w projektowaniu AI
  - Analiza ataków na systemy AI oraz stosowanie mechanizmów kompensacyjnych
    - Analiza ataków na AI
    - Ataki typu backdoor i trojan
    - Zatrucie modelu i danych
    - Inwersja modelu oraz kradzież modelu
    - Ćwiczenie: inwersja lub kradzież modelu
    - Analiza ataków na AI oraz mechanizmy kontroli
    - Stosowanie mechanizmów kompensacyjnych
    - Ćwiczenie: analiza Lessons Learned i raportowanie poincydentowe
    - Laboratorium: testowanie ataków typu prompt injection

- Wykorzystanie AI w bezpieczeństwie oraz zrozumienie potencjalnych nadużyć
  - Wykorzystanie narzędzi wspieranych przez AI w zadaniach bezpieczeństwa
    - Narzędzia AI w operacjach bezpieczeństwa
    - Ćwiczenie: analiza podatności wspomagana przez AI
    - Przypadki użycia AI: wykrywanie i analiza
    - Ćwiczenie: przypadek użycia – rozpoznawanie wzorców

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Przypadki użycia AI w bezpieczeństwie
- Przypadki użycia AI: testowanie i zarządzanie
- AI i zarządzanie incydentami

- Przegląd wektorów ataku wykorzystujących AI oraz wzmacnianych przez AI
  - AI w dezinformacji i socjotechnice
  - Ćwiczenie: identyfikacja deepfake
  - AI w rekonesansie i korelacji danych
  - AI w zautomatyzowanych atakach
  - Wektory ataku z użyciem AI
  - Laboratorium: identyfikacja wektorów ataku wspomagana przez AI
- Wykorzystanie AI do automatyzacji zadań bezpieczeństwa
  - AI w automatyzacji bezpieczeństwa i syntezie informacji
  - Laboratorium: automatyzacja zadań bezpieczeństwa z wykorzystaniem AI
  - Laboratorium: przekształcanie dokumentacji w użyteczne wnioski z AI
  - AI w przepływach pracy bezpieczeństwa
  - Automatyzacja zadań bezpieczeństwa
  - Ćwiczenie: akceptacja wspomagana przez AI
  - AI w DevSecOps
  - Laboratorium: automatyzacja przepływów pracy z użyciem AI

- Ład organizacyjny, ryzyko i zgodność (GRC) w kontekście AI
  - Klasyfikacja struktur ładu organizacyjnego dla AI
    - Ustanowienie ładu organizacyjnego AI
    - Kluczowe role w obszarze AI
    - Zasady ładu AI
    - Ćwiczenie: projektowanie struktury ładu korporacyjnego z użyciem AI
  - Definicja ryzyk związanych z AI
    - Zasady odpowiedzialnego użycia AI w środowiskach korporacyjnych
    - Identyfikacja ryzyk specyficznych dla AI
    - Operacjonalizacja etyki i standardów AI
    - Najczęstsze ryzyka związane z AI
    - Ćwiczenie: przeprowadzenie oceny ryzyka
  - Ramy regulacyjne a dynamika innowacji AI w przedsiębiorstwie
    - Wspólne motywy w regulacjach AI
    - Kluczowe ramy zgodności dla AI
    - Organizacyjne polityki dotyczące AI
    - Ćwiczenie: przygotowanie raportu zgodności

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Wpływ otoczenia regulacyjnego na ład organizacyjny
- Ćwiczenie: analiza struktury AI w organizacji

Wymagania:

Rekomendowane doświadczenie: 3–4 lata w IT, w tym co najmniej 2 lata praktycznej pracy w obszarze cyberbezpieczeństwa; zalecane certyfikaty: Security+, CySA+, PenTest+ lub równoważne.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę CompTIA. Kurs przygotowuje do egzaminu certyfikacyjnego CompTIA SecAI+, dostępnego w centrach egzaminacyjnych Pearson VUE.

Każdy uczestnik autoryzowanego szkolenia CompTIA SecAI+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA SecAI+ CY0-001.

Prowadzący:

Autoryzowany trener CompTIA

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001