kod szkolenia: SecAI+ (+exam) / PL DL 5d NIS2

CompTIA SecAI+ szkolenie autoryzowane wraz z egzaminem CY0-001

Szkolenie CompTIA SecAI+ to autoryzowany kurs koncentrujący się na zabezpieczaniu systemów sztucznej inteligencji oraz wykorzystaniu AI w nowoczesnych operacjach cyberbezpieczeństwa.

Program został zaprojektowany dla specjalistów IT i bezpieczeństwa, którzy chcą rozumieć zarówno techniczne fundamenty AI, jak i realne zagrożenia związane z modelami językowymi, uczeniem maszynowym, pipeline'ami danych oraz integracją AI z infrastrukturą organizacji.

Uczestnicy zdobywają umiejętności:

- analizowania i modelowania zagrożeń w systemach AI,
- projektowania i wdrażania technicznych zabezpieczeń,
- monitorowania i audytowania modeli AI,
- stosowania AI w operacjach SOC, DevSecOps i threat huntingu,
- zarządzania ryzykiem, zgodnością i odpowiedzialnym wykorzystaniem AI.

Szkolenie przygotowuje do egzaminu SecAI+ (CY0-001) i potwierdza kompetencje w obszarze bezpieczeństwa AI na poziomie specjalistycznym.

Rosnące wykorzystanie AI w biznesie oraz regulacje takie jak AI Act, NIS2, NIST – AI Risk Management Framework, ISO/IEC 42001 powodują, że organizacje muszą nie tylko wdrażać AI, ale również ją zabezpieczać i nadzorować.

SecAI+ odpowiada na ten problem – uczy jak łączyć techniczne zabezpieczenia, procesy bezpieczeństwa i governance w jednym spójnym modelu.

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- **CompTIA CySA+**
- **CompTIA Security+**
- **CompTIA Network+**
- **OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji**
- **CEH - Certified Ethical Hacker**
- **ECIH - Certified Incident Handler**
- **Testy penetracyjne (PenTest+/CPENT)**

Odbiorcy szkolenia

Szkolenie CompTIA SecAI+ jest przeznaczone dla specjalistów technicznych i osób odpowiedzialnych za bezpieczeństwo informacji, którzy chcą pogłębić zrozumienie zagrożeń, mechanizmów ochronnych oraz wymagań regulacyjnych związanych z systemami sztucznej inteligencji. Program koncentruje się na analizie architektury AI, modelowaniu ryzyka, interpretacji standardów oraz zrozumieniu ataków charakterystycznych dla modeli ML i LLM.
Szkolenie jest szczególnie wartościowe dla osób, które potrzebują uporządkowanej wiedzy na temat bezpieczeństwa AI w kontekście organizacyjnym i strategicznym — w tym dla zespołów bezpieczeństwa, architektów, analityków ryzyka oraz specjalistów zajmujących się governance i compliance.
W szczególności szkolenie polecane jest dla:

- Analityków SOC i zespołów cyberbezpieczeństwa
- Inżynierów bezpieczeństwa i architektów systemów
- Specjalistów DevSecOps i Cloud Security
- Osób posiadających certyfikaty Security+, CySA+, PenTest+ lub równoważne doświadczenie

- Specjalistów odpowiedzialnych za AI governance i risk management
- Organizacji wdrażających LLM, RAG, agentów AI lub rozwiązania oparte na ML

Rekomendowane doświadczenie: 3–4 lata pracy w IT oraz około 2 lata w obszarze bezpieczeństwa.

Korzyści

Ukończenie szkolenia CompTIA SecAI+ pozwala uczestnikowi zrozumieć, w jaki sposób systemy sztucznej inteligencji zmieniają krajobraz cyberbezpieczeństwa — zarówno po stronie obrony, jak i zagrożeń. Uczestnik nie tylko poznaje teoretyczne podstawy, ale uczy się również identyfikować realne techniczne i operacyjne ryzyka związane z modelami językowymi, pipeline'ami danych, integracjami API oraz agentami AI wykorzystywanymi w środowisku organizacji.
Szkolenie rozwija kompetencje projektowania i wdrażania zabezpieczeń dla systemów AI. Obejmuje to zarówno kontrolę dostępu do modeli i danych, jak i implementację mechanizmów takich jak guardrails, rate limiting, szyfrowanie danych czy monitorowanie promptów i logów. Uczestnik potrafi ocenić, gdzie w cyklu życia AI pojawiają się krytyczne punkty ryzyka oraz jakie techniczne i proceduralne środki należy zastosować, aby te ryzyka ograniczyć.
Uczestnik potrafi osadzić systemy sztucznej inteligencji w ramach polityk bezpieczeństwa organizacji, wymagań regulacyjnych oraz zasad odpowiedzialnego wykorzystania technologii. Dzięki temu jest w stanie współpracować nie tylko z zespołami technicznymi, ale również z działami compliance, audytu i zarządzania ryzykiem.
W efekcie absolwent szkolenia jest przygotowany do świadomego zabezpieczania rozwiązań opartych na AI, integrowania ich z istniejącą infrastrukturą bezpieczeństwa oraz do podejścia egzaminu CompTIA SecAI+ (CY0-001), który formalnie potwierdza zdobyte kompetencje.

Program szkolenia

1. Podstawowe koncepcje AI w cyberbezpieczeństwie
   - Typy AI stosowane w bezpieczeństwie
   - Prompt engineering i bezpieczeństwo promptów
   - Proces trenowania modeli i walidacja
   - Bezpieczeństwo danych w AI
   - Znaczenie bezpieczeństwa w całym cyklu życia AI
2. Modelowanie zagrożeń i zabezpieczanie systemów AI
   - AI threat modeling (OWASP LLM Top 10, MITRE ATLAS)
   - Identyfikacja podatności w modelach AI
   - Model controls i guardrails

- Gateway controls (rate limiting, prompt firewalls)
- Zabezpieczanie modeli on-prem i vendor-delivered
- Walidacja i testowanie zabezpieczeń

3. Kontrola dostępu i bezpieczeństwo danych w AI
   - RBAC i ABAC w kontekście AI
   - Kontrola dostępu do modeli, danych, agentów i API
   - Szyfrowanie danych (in transit, at rest, in use)
   - Maskowanie, anonimizacja, minimalizacja danych
   - Monitoring promptów i logów
   - AI cost monitoring i auditing jakości
4. Ataki na systemy AI i mechanizmy kompensacyjne
   - Prompt injection i jailbreaking
   - Data poisoning i model poisoning
   - Model inversion i model theft
   - Supply chain attacks
   - Sensitive information disclosure
   - Projektowanie compensating controls
   - Red teaming modeli AI
5. AI w operacjach bezpieczeństwa
   - AI w analizie podatności
   - AI w detection & response
   - Automatyzacja IR i DevSecOps
   - AI-assisted scripting
   - AI w threat modeling
   - AI-enhanced attack vectors (deepfake, OSINT automation, reconnaissance)
6. Governance, Risk & Compliance w AI
   - Struktury governance (AI CoE)
   - Role w organizacji (AI Risk Analyst, AI Governance Engineer)
   - Odpowiedzialne AI (human-in-the-loop, oversight)
   - Monitorowanie ryzyka i driftu modeli
   - Dokumentacja i audyt AI

Oczekiwane przygotowanie uczestnika

Szkolenie CompTIA SecAI+ zostało zaprojektowane z myślą o osobach posiadających już doświadczenie w obszarze IT oraz cyberbezpieczeństwa. Uczestnik powinien swobodnie poruszać się w zagadnieniach związanych z architekturą systemów, analizą logów, kontrolą dostępu oraz podstawowymi mechanizmami ochrony infrastruktury.
Wskazana jest praktyczna znajomość środowisk bezpieczeństwa — takich jak systemy SIEM, rozwiązania

EDR/XDR, narzędzia do analizy podatności czy mechanizmy monitorowania zdarzeń. Uczestnik nie musi być ekspertem w dziedzinie sztucznej inteligencji, jednak powinien rozumieć podstawowe koncepcje związane z AI.
Rekomendowane jest wcześniejsze doświadczenie na poziomie odpowiadającym certyfikatom takim jak Security+ lub równoważna praktyka zawodowa w obszarze bezpieczeństwa informacji.

Szkolenie obejmuje

- 5 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Autoryzowany podręcznik: CompTIA SecAI+
- Środowisko laboratoryjne zintegrowane z podręcznikiem
- Voucher egzaminacyjny CY0-001

Język

- Szkolenie: polski
- Materiały: angielski

Czas trwania

5 dni / 35 godzin

Opis egzaminu

Do egzaminu można przystąpić w autoryzowanych ośrodkach egzaminacyjnych **PearsonVue**.
Egzamin jest zawarty w cenie szkolenia.
Kod egzaminu: CY0-001
Ilość pytań – max 60 pytań (multiple-choice + performance-based)
Skala ocen: 100–900
Wynik pozytywny: od 600

Format testu: Kombinacja pytań wielokrotnego wyboru

Czas trwania: 60 minut

*** Istnieje możliwość wykupienia vouchera z opcją retake za dodatkową dopłatą 450zł, opcja ta dostępna jest do wyboru wyłącznie w momencie zgłoszenia na szkolenie.**