Szkolenie: CompTIA
CompTIA SecAI+ Prep Course

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 codzienną pracę.
- Inżynier chmurowy (Cloud Engineer) – szkolenie pozwoli inżynierowi chmurowemu lepiej projektować i utrzymywać środowiska chmurowe z wykorzystaniem AI, co przełoży się na

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

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.

Poziom trudności

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