Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

AI w Cyberbezpieczeństwie

Cele szkolenia

Szkolenie to ma na celu nie tylko przekazanie wiedzy teoretycznej, ale także praktyczne przygotowanie uczestników do wyzwań, jakie niesie ze sobą dynamicznie rozwijająca się dziedzina cyberbezpieczeństwa w kontekście sztucznej inteligencji.

Umiejętności

Uczestnicy zdobędą umiejętności w zakresie identyfikacji zagrożeń, analizy ryzyk oraz implementacji rozwiązań opartych na AI, które wspierają obronę przed cyberatakami.

Uczestnicy po ukończeniu szkolenia będą potrafili:

- Zrozumieć podstawowe pojęcia związane z cyberbezpieczeństwem i sztuczną inteligencją.
- Zidentyfikować i analizować zagrożenia związane z AI w kontekście cyberbezpieczeństwa.
- Wykorzystywać AI do identyfikacji i neutralizacji zagrożeń cybernetycznych.
- Ocenić ryzyka i proponować odpowiednie zabezpieczenia w oparciu o analizę danych.
- Rozpoznawać techniki ataków socjotechnicznych i implementować strategie ich zapobiegania.
- Zastosować zasady cyber higieny w kontekście stosowania AI.

Profil uczestników

Szkolenie skierowane jest do:

- Specjalistów ds. bezpieczeństwa IT.
- Analitków danych i programistów.
- Menedżerów IT i kierowników projektów.
- Osób odpowiedzialnych za zarządzanie ryzykiem w organizacjach.
- Wszystkich zainteresowanych tematyką AI i cyberbezpieczeństwa.

Przygotowanie uczestników

- Podstawowa wiedza z zakresu IT i bezpieczeństwa informatycznego.
- Znajomość podstawowych pojęć związanych z sztuczną inteligencją będzie dodatkowym atutem.

Szczegółowy program szkolenia

Wprowadzenie do cyberbezpieczeństwa i sztucznej inteligencji

1. **Definicja cyberbezpieczeństwa**: Zrozumienie podstawowych terminów i koncepcji związanych z ochroną danych, systemów i sieci przed zagrożeniami, w tym atakami hakerskimi i złośliwym oprogramowaniem.
2. **OWASP Top 10 dla LLM**: Przegląd najważniejszych zagrożeń związanych z modelami językowymi, takich jak manipulacja danymi wejściowymi, generowanie dezinformacji oraz ryzyko związane z przechowywaniem danych.
3. **Zastosowanie sztucznej inteligencji**: Jak AI może wspierać cyberbezpieczeństwo, identyfikując i neutralizując zagrożenia w czasie rzeczywistym.
4. **Zrozumienie ryzyk**: Analiza potencjalnych skutków cyberataków na organizacje w kontekście rosnącej popularności modeli AI.

Wykorzystanie AI w obronie przed cyberzagrożeniami

1. **Detekcja anomalii**: Jak algorytmy AI mogą analizować ruch sieciowy w poszukiwaniu nietypowych wzorców, które mogą wskazywać na atak.
2. **Automatyzacja odpowiedzi**: Wykorzystanie AI do automatyzacji procesów odpowiedzi na incydenty, co pozwala na szybsze reagowanie na zagrożenia.
3. **Predykcja zagrożeń**: Modele AI mogą przewidywać przyszłe ataki na podstawie analizy danych historycznych, co umożliwia wcześniejsze wprowadzenie środków ochronnych.
4. **Współpraca z zespołami IT**: AI jako narzędzie wspierające zespoły bezpieczeństwa w codziennych zadaniach, takich jak analiza logów czy monitorowanie systemów.

Analiza ryzyk i zabezpieczeń z wykorzystaniem AI

1. **Identyfikacja ryzyk**: Jak AI może wspierać proces identyfikacji i oceny ryzyk związanych z infrastrukturą IT.
2. **Ocena efektywności zabezpieczeń**: Wykorzystanie technik AI do oceny, jak skuteczne są obecne zabezpieczenia w organizacji i gdzie można je poprawić.
3. **Modelowanie scenariuszy ataków**: AI może symulować różne scenariusze ataków, co pozwala na lepsze przygotowanie się na potencjalne zagrożenia.
4. **Dostosowywanie zabezpieczeń**: Zastosowanie uczenia maszynowego do ciągłego dostosowywania zabezpieczeń w odpowiedzi na zmieniające się zagrożenia.

Rola AI w zapobieganiu atakom socjotechnicznym

1. **Wykrywanie phishingu**: Jak AI może analizować wiadomości e-mail i inne formy komunikacji, aby identyfikować potencjalnie złośliwe treści.
2. **Edukacja użytkowników**: Użycie AI do tworzenia spersonalizowanych programów szkoleniowych, które zwiększają świadomość pracowników na temat technik socjotechnicznych.
3. **Analiza zachowań użytkowników**: AI może monitorować zachowania pracowników, aby szybko identyfikować nietypowe aktywności, które mogą sugerować próby oszustwa.
4. **Tworzenie polityk bezpieczeństwa**: Wspieranie organizacji w opracowywaniu polityk mających na celu przeciwdziałanie atakom socjotechnicznym przy użyciu analizy danych.

AI w rękach atakujących – Jak się chronić?

1. **Zrozumienie narzędzi atakujących**: Przegląd technik i narzędzi AI, które mogą być wykorzystywane przez cyberprzestępców, takich jak generowanie fałszywych treści.
2. **Edukacja i świadomość**: Szkolenie pracowników w zakresie zagrożeń związanych z użyciem AI przez atakujących oraz wskazówki, jak rozpoznać potencjalne ataki.
3. **Wdrażanie zaawansowanych zabezpieczeń**: Wykorzystanie AI do wzmocnienia zabezpieczeń, np. poprzez analizę ryzyk w czasie rzeczywistym i wprowadzanie dynamicznych środków ochronnych.
4. **Monitorowanie i analiza**: Utworzenie systemów monitorujących, które wykorzystują AI do identyfikacji podejrzanych działań i potencjalnych naruszeń bezpieczeństwa.

Przyszłość cyberbezpieczeństwa z AI

1. **Ewolucja zagrożeń**: Jak rozwój AI może prowadzić do powstawania nowych form cyberzagrożeń oraz jak organizacje powinny się na nie przygotować.
2. **Kooperacja AI i ludzi**: Zrozumienie, jak AI może wspierać ludzkich specjalistów w dziedzinie bezpieczeństwa, a nie ich zastępować.
3. **Regulacje i etyka**: Wyzwania związane z regulacją użycia AI w cyberbezpieczeństwie oraz kwestie etyczne z tym związane.
4. **Innowacyjne technologie**: Zastosowanie nowych technologii, takich jak blockchain czy kwantowe szyfrowanie w połączeniu z AI, w celu wzmocnienia bezpieczeństwa.

Cyber higiena, a AI

1. **Podstawy cyber higieny**: Definicja i znaczenie cyber higieny w kontekście ochrony danych i systemów.
2. **Zastosowanie AI w monitorowaniu**: Jak narzędzia AI mogą wspierać organizacje w utrzymaniu odpowiednich standardów cyber higieny poprzez automatyczne skanowanie i analizę systemów.
3. **Personalizacja praktyk bezpieczeństwa**: Użycie AI do dostosowywania praktyk cyber higieny do specyficznych potrzeb i ryzyk danej organizacji.
4. **Wzmacnianie kultury bezpieczeństwa**: Jak AI może pomóc w tworzeniu kultury bezpieczeństwa w organizacjach, w tym poprzez analizę danych dotyczących zachowań użytkowników i identyfikację obszarów do poprawy.

Metoda realizacji szkolenia

Wykłady teoretyczne

Warsztaty praktyczne

Studium przypadku

Dyskusje grupowe

Liczba dni, liczba godzin szkoleniowych

1 dzień, 8 godzin szkoleniowych

Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Ścieżka rozwoju po szkoleniu

Zaawansowane kursy z zakresu AI i Machine Learning

Mechanizmy obrony przed atakami hakerskimi