Krzysztof Dyki
Prezes Zarządu
ComCERT SA

„Sztuczna Inteligencja – Zagrożenia Infiltracji i Infekcji"

Prezentacja koncentruje się na kluczowych zagrożeniach związanych z AI w kontekście cyberbezpieczeństwa. Przedstawione zostaną globalne ryzyka i zagrożenia na rynku cyberbezpieczeństwa, konflikt interesów pomiędzy producentami technologii AI a bezpieczeństwem AI, cele ataków na AI zarówno ze strony przestępców, jak i wrogich rządów oraz ostrzeżenia NIST dotyczące braku niezawodnej ochrony AI przed cyberatakami. Dodatkowo, przedstawione będą wektory ataków na AI z podziałem na sprzęt, oprogramowanie, dane i procesy, a także nowe wyzwania związane z problematyką rozumienia kodu maszynowego przez AI. Zwrócona zostanie uwaga na możliwość samo modyfikacji kodu AI oraz ograniczenia horyzontu zdarzeń i wiedzy twórców AI względem silników AI.

- Sytuacja globalna na rynku cyberbezpieczeństwa w kontekście ogólnych ryzyk i zagrożeń
- Konflikt interesów: wyścig technologiczny producentów AI a bezpieczeństwo AI
- Cele ataków na AI z podziałem na przestępców i wrogie rządy
- Ostrzeżenia NIST dotyczące braku niezawodnej ochrony AI przed cyberatakiem
- Wektory ataków na AI z podziałem na sprzęt, oprogramowanie, dane i procesy
- Nowe wyzwania związane z problematyką rozumienia kodu maszynowego przez AI
- Horyzont zdarzeń i wiedzy twórców AI względem silników AI
- Problematyka możliwości samo modyfikacji kodu AI