AI w cyberbezpieczeństwie – praktyczne wykorzystanie sztucznej inteligencji w ochronie organizacji

Zakres tematyczny

Wprowadzenie do AI w cyberbezpieczeństwie

- AI i machine learning w bezpieczeństwie IT
- Aktualne trendy i kierunki rozwoju
- AI po stronie obrony i ataku
- Zagrożenia wynikające z generative AI

Cyberzagrożenia wykorzystujące AI

- AI-driven phishing
- Deepfake i socjotechnika
- Generowanie malware przy użyciu AI
- Automatyzacja cyberataków
- Analiza współczesnych scenariuszy zagrożeń

AI w wykrywaniu zagrożeń

- Behavioral analytics
- Analiza logów i wykrywanie anomalii
- SIEM wspierany AI
- Threat Intelligence
- Predykcja zagrożeń

AI w SOC i automatyzacji bezpieczeństwa

- SOAR i automatyzacja reakcji
- AI w Security Operations Center
- Automatyczne klasyfikowanie incydentów
- Redukcja false positives
- Automatyzacja procesów bezpieczeństwa

Narzędzia AI dla cyberbezpieczeństwa

- Microsoft Security Copilot
- Darktrace
- CrowdStrike
- SentinelOne
- ChatGPT i GenAI w analizie bezpieczeństwa
- AI do analizy podatności

Imperium Szkoleniowe
Tel. 22 402 15 04, Fax: 22 258 23 62
biuro@imperiumszkoleniowe.pl

Bezpieczeństwo danych i governance AI

- → Ryzyka związane z wdrażaniem AI
- → Ochrona danych i compliance
- → AI Act i regulacje
- → Bezpieczne korzystanie z modeli AI
- → Tworzenie polityk bezpieczeństwa AI

Warsztaty praktyczne

- → Analiza incydentów bezpieczeństwa
- → Wykrywanie prób phishingu
- → Analiza logów z wykorzystaniem AI
- → Automatyzacja reakcji na incydenty
- → Scenariusze SOC

Imperium Szkoleniowe
Tel. 22 402 15 04, Fax: 22 258 23 62
biuro@imperiumszkoleniowe.pl