CYBER|NTELLIGENCE
.Institute

Think visionary.
Act together.
Secure tomorrow.

Sichere KI? Zwischen Prompt Hacks, Datenvergiftung und Manipulationsangriffe: Deep Dive in KI- und LLM-Cybersecurity

Inhalt der Schulung:
Diese Schulung im deep dive Format von 2 Stunden bietet einen Einblick in die Cybersecurity-Implikationen von generativen KI-Anwendungen. Generative KI, vor allem LLM-Chatbots, werden in immer mehr Arbeitsprozesse integriert; doch sie bergen auch Sicherheitsrisiken. Dieser Kurs vermittelt praxisnah einen Überblick über die speziellen Cybersecurity-Bedrohungen von KI-Chatbots und LLM-Systemen (z.B. Datenlecks, Manipulationsangriffe, Prompt Hacking, Data Poisoning oder Model Evasion). Darüber hinaus vermittelt diese Schulung einen Überblick über rechtlichen Vorgaben und Sicherheitsnormen und wie Unternehmen sich mit Software-Lösungen, Red Teaming, Monitoring und Incident Response gegen Angriffe wappnen können.

Zielgruppen
- Führungskräfte
- Mitarbeiter und Fachkräfte im Bereich KI, Cybersecurity und IT
- CISOs und Informationssicherheitsbeauftragte

Trainer
Dr. Christopher Nehring, cyberintelligence.institute (CII), Frankfurt am Main

Schulungsablauf

Einführung

- Generative KI vs. „systemische KI“
- LLM und ihre Integration
- Open Source oder closed models?
- DeepSeek vs ChatGPT vs Mistral
- Vergleichsparameter & Benchmarking

Modul 1: Angriffsvektoren für LLMs und Chatbots

- Übung: LLM-Angriff & Prompt Hacking
- Überblick über verschiedene Angriffsvektoren

Modul 2: LLM-Cybersecurity

- Modell Scanner
- LLM Proxy & Prompt Analyzer
- Incident Response für LLM-Angriffe
- Protective Shields
- Weitere Sicherheitsmaßnahmen

Modul 3: Recht, Normen, Standards

- KI-Ethik, Bias und Explainability
- Gesetze und Regelungen (AI Act, NIS2, CRA, DSGVO)
- Sicherheitsnormen (ISO 27001, ISO 42001, NIST AI RMF)

Der Kurs wird nur remote/online angeboten.

Teilnehmer: 20 max.

Dauer: Dieses Kursangebot ist speziell als deep dive von 2 Stunden (nur online) designed; upgrade zu einem Halbtages-Workshop (4 Stunden, ggf. auch in Präsenz) nach individueller Absprache möglich!

Kontakt

cyberintelligence.institute

MesseTurm
Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute
+49 69 505034602