

Mastering Large Language Models

Sicherheit in der Entwicklung und Nutzung großer Sprachmodelle – Intensivkurs

Erhalten Sie ein umfassendes Verständnis von großen Sprachmodellen (LLMs) und lernen Sie, gängige Sicherheitsrisiken zu erkennen und zu vermeiden. Unser Intensivkurs vermittelt Ihnen Wissen über die Entwicklung und die kritischen Sicherheitsherausforderungen von LLMs.

Durch zahlreiche praktische Übungen erlangen Sie Fähigkeiten in der Erstellung von LLM-Anwendungen, fortgeschrittene Techniken wie Prompt Engineering und RAG sowie in der Analyse von Sicherheitsrisiken gemäß den OWASP Top 10 LLM-Risiken. Entwickeln Sie Strategien gegen Bedrohungen wie Prompt Injection und Model Theft und integrieren Sie Sicherheitsanalysen in Ihre Praxis.

Dieses Seminar bietet Ihnen:

- Fundierte Kenntnisse über LLM Grundlagen und deren Entwicklung
- Praktische Erfahrungen in der Implementierung und Anpassung von LLM Anwendungen
- Intensive Betreuung bei Programmieraufgaben
- Verwendung von OSS Software und freien Modellen

- Systematische Anwendung auf industrie-relevante Praktiken und Prozesse wie DevOps und MLOps

Nach dem Seminar können Sie:

- Sicherheitsrisiken in LLM-basierten Anwendungen analysieren, bewerten und vermeiden
- Strategien gegen Bedrohungen wie Prompt Injection entwickeln
- LLM-Modelle effizient bewerten und optimieren

Ihr Nutzen

- Nach dem Seminar können Sie die grundlegenden Konzepte und Architekturen von/für LLMs erklären.
- Sie verstehen die Prinzipien und praktischen Grundlagen für das Training von Modellen, Fine-tuning und den Betrieb von Open Source LLMs.

Informationen im Überblick



– Datenwissenschaftler*innen, Softwareentwickler*innen und Sicherheitsexpert*innen mit praktischem Grundwissen im maschinellen Lernen

Voraussetzungen:

- Programmiererfahrung mit Python
- Grundlegende Kenntnisse im Maschinellen Lernen



3,5 Tage



Inhouse, nach Absprache



Berlin

Referenten



Dorian Knoblauch,
Fraunhofer FOKUS



Paul Ranly,
Fraunhofer SIT



Lukas Graner,
Fraunhofer SIT

Weitere Infos und Anmeldung unter:
www.fokus-akademie.de/de/kurse/llm-schulung

