AI340 Effiziente Sicherheit und Compliance mit KI-basierten RAG-Systemen

Kurzbeschreibung:

Im Workshop **AI340 Effiziente Sicherheit und Compliance mit KI-basierten RAG-Systemen** lernen Sie, wie Sie ein modernes, auf Retrieval-Augmented Generation (RAG) basierendes System entwickeln, das strukturiertes Wissen aus spezialisierten Datenquellen intelligent nutzt, um komplexe Fragen zu beantworten und Entscheidungsprozesse zu unterstützen. RAG-gestützte Systeme lassen sich in zahlreichen Domänen sinnvoll einsetzen:

- Informationssicherheit
- Rechtswesen & Compliance
- Gesundheitswesen
- Industrie 4.0 & Qualitätsmanagement
- Unternehmensinterne Richtlinien & Betriebsvereinbarungen

Der Kurs gliedert sich in zwei zentrale Bereiche:

Aufbau eines generischen, KI-basierten RAG-Systems: Im ersten Teil der Schulung erhalten Sie eine fundierte Einführung in die Architektur moderner RAG-Systeme (Retrieval-Augmented Generation) und lernen praxisnah, wie sich Schlüsselkomponenten wie Large Language Models, LangChain und Vektordatenbanken zu einem leistungsfähigen Frage-Antwort-System kombinieren lassen. Sie bauen ein solches System lokal eigenständig auf und lernen, es flexibel an unterschiedliche Datenquellen anzupassen. Dabei vertiefen Sie, wie RAG-Systeme Informationen aus Vektordatenbanken gezielt abrufen und mit großen Sprachmodellen zu konsistenten und kontextrelevanten Antworten verknüpfen.

Domänenspezifische Anwendungsszenarien von RAG-Systemen: Im zweiten Teil des Workshops stehen konkrete Anwendungsfelder im Fokus, in denen Retrieval-Augmented Generation (RAG) signifikant zur Effizienzsteigerung, Risikominimierung und regelkonformen Entscheidungsfindung beitragen kann. Am Beispiel der Informationssicherheit und ISMS zeigen wir, wie KI-basierte Systeme dabei unterstützen, komplexe Regelwerke wie ISO 27001, DORA, NIS2 oder CRA verständlich aufzubereiten und bedarfsgerecht bereitzustellen.

Nach Abschluss des Kurses können Sie einen maßgeschneiderten Chatbot entwickeln und bereitstellen, der die Einhaltung gesetzlicher Vorgaben sicherstellt und Ihre Prozesse effizienter gestaltet.

Zielgruppe:

Der Kurs richtet sich an jene, die KI-basierte Assistenzsysteme zur Unterstützung komplexer Regelwerke implementieren werden.

- IT-Sicherheitsverantwortliche
- IT-Sicherheitsexperten
- (KI-)Entwickler
- Software-Architekten

- Fachverantwortliche (mit technischem Hintergrund)

Voraussetzungen:

Um den Inhalten und dem Lerntempo des Kurses **AI340 Effiziente Sicherheit und Compliance mit KI-basierten RAG-Systemen** gut folgen zu können, empfehlen wir folgende Vorkenntnisse:

- AI020 AI & Data Science Practitioner (alternativ Grundkenntnisse in Python und ein Grundverständnis von LLMs)
- Grundkenntnisse in IT-Sicherheit

Sonstiges:

Dauer: 2 Tage

Preis: 1850 Euro plus Mwst.

Ziele:

Die Schulung **AI340 Effiziente Sicherheit und Compliance mit KI-basierten RAG-Systemen** vermittelt, wie ein intelligenter Chatbot entwickelt wird, der komplexe und spezialisierte Datenquellen automatisiert überprüft, Mitarbeiter in Echtzeit unterstützt und nahtlos in Managementsysteme integriert werden kann. Die Teilnehmer lernen, moderne KI-Technologien wie OpenAI, LlamaIndex und Vector-Datenbanken zu nutzen, um Standards, Gesetze und andere umfangreiche Quellenwerke effizient in einer interaktiven Wissensdatenbank abzubilden. Anwendungsbeispiele aus dem Bereich Informationssicherheit dienen exemplarisch der Veranschaulichung, welche Aufgaben ein RAG-System übernehmen kann:

- Beratung bei Audits und der Vorbereitung auf Zertifizierungen
- Assistenz bei der Erstellung, Pflege und Einhaltung von Sicherheitsrichtlinien und Risikoanalysen
- Interaktive Schulung und Unterstützung neuer Mitarbeitender im Bereich ISMS

RAG-gestützte Systeme lassen sich in zahlreichen weiteren Domänen sinnvoll einsetzen:

- *Rechtswesen & Compliance*
  - Interne Compliance-Assistenten mit Zugriff auf jurische Leitfäden, Verfahrensvorgaben und interne Policies
  - Schnellbeantwortung häufig wiederkehrender rechtlicher Fragestellungen
  - Unterstützung bei der Vertragsprüfung und Risikoeinschätzung rechtlicher Dokumente

- *Gesundheitswesen*
  - Rechtssichere Entscheidungsunterstützung für medizinisches Personal im klinischen Alltag
  - Direkter Zugriff auf medizinische Leitlinien, Hygienevorgaben oder Kodierstandards
  - Unterstützung von Datenschutzbeauftragten bei der Umsetzung regulatorischer Anforderungen (z. B. DSGVO, KHZG)

- *Industrie 4.0 & Qualitätsmanagement*
  - Assistenzsysteme für Produktions- und Qualitätssicherungsteams in Echtzeit
  - Zugriff auf technische Dokumentationen, Audit-Checklisten oder Verfahrensanweisungen
  - Dokumentation und Validierung von Normkonformität gemäß ISO 9001, ISO 13485 oder vergleichbarer Standards

- *Unternehmensinterne Richtlinien & Betriebsvereinbarungen*
    - Einheitliche Auslegung und Durchsetzung interner Regelwerke und Betriebsvereinbarungen
    - Automatisierte Beantwortung häufig gestellter Fragen zu Themen wie Homeoffice, IT-Nutzung, Reiserichtlinien
    - Unterstützung der Personalabteilung bei regelkonformer Kommunikation und Mitarbeiterberatung

Inhalte/Agenda:

- ♦ **Einführung und Grundlagen**
  - ♦ ◊ Begriffsdefinitionen und Konzepte
- ♦ ◊
- ♦ **Aufbau eines RAG-Systems**
  - ♦ ◊ Architektur und Bestandteile
    ◊ Vectordatenbanken und Embeddings
    ◊ Einführung in LangChain
    ◊ Prompt Engineering und Templates
    ◊ Alternative Frameworks (z.B. LlamaIndex)
- ♦ ◊
- ♦ **Implementierung am Beispiel ISMS**
  - ♦ ◊ User Intents und Interaktionsdesign
    ◊ Integration von Sicherheitsrichtlinien und Regularien (z.B. NIS2, CRA, DORA)
    ◊ Integration eines Chatbots im ISMS
- ♦ ◊
- ♦ **Praxisübung: Erstellung eines Prototyps**
  - ♦ ◊ Chatbot-Anpassung für spezifische ISMS-Prozesse
    ◊ Erweiterte Funktionen: Threat Modeling und Risikoanalysen
- ♦ ◊
- ♦ **Ergänzende Technologien**
  - ♦ ◊ KAG – Knowledge-Augmented Generation
    ◊ Agenten-Architekturen (z. B. LangGraph, CrewAI)
    ◊ Multimodale Systeme
    ◊ Wissensvalidierung & Trustworthiness
    ◊ Domänenspezifisches Fine-Tuning und Embedding-Optimierung
- ♦ ◊
- ♦ **Abschlussdiskussion: Herausforderungen und Lösungsansätze**
  - ♦