# *AI340 KI-gestützte Risikominimierung und Effizienzsteigerung im ISMS*

**Kurzbeschreibung:**

Im Workshop **AI340 KI-gestützte Risikominimierung und Effizienzsteigerung im ISMS** lernen Sie, wie Sie einen intelligenten Chatbot entwickeln, der die Einhaltung von Sicherheitsrichtlinien in Ihrem Unternehmen unterstützt und nahtlos in ein Informationssicherheitsmanagementsystem (ISMS) integriert werden kann. Der Fokus liegt auf der Umsetzung einer KI-gestützten Lösung, die Mitarbeiter in Echtzeit berät und Sicherheitsstandards automatisiert überprüft. Sie erhalten eine Einführung in moderne KI-Technologien wie OpenAI und LlamaIndex und erfahren, wie Sie Vector-Datenbanken nutzen, um Sicherheitsrichtlinien effizient zu speichern und abzufragen.

Ein zentraler Bestandteil des Kurses ist die Integration von Sicherheitsrichtlinien in eine Wissensdatenbank, die aktuelle Standards und Regularien wie NIS2, CRA oder DORA abdeckt. Sie lernen, wie Sie User Intents konfigurieren, um gezielte Interaktionen zu ermöglichen, und wie Sie Ihren Chatbot auf die Anforderungen eines ISMS zuschneiden können. Praxisnahe Anwendungsfälle, wie die automatisierte Unterstützung bei Threat Modeling und Risikoanalysen, verdeutlichen die vielseitigen Einsatzmöglichkeiten solcher Chatbots.

Zusätzlich vermittelt der Kurs Best Practices zur Sicherstellung von Datenschutz und Compliance bei der Nutzung der entwickelten Lösungen. Er richtet sich an IT-Sicherheitsverantwortliche, ISMS-Beauftragte, Software-Architekten, KI-Entwickler und all jene, die KI-Lösungen zur Unterstützung von Sicherheitsrichtlinien und ISMS-Prozessen implementieren möchten. Grundlegende Kenntnisse in IT-Sicherheit, Programmierung und KI-Technologien sind hilfreich, aber nicht zwingend erforderlich. Nach Abschluss des Kurses können Sie einen maßgeschneiderten Chatbot entwickeln und bereitstellen, der die Einhaltung gesetzlicher Vorgaben sicherstellt, Prozesse effizienter gestaltet und Ihre ISMS-Anforderungen optimal unterstützt.

**Zielgruppe:**

- Entwickler
- IT-Fachleute
- Compliance-Beauftragte

**Voraussetzungen:**

Um den Inhalten und dem Lerntempo des Kurses **AI340 KI-gestützte Risikominimierung und Effizienzsteigerung im ISMS** gut folgen zu können, empfehlen wir folgende Vorkenntnisse:

- AI020 AI & Data Science Practitioner (alternativ Grundkenntnisse in Python)
- AI030 AI & Data Science Expert (alternativ Grundkenntnisse in Empfehlungssystemen sowie Prompt Engineering)
- Grundkenntnisse im Bereich Datenschutz und Compliance sind von Vorteil

**Sonstiges:**

**Dauer:** 3 Tage

**Preis:** 2150 Euro plus Mwst.

**Ziele:**

Die Schulung **AI340 KI-gestützte Risikominimierung und Effizienzsteigerung im ISMS** vermittelt, wie ein intelligenter Chatbot entwickelt wird, der Sicherheitsrichtlinien automatisiert überprüft, Mitarbeiter in Echtzeit unterstützt und nahtlos in ein ISMS integriert wird. Die Teilnehmer lernen, moderne KI-Technologien wie OpenAI, LlamaIndex und Vector-Datenbanken zu nutzen, um Standards und Regularien wie NIS2, CRA und DORA effizient in einer Wissensdatenbank abzubilden.

Praxisorientierte Anwendungsfälle, etwa für Threat Modeling und Risikoanalysen, verdeutlichen die vielseitigen Einsatzmöglichkeiten. Zusätzlich wird gezeigt, wie Datenschutz und Compliance durch Best Practices sichergestellt werden können. Das Training richtet sich an IT-Sicherheitsverantwortliche, ISMS-Beauftragte und Entwickler, die KI-Lösungen für Sicherheitsprozesse umsetzen möchten. Nach Abschluss sind die Teilnehmer in der Lage, eine individuelle KI-Lösung bereitzustellen, die gesetzliche Vorgaben erfüllt, Prozesse automatisiert und ISMS-Anforderungen optimal unterstützt.

**Inhalte/Agenda:**

- ♦ **Modul 1: Einführung und Grundlagen**
- ♦ ◊ Begrüßung und Vorstellung der Teilnehmer
  ◊ Einführung in KI-gestützte Chatbots für Sicherheitsrichtlinien
  ◊ Überblick über ISMS: Anforderungen und Integration eines Chatbots
  ◊ Einführung in OpenAI und LlamaIndex
  ◊ Aufbau und Nutzung von Vector-Datenbanken für Sicherheitsrichtlinien
- ♦ ◊
- ♦ **Modul 2: Praxis und Implementierung**
- ♦ ◊ Reflexion des vorhergehenden Tages
  ◊ User Intents und Interaktionsdesign
  ◊ Integration von Sicherheitsrichtlinien und Regularien (z. B. NIS2, CRA, DORA)
  ◊ Praxisübung: Erstellung eines einfachen Prototyps
  ◊ Best Practices: Datenschutz und Compliance
- ♦ ◊
- ♦ **Modul 3: Erweiterte Funktionen und Abschluss**
- ♦ ◊ Reflexion des vorhergehenden Tages
  ◊ Erweiterte Funktionen: Threat Modeling und Risikoanalysen
  ◊ Praxisübung: Chatbot-Anpassung für spezifische ISMS-Prozesse
  ◊ Diskussion: Herausforderungen und Lösungsansätze
  ◊ Abschluss: Präsentation der Ergebnisse und Zertifikatsvergabe
- ♦ ◊