AI050 KI Security Specialist

Kurzbeschreibung:

Teilnehmende erhalten eine praxisnahe Einführung in den Einsatz von KI in der Cybersicherheit. Vermittelt werden aktuelle Angriffsmethoden, Bedrohungen durch KI-gestützte Systeme und Möglichkeiten zur Abwehr. Behandelt werden Praxisbeispiele realer Cyberangriffe, KI-basierte Schutzmechanismen in Hardware und Software sowie Kriterien zur Entwicklung vertrauenswürdiger Anwendungen.

Zielgruppe:

- CISOs
- Fachexperten
- IT-Fachkräfte
- Entwickler

Voraussetzungen:

- AI020 KI-Implementierung Basics oder vergleichbare Vorkenntnisse

Sonstiges:

Dauer: 5 Tage

Preis: 3950 Euro plus Mwst.

Ziele:

- Begriffe der Cyber Security kennenlernen und verstehen
- Die Rolle von KI bei Cyberangriffen kennenlernen und verstehen
- Theoretisch mögliche Cyberangriffsmethoden mit KI kennenlernen
- Praxisbeispiele für Cyberangriffe mit KI kennenlernen
- Risiken von KI-unterstützten Cyberangriffen verstehen und nachvollziehen
- Die Chancen von KI zur Abwehr von Cyberangriffen kennenlernen und verstehen
- Theoretisch mögliche Abwehrmethoden mit KI kennenlernen
- Praxisbeispiele für Abwehr mit KI kennenlernen
- Strategische Umsetzungsvorschläge kennenlernen und nachvollziehen
- Angriffsmuster auf technischer Ebene erkennen
- KI-Sicherheitslösungen gezielt auswählen, entwickeln und angemessen dokumentieren
- Risikoanalysen für KI-Anwendungen durchführen können
- KPI für KI-Anwendungen kennenlernen und anwenden können
- Kriterien für vertrauenswürdige KI-Anwendungen vertieft verstehen und bei Eigenentwicklungen zielgerichtet anwenden können

Darüber hinaus bildet der Kurs eine gute Basis für weitere Aufbaukurse, z.B.:
AI100 KI-Beauftragter

AI135 KI-Auditor
AI060 KI GRC Specialist

Inhalte/Agenda:

- ♦ **Modul 1: KI als Risiko für die Cybersicherheit**
  - ♦ ◊ Begriffe im Themengebiet der Cyberangriffe
  - ◊ Angriffsmethoden mit IT-Unterstützung
  - ◊ Aktuelle Bedrohungslage durch Cyberangriffe
  - ◊ Cyberangriffsmethoden mit KI-Unterstützung
  - ◊ Praxisbeispiele für erfolgreiche Cyberangriffe mit KI
  - ◊ Technische Umsetzungen von Angriffssystemen mit KI
  - ◊ Übersicht der Entwicklung von Bedrohungen durch KI
  - ◊ Risiken für die Cybersicherheit durch KI-Einsatz
  - ◊ Diskussion und Q&A
- ♦ ◊
- ♦ **Modul 2: KI als Chance für die Cybersicherheit**
  - ♦ ◊ Abwehrmethoden mit KI-Unterstützung
  - ◊ Praxisbeispiele für abgewendete Cyberangriffe durch KI
  - ◊ Technische Umsetzungen von Abwehrsystemen mit KI
  - ◊ Übersicht der Entwicklung von Abwehrmöglichkeiten durch KI
  - ◊ Chancen für die Cybersicherheit durch KI-Einsatz
  - ◊ Diskussion und Q&A
- ♦ ◊
- ♦ **Modul 3: Technische Angriffserkennung mit KI**
  - ♦ ◊ Vorstellung von bekannten Cyberangriffsmustern
  - ◊ Deep Dive in die technischen Abläufe
  - ◊ Methoden zur effizienten Gestaltung von KI-Trainigsdaten
  - ◊ Laborbedingungen vs. Realität
  - ◊ Praxis-Use-Case anhand von Fallbeispiel
  - ◊ Vorstellung Security Intelligence Modeling
  - ◊ Dokumentation von KI-Sicherheitslösungen in der Praxis
  - ◊ Abschließende Diskussion und Q&A
- ♦ ◊
- ♦ **Modul 4: Gestaltung vertrauenswürdiger KI**
  - ♦ ◊ Grundlegende Konzepte und Methodik des Prüfkataloges
  - ◊ KI-Steckbrief
  - ◊ Dimension: Fairness
  - ◊ Dimension: Autonomie und Kontrolle
  - ◊ Dimension: Transparenz
  - ◊ Dimension: Verlässlichkeit
  - ◊ Dimension: Sicherheit
  - ◊ Dimension: Datenschutz
  - ◊ Dimensionsübergreifende Beurteilung der Vertrauenswürdigkeit
  - ◊ Abschließende Diskussion und Q&A
- ♦ ◊
- ♦ **Zertifikatsprüfung**
  - ♦