AI050 AI Cyber Security Specialist

Kurzbeschreibung:

Der Zertifikatslehrgang **AI050 AI Cyber Security Specialist** bildet Sie zu einem KI-Experten für Cybersicherheit aus.

Erfahren Sie, wie KI bereits bei Cyberangriffen eingesetzt wird und welche Bedrohungen sich daraus ergeben können. Sie erhalten einen aktuellen Überblick über Angriffsmethoden und technische Systeme, die mit KI-Unterstützung möglich sind. Darüber hinaus werden Ihnen konkrete Praxisbespiele erfolgreicher Cyberangriffe vorgestellt, bei denen KI zum Einsatz kam. Der Lehrgang bildet ein Verständnis für die Entwicklungen in der Gegenwart und der absehbaren Zukunft, durch welches die Teilnehmer überblicken und nachvollziehen können, welche Risiken heute und morgen durch KI für die Cybersicherheit bestehen.

Erfahren Sie ebenso, wie KI umgekehrt Ihnen dabei helfen kann, Cyberangriffe abzuwehren und vorzubeugen: Von strategischen Überlegungen über Vorschläge für die Umsetzung in Unternehmen bis hin zu konkreten Einsatzszenarien. Lernen Sie Techniken kennen, die gezielt zum Schutz von IT-Systemen entwickelt und verwendet werden. Neben Hardware-Lösungen stehen dabei auch Software-Lösungen im Fokus. Zusätzlich werden aktuelle und zukünftig mögliche Entwicklungen von Sicherheitslösungen mit KI-Einsatz vorgestellt. Nach Abschluss des Kurses haben Sie das nötige Wissen, um Entscheidungen für Ihre individuellen Sicherheitsbedarfe treffen zu können.

Sie erhalten einen detaillierten Einblick in den technischen Ablauf von Cyberangriffen mit und ohne KI-Einsatz und können so nachvollzeihen, welche Maßnahmen mit Hilfe von KI möglich sind, um sich dagegen zu schützen. Für ein strukturiertes Vorgehen bei der Umsetzung von Sicherheitslösungen gegen diese Art von Angriffen wird den Teilnehmern eine Anleitung gegeben, mit der sie in der Praxis gezielt arbeiten können. Dadurch sollen zum einen Grundlagen für die Entwicklung solcher Systeme vermittelt und zum anderen Möglichkeiten der Dokumentation aufgezeigt werden.

Lernen Sie, wie Sie anhand eines Prüfkataloges KI-Anwendungen vertrauenswürdig entwickeln und überprüfen können. Damit ist Ihnen auch die Entwicklung von KI-Anwendungen möglich, die diese Kriterien beachten und somit den Ansprüchen an die Vertrauenswürdigkeit gerecht werden. Das Hauptaugenmerk liegt auf KI-Anwendungen, die auf Maschinellem Lernen beruhen.

Zielgruppe:

- CISOs
- Fachexperten
- IT-Fachkräfte
- Entwickler

Voraussetzungen:

- AI020 AI & Data Science Practitioner

oder mindestens

- AI200 Einführung in Python für Data Science und KI (alternativ Grundkenntnisse in Python)
- AI220 Einführung in Machine Learning

- AI225 Einführung in Deep Learning und KI

Sonstiges:

Dauer: 9 Tage

Preis: 3650 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

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**
  - ◊