AI510 Technische Angriffserkennung mit KI

Kurzbeschreibung:

Erfahren Sie, wie Muster von Angriffen durch KI erkannt und abgewehrt werden können. Dabei werden Ihnen zunächst die Schritte der KI zur Mustererkennung anhand von Beispielen erläutert. Mit diesem tiefen technischen Verständnis können praktisch mögliche Angriffe identifiziert werden und Sie werden befähigt zur Auswahl bzw. Gestaltung von eigenen KI-Sicherheitslösungen in Ihrem Unternehmen. Außerdem wird Ihnen ein Modell zum Erstellen von Sicherheitskonzepten vermittelt, das Sie für Ihre Bedarfe anwenden können.

Im Workshop **AI510 Technische Angriffserkennung mit KI** erhalten die Teilnehmer 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.

Zielgruppe:

- CISOs
- Fachexperten
- IT-Fachkräfte

Voraussetzungen:

Vorkenntnisse im Themengebiet der Cyberangriffe sind hilfreich. Wir empfehlen vorab den Besuch folgender Workshops:

- AI500 KI als Risiko für die Cybersicherheit
- AI225 Einführung in Deep Learning und KI

Sonstiges:

Dauer: 2 Tage

Preis: 900 Euro plus Mwst.

Ziele:

- Angriffsmuster auf technischer Ebene erkennen
- KI-Sicherheitslösungen gezielt auswählen
- KI-Sicherheitslösungen gezielt entwickeln
- KI-Sicherheitslösungen angemessen dokumentieren

Inhalte/Agenda:

- ♦ 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
- ♦