AI035-WS Wie KI die ISO 27001-Compliance automatisiert und Entwickler produktiver macht

Kurzbeschreibung:

In der modernen Softwareentwicklung stehen Entwickler vor der Herausforderung, umfangreiche Sicherheitsrichtlinien, wie die **ISO 27001**, zu implementieren und gleichzeitig effiziente Entwicklungsprozesse beizubehalten. In diesem Web-Seminar werden innovative Lösungen vorgestellt, die Large Language Models (LLMs) nutzen, um **Entwickler** bei der Einhaltung dieser **Richtlinien** zu unterstützen, indem sie repetitive und zeitaufwändige Aufgaben automatisiert.

Wir zeigen auf, wie durch den Einsatz von LLMs Dev-Tickets (z.B. in Jira) im Hintergrund gescannt werden können, um automatisiert ein Threat Modelling durchzuführen und eine Checkliste inklusive Verweise auf die relevanten Richtlinien zu generieren. Diese Checkliste wird dann dem Ticket angehängt, um Entwickler bei der Arbeit zu unterstützen.

Zielgruppe:

- Entscheider
- Anwender
- Softwareentwickler / DevOps
- IT-Fachkräfte
- GRC-Verantwortliche

Voraussetzungen:

Interesse an Künstlicher Intelligenz (KI)

Sonstiges:

Dauer: 1 Tage

Preis: 0 Euro plus Mwst.

Ziele:

Durch die Automatisierung von Sicherheitsüberprüfungen und die Unterstützung der Entwickler bei der Einhaltung von ISO 27001 Richtlinien mittels LLMs kann die Effizienz und Sicherheit in der Softwareentwicklung erheblich gesteigert werden. Sie erhalten praktische Einblicke und Anleitungen zur Implementierung dieser innovativen Lösung.

Nutzen für die Teilnehmer:

- Einsparung von Zeit und Ressourcen durch die Automatisierung von Sicherheitsprüfungen und Dokumentationen
- Verbesserung der Einhaltung von ISO 27001 Richtlinien
- Erhöhung der Effizienz und Genauigkeit im Entwicklungsprozess
- Tieferes Verständnis für die Integration von LLMs in bestehende Entwicklungs- und Sicherheitsprozesse

Inhalte/Agenda:

- **Live Demos verschiedener Use-Cases:**

- ♦ **Scanning und Threat Modelling:**
  - ♦ ◊ Erläuterung der Methode, wie LLMs Inhalte von Dev-Tickets analysieren
    ◊ Automatisierte Erkennung von Sicherheitsanforderungen, wie Vertraulichkeit, Integrität und Verfügbarkeit
    ◊ Generierung eines detaillierten Threat Modelling Berichts
  - ♦ ◊
- ♦ **Checklisten-Generierung:**
  - ♦ ◊ Erstellung einer dynamischen Checkliste basierend auf den Inhalten des Tickets
    ◊ Verweise auf die relevanten ISO 27001 Richtlinien
    ◊ Integration der Checkliste direkt in das Dev-Ticket
  - ♦ ◊
- ♦ **Kategorisierung nach AI Act:**
  - ♦ ◊ Automatisierte Kategorisierung von AI-Features gemäß den Vorgaben des AI Acts
    ◊ Einbindung in das Checklisten- und Threat Modelling System
  - ♦ ◊
- ♦ **Peer Review Unterstützung:**
  - ♦ ◊ Automatische Überprüfung, ob die Checkliste im Peer Review erfüllt wurde
    ◊ Vorbefüllung eines Formulars zur Dokumentation der Überprüfung
    ◊ Ergänzung der Dokumentation durch den Reviewer
  - ♦ ◊
- ♦ **Integration in GRC-Tools:**
  - ♦ ◊ Darstellung, wie die generierten Daten und Berichte in Governance, Risk, and Compliance (GRC) Tools integriert werden können
    ◊ Vorteile der automatisierten Dokumentation und Nachverfolgbarkeit
  - ♦ ◊

Q&A Session