Advanced Artificial Intelligence Security Training – Attacks and Defenses

Trainings-ID: AAIS-Mod2

Zum Seminar →

Das nehmen Sie mit

Die fortschreitende Integration von Künstlicher Intelligenz (KI) in Geschäftsprozesse stellt Unternehmen vor neue Chancen und Herausforderungen. Unternehmen müssen sich nicht nur mit herkömmlichen Cyberbedrohungen auseinandersetzen, sondern auch mit spezifischen Risiken, die aus der Nutzung oder Entwicklung von KI-Technologien resultieren. Dazu gehören Manipulationen durch Injection Angriffe, Datenlecks, Bias in Entscheidungsprozessen und die potenzielle Verletzung von Datenschutz- und Urheberrechts-Aspekten. Eine umfassende Sicherheitsstrategie, die sowohl technische als auch organisatorische Maßnahmen umfasst, ist daher unerlässlich.
Ziel des Trainings ist es, fundiertes Wissen über die Grundfunktion und die Sicherheitsaspekte von KI-Systemen zu vermitteln. Dabei werden Managementsystem-Aspekte, Bedrohungsszenarien, Sicherheitsarchitekturen und Schutzmaßnahmen detailliert trachtet. Die Teilnehmer lernen, wie sie Risiken erkennen, bewerten und mit adäquaten Maßnahmen begegnen können. Praxisnahe Fallstudien und interaktive Workshops ermöglichen es den Teilnehmern, das erworbene Wissen direkt anzuwenden und maßgeschneiderte Sicherheitsstrategien für ihre Organisation zu entwickeln. Somit wird ein ganzheitliches Verständnis für die sichere Implementierung und den Betrieb von KI-Systemen gewährleistet.

Das Training führt die Teilnehmer*innen schnell, kompakt und umfassend in das Thema Künstliche Intelligenz sowie damit zusammenhängende Risiken und notwendigen Sicherheitsmaßnahmen ein.
Aufbauend auf dem separat verfügbaren Basismodul („Advanced Artificiail Intelloigence Security Basics“) werden in diesem Training die Inhalte der ISO/IEC 42001:2024, welche die Zertifizierung von KI-Systemen ermöglicht, sowie damit zusammenhängende

Sicherheitsmaßnahmen dargestellt, um den Teilnehmern einen ganzheitlichen Überblick zum Thema Management von KI-Systemen zu vermitteln.
Einen weiteren Teil des Trainings stellt eine Einführung in vorsätzliche Angriffe und die Verteidigung gegen unterschiedliche Schwachstellen von KI-Systemen (wie Prompt Injection, Training Data Poisoning, etc.) dar, welche sowohl bei der Entwicklung als auch bei der Verwendung von KI-Systemen eine entscheidende Sicherheitsrolle spielen. Zudem erhalten die Teilnehmer eine Übersicht über die wichtigsten Regelungen der EU-Verordnung zu Künstlicher Intelligenz, welche einen ersten risikobasierten Ansatz für KI-Systeme und deren Überwachung bildet.
Im (separat verfügbaren) anwendungsorientierten Teil des Trainings wird ein klares Verständnis für neurale Netze aufgebaut, um weiters konkrete Anwendungen in den Bereichen Computer Vision und Natural Language Processing nachvollziehen zu können. Zudem werden Methoden wie moderne Reinforcement Learning Techniken für die Entwicklung von Agents betrachtet.
Im Zuge des Trainings werden explizit keine Softwareentwicklungs-Erfahrungen vorausgesetzt - es finden auch keine Coding-Übungen statt. Ein Grundverständnis der Konzepte in der Softwareentwicklung ist hilfreich, aber keine Voraussetzung.

Das nehmen Sie mit

Die fortschreitende Integration von Künstlicher Intelligenz (KI) in Geschäftsprozesse stellt Unternehmen vor neue Chancen und Herausforderungen. Unternehmen müssen sich nicht nur mit herkömmlichen Cyberbedrohungen auseinandersetzen, sondern auch mit spezifischen Risiken, die aus der Nutzung oder Entwicklung von KI-Technologien resultieren. Dazu gehören Manipulationen durch Injection Angriffe, Datenlecks, Bias in Entscheidungsprozessen und die potenzielle Verletzung von Datenschutz- und Urheberrechts-Aspekten. Eine umfassende Sicherheitsstrategie, die sowohl technische als auch organisatorische Maßnahmen umfasst, ist daher unerlässlich.
Ziel des Trainings ist es, fundiertes Wissen über die Grundfunktion und die Sicherheitsaspekte von KI-Systemen zu vermitteln. Dabei werden Managementsystem-Aspekte, Bedrohungsszenarien, Sicherheitsarchitekturen und Schutzmaßnahmen detailliert trachtet.
Die Teilnehmer lernen, wie sie Risiken erkennen, bewerten und mit adäquaten Maßnahmen begegnen können. Praxisnahe Fallstudien und interaktive Workshops ermöglichen es den Teilnehmern, das erworbene Wissen direkt anzuwenden und maßgeschneiderte Sicherheitsstrategien für ihre Organisation zu entwickeln. Somit wird ein ganzheitliches

Verständnis für die sichere Implementierung und den Betrieb von KI-Systemen gewährleistet.

Das Training führt die Teilnehmer*innen schnell, kompakt und umfassend in das Thema Künstliche Intelligenz sowie damit zusammenhängende Risiken und notwendigen Sicherheitsmaßnahmen ein.
Aufbauend auf dem separat verfügbaren Basismodul („Advanced Artificiail Intelloigence Security Basics“) werden in diesem Training die Inhalte der ISO/IEC 42001:2024, welche die Zertifizierung von KI-Systemen ermöglicht, sowie damit zusammenhängende Sicherheitsmaßnahmen dargestellt, um den Teilnehmern einen ganzheitlichen Überblick zum Thema Management von KI-Systemen zu vermitteln.
Einen weiteren Teil des Trainings stellt eine Einführung in vorsätzliche Angriffe und die Verteidigung gegen unterschiedliche Schwachstellen von KI-Systemen (wie Prompt Injection, Training Data Poisoning, etc.) dar, welche sowohl bei der Entwicklung als auch bei der Verwendung von KI-Systemen eine entscheidende Sicherheitsrolle spielen. Zudem erhalten die Teilnehmer eine Übersicht über die wichtigsten Regelungen der EU-Verordnung zu Künstlicher Intelligenz, welche einen ersten risikobasierten Ansatz für KI-Systeme und deren Überwachung bildet.
Im (separat verfügbaren) anwendungsorientierten Teil des Trainings wird ein klares Verständnis für neurale Netze aufgebaut, um weiters konkrete Anwendungen in den Bereichen Computer Vision und Natural Language Processing nachvollziehen zu können. Zudem werden Methoden wie moderne Reinforcement Learning Techniken für die Entwicklung von Agents betrachtet.
Im Zuge des Trainings werden explizit keine Softwareentwicklungs-Erfahrungen vorausgesetzt - es finden auch keine Coding-Übungen statt. Ein Grundverständnis der Konzepte in der Softwareentwicklung ist hilfreich, aber keine Voraussetzung.

Zielgruppen

- Geschäftsleitung/CIO/CTO/CRO
- IT-Verantwortliche
- Informationssicherheitsbeauftrage
- Risikomanager
- Incident Manager

- Datenschutzbeauftragte und –koordinatoren
- Manager
- Interessierte

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
12.03.2025-13.03.2025	2 Tage	Wien	Trainingspreis (Vor Ort)	€ 2.615,-
12.03.2025-13.03.2025	2 Tage	Wien	Trainingspreis (Online)	€ 2.615,-
14.05.2025-15.05.2025	2 Tage	Wien	Trainingspreis (Vor Ort)	€ 2.615,-
14.05.2025-15.05.2025	2 Tage	Wien	Trainingspreis (Online)	€ 2.615,-
30.07.2025-31.07.2025	2 Tage	Wien	Trainingspreis (Vor Ort)	€ 2.615,-
30.07.2025-31.07.2025	2 Tage	Wien	Trainingspreis (Online)	€ 2.615,-
19.11.2025-20.11.2025	2 Tage	Wien	Trainingspreis (Vor Ort)	€ 2.615,-
19.11.2025-20.11.2025	2 Tage	Wien	Trainingspreis (Online)	€ 2.615,-