Advanced Artificial Intelligence Security Training – Full Course

Trainings-ID: AAIS

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 Bedrohungsszenarien, Sicherheitsarchitekturen und Schutzmaßnahmen detailliert trachtet.
Die Teilnehmer*innen lernen, wie sie Risiken erkennen, bewerten und mit adäquaten Maßnahmen begegnen können. Praxisnahe Fallstudien und Diskussionen 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.

1. AAIS Basismodul (2 Tage): Im Basiskurs werden die Grundlagen bzgl. Taxonomie, Konzepte, Lebenszyklus, Funktionen und Ökosystemen von KI-Systemen auf Basis der ISO/IEC 22989:2022 betrachtet. Dabei wird sowohl auf die grundlegende Funktion von KI-Systemen, deren Komponenten als auch deren Risiken und bekannte Angriffe vermittelt. Weiters erhalten die Teilnehmer einen Einblick in aktuelle rechtliche Regelungen der EU zum risikobasierten Management von Künstlicher Intelligenz.

2. AAIS Angriffe & Verteidigung (2 Tage): Im Aufbaumodul werden die Managementsystem-Anforderungen im Kontext der ISO/IEC 42001:2024 dargestellt. Ein weiterer Teil des Aufbaumoduls beinhaltet eine detaillierte Einführung in vorsätzliche Angriffe und die Verteidigung gegen unterschiedliche Schwachstellen von KI-Systemen (wie Prompt Injection, Training Data Poisoning, etc.), welche sowohl bei der Entwicklung als auch bei der Verwendung von KI-Systemen eine entscheidende Sicherheitsrolle spielen.

3. AAIS Anwendungmodul (1 Tag): Im anwendungsorientierten Teil des Trainings wird ein klares Verständnis für neuronale 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.

Die Teilnehmer erhalten eine Übersicht über die wichtigsten Begriffe, Konzepte und Komponenten von KI-Systemen, aktuelle Regelungen der EU-Verordnung zu Künstlicher Intelligenz, sowie über Risiken und mögliche Sicherheitsmaßnahmen bei der Nutzung und/oder Implementierung von KI-Systemen.
Weiters werden die Inhalte der ISO 42001, 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 geben.

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 Bedrohungsszenarien, Sicherheitsarchitekturen und Schutzmaßnahmen detailliert trachtet.
Die Teilnehmer*innen lernen, wie sie Risiken erkennen, bewerten und mit adäquaten Maßnahmen begegnen können. Praxisnahe Fallstudien und Diskussionen 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.

1. AAIS Basismodul (2 Tage): Im Basiskurs werden die Grundlagen bzgl. Taxonomie, Konzepte, Lebenszyklus, Funktionen und Ökosystemen von KI-Systemen auf Basis der ISO/IEC 22989:2022 betrachtet. Dabei wird sowohl auf die grundlegende Funktion von KI-Systemen, deren Komponenten als auch deren Risiken und bekannte Angriffe vermittelt. Weiters erhalten die Teilnehmer einen Einblick in aktuelle rechtliche Regelungen der EU zum risikobasierten Management von Künstlicher Intelligenz.

2. AAIS Angriffe & Verteidigung (2 Tage): Im Aufbaumodul werden die Managementsystem-Anforderungen im Kontext der ISO/IEC 42001:2024 dargestellt. Ein weiterer Teil des Aufbaumoduls beinhaltet eine detaillierte Einführung in vorsätzliche Angriffe und die Verteidigung gegen unterschiedliche Schwachstellen von KI-Systemen (wie Prompt Injection, Training Data Poisoning, etc.), welche sowohl bei der Entwicklung als auch bei der Verwendung von KI-Systemen eine entscheidende Sicherheitsrolle spielen.

3. AAIS Anwendungmodul (1 Tag): Im anwendungsorientierten Teil des Trainings wird ein klares Verständnis für neuronale 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.

Die Teilnehmer erhalten eine Übersicht über die wichtigsten Begriffe, Konzepte und Komponenten von KI-Systemen, aktuelle Regelungen der EU-Verordnung zu Künstlicher Intelligenz, sowie über Risiken und mögliche Sicherheitsmaßnahmen bei der Nutzung und/oder Implementierung von KI-Systemen.
Weiters werden die Inhalte der ISO 42001, 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 geben.

Zielgruppen

- Geschäftsleitung/CIO/CTO/CRO, IT-Verantwortliche
- Informationssicherheitsbeauftrage
- Risikomanager
- Incident Manager
- Datenschutzbeauftragte und –koordinatoren
- Manager
- Interessierte

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
10.03.2025-14.03.2025	5 Tage	Wien	Trainingspreis (Vor Ort)	€ 4.505,-
10.03.2025-14.03.2025	5 Tage	Wien	Trainingspreis (Online)	€ 4.505,-
12.05.2025-16.05.2025	5 Tage	Wien	Trainingspreis (Vor Ort)	€ 4.505,-
12.05.2025-16.05.2025	5 Tage	Wien	Trainingspreis (Online)	€ 4.505,-
28.07.2025-01.08.2025	5 Tage	Wien	Trainingspreis (Vor Ort)	€ 4.505,-
28.07.2025-01.08.2025	5 Tage	Wien	Trainingspreis (Online)	€ 4.505,-
17.11.2025-21.11.2025	5 Tage	Wien	Trainingspreis (Vor Ort)	€ 4.505,-
17.11.2025-21.11.2025	5 Tage	Wien	Trainingspreis (Online)	€ 4.505,-