Künstliche Intelligenz (KI) und Cybersicherheit

WEKA Business Media AG

Donnerstag, 30. Oktober 2025 in Zürich

Im Zeitalter digitaler Transformation wird die KI immer mehr zu einem integralen Bestandteil unserer täglichen Abläufe. Als Verantwortliche/r für Künstliche Intelligenz spielen Sie eine entscheidende Rolle bei der Gewährleistung der Sicherheit dieser technologischen Lösungen. Sie sind verantwortlich für die Analyse und Behandlung von Sicherheitsrisiken, die mit der Implementierung und Nutzung von KI verbunden sind.

Schaffen Sie das Bewusstsein für Sicherheitsrisiken und ergreifen Sie die geeigneten Massnahmen

Es ist entscheidend, ein Bewusstsein für die Sicherheitsrisiken zu schaffen und geeignete Massnahmen zur **Verbesserung der Sicherheit von KI-Modellen** zu ergreifen. Im Seminar lernen Sie, wie die Einhaltung von Sicherheitsstandards und Richtlinien sowie die Implementierung von Sicherheitskontrollen und Prüfungen dazu beitragen kann, die **Risiken zu minimieren und die Sicherheit und Zuverlässigkeit von KI-Modellen zu gewährleisten**. In diesem Seminar werden wir tiefer in die Welt der Künstlichen Intelligenz eintauchen, speziell im Kontext von Cybersicherheit. Ihnen wird ein grundlegendes Verständnis vermittelt, wie KI-Technologien zum Schutz digitaler Systeme beitragen können und welche Herausforderungen damit verbunden sind.

CHF 890.00

Mehr Informationen und Anmeldung

Zusätzliche Infos zur Veranstaltung

Zertifikat/Bestätigung

Teilnahmebestätigung

Referenten

Hermann Escher
MIT certified AI Business Strategist, CEO & Gründer - A+E Informatik GmbH

Veranstalter

WEKA Business Media AG

Telefon bei Fragen

044 586 86 37

Beschreibung

Ihr Praxis-Nutzen

- Sie erhalten ein Verständnis der Grundlagen der KI und Cybersicherheit.
- Sie lernen die Anwendung von maschinellen Lernalgorithmen zur Verbesserung der Cybersicherheit.
- Sie wissen, wie Sie die Entwicklung und Implementierung von KI-gestützten Sicherheitssystemen umsetzen.
- Sie lernen die Analyse und Reaktion auf Cyberbedrohungen mit KI.
- Sie erlangen ein Verständnis ethischer und rechtlicher Aspekte der KI in der Cybersicherheit.
- Sie wissen, auf was es bei der Zusammenarbeit mit anderen Teams in Bezug auf das Bewusstsein allfälliger Sicherheitsrisiken drauf ankommt. Sie erfahren alles über Prognose zukünftiger Entwicklungen und Trends in der KI-gestützten Cybersicherheit

Inhalte des Seminars

KI-gestützte Cybersicherheitssysteme

- Entwicklung autonomer KI-Systeme für Echtzeit-Bedrohungserkennung und -abwehr.

Ethische KI in der Cybersicherheit

- Ethische Überlegungen bei KI-gestützter Cybersicherheit sicherstellen.
- Diskussion von Rahmenwerken und Richtlinien, um sicherzustellen, dass KI-Systeme weder Privatsphäre noch Bürgerrechte verletzen, während sie robuste Sicherheit bieten.

KI-gestützte Incident Response

- Verbesserung der Reaktionszeiten und -strategien bei Sicherheitsvorfällen mithilfe von KI.
- Implementierung von KI zur schnellen Analyse und Reaktion auf Sicherheitsverletzungen, um Schäden und Erholungszeit zu minimieren.

KI in der Phishing-Erkennung

- Nutzung von KI zur Identifizierung und Verhinderung von Phishing-Attacken.

- Entwicklung von maschinellen Lernmodellen, die Phishing-Versuche in Echtzeit erkennen und bekämpfen können.

KI für Sicherheitskonformität und Audits

- Automatisierung von Compliance- und Auditprozessen mit KI.
- Einsatz von KI, um sicherzustellen, dass Systeme den regulatorischen Standards entsprechen und regelmäßige Sicherheitsaudits ohne menschliche Aufsicht durchgeführt werden.

KI-verbesserte Benutzerauthentifizierung

- Verbesserung der Benutzerauthentifizierungsprozesse mit KI.
- Implementierung von KI für dynamische, verhaltensbasierte Authentifizierungsmethoden, die sich an die Verhaltensmuster der Nutzer anpassen.

KI und Cybersicherheitsbildung

- Ausbildung der nächsten Generation von Cybersicherheitsexperten mit KI-Tools.
- Erstellung KI-gesteuerter Bildungsplattformen, die personalisierte Lernerfahrungen bieten und reale Cyber-Angriff Szenarien simulieren.

KI für Malware-Erkennung und -Entfernung

- Fortgeschrittene KI-Techniken zur Identifizierung und Eliminierung von Malware.
- Entwicklung ausgereifter KI-Modelle, die Malware mit hoher Genauigkeit erkennen, analysieren und entfernen können.

KI in der sicheren Softwareentwicklung

- Integration von KI in den Softwareentwicklungsprozess zur Verbesserung der Sicherheit.
- Nutzung von KI zur Identifizierung und Behebung von Sicherheitslücken während der Entwicklungsphase, um sicherere Softwareprodukte zu gewährleisten.

Entwicklung von Richtlinien zur KI-Cybersicherheit

- Gestaltung von Richtlinien für den Einsatz von KI in der Cybersicherheit.
- Diskussion über die Erstellung von Richtlinien, die die ethische und effektive Nutzung von KI in Sicherheitsmaßnahmen regeln.

KI in der Netzwerksicherheit

- Verbesserung der Netzwerksicherheit durch KI.
- Einsatz von KI-Systemen zur kontinuierlichen Überwachung des Netzwerkverkehrs, Erkennung von Anomalien und Verhinderung unbefugten Zugriffs.

KI für die Sicherheit von Cloud-Diensten

- Schutz cloudbasierter Dienste mit KI.
- Nutzung von KI zur Verbesserung der Sicherheit von Cloud-Infrastrukturen und -Diensten, um Datenintegrität und Verfügbarkeit zu gewährleisten.

KI und biometrische Sicherheit

- Kombination von KI mit biometrischen Systemen für verbesserte Sicherheit.
- Entwicklung von KI-gestützten biometrischen Systemen, die eine genauere und sichere Benutzeridentifikation bieten.

Zukünftige Trends in KI und Cybersicherheit

- Prognose zukünftiger Entwicklungen in der KI-gestützten Cybersicherheit.
- Analyse aufkommender Trends und Technologien, die die Zukunft der KI in der Cybersicherheit prägen werden, einschliesslich potenzieller Herausforderungen und Chancen.

Zielgruppe

CAIO, Geschäftsführer/innen, Entscheidungsträger/innen, Datenschutzbeauftragte, IT-Verantwortliche, Projektleiter/innen, Security Officer.

Seminarzeiten

09:00 - 16:30 Uhr

Mehr Informationen und Anmeldung

Buchungsbedingungen

AGB für Praxis-Seminare und Fachkongresse

Anmeldefristen/Teilnehmerzahl

Die Teilnehmerzahl pro Seminartag ist begrenzt um Ihre optimale Betreuung zu gewährleisten. Die Anmeldungen werden in der Reihenfolge ihres Eingangs berücksichtigt.

Abmeldungen/Verschiebungen/Fernbleiben

Abmeldungen sind bis 30 Tage vor dem jeweiligen Seminartermin ohne Kostenfolgen möglich. Bei Abmeldungen bis 14 Tage vor dem Seminartermin wird eine Bearbeitungspauschale von 50% der Teilnahmegebühr fällig. Bei späterer Abmeldung oder Fernbleiben ist – unabhängig vom Verhinderungsgrund – die ganze Teilnahmegebühr geschuldet. In diesem Fall wird der angemeldeten Person die

Seminardokumentation per Post zugestellt.

Umbuchungen

Sie können bis 30 Tage vor dem jeweiligen Seminartermin ohne Kostenfolgen umbuchen. Bei Umbuchungen bis 14 Tage vor Seminarbeginn wird eine Bearbeitungspauschale von 30%, bei späterer Umbuchung 50% der Teilnahmegebühr fällig.

Ersatzteilnehmer

Gerne akzeptieren wir ohne zusätzliche Kosten einen Ersatzteilnehmer.

Preis und Rechnungsstellung

Im Seminarpreis inbegriffen sind die Seminarunterlagen, Getränke, Mittagessen (nur bei ganztägigen Seminaren), Pausenverpflegung sowie ein Zertifikat. Die Rechnungsstellung erfolgt in der Regel nach Ihrer Anmeldung und ist sofort fällig. Unsere Veranstaltungen sind grundsätzlich mehrwertsteuerpflichtig.

Durchführung

Programmänderungen oder Umbuchungen aufgrund Unterbesetzung behält sich der Veranstalter vor.

Lehrgang

Für die einzelnen Module gelten die oben genannten Teilnahmebedingungen. Der Abbruch eines Lehrgangs wird individuell mit dem Veranstalter besprochen.