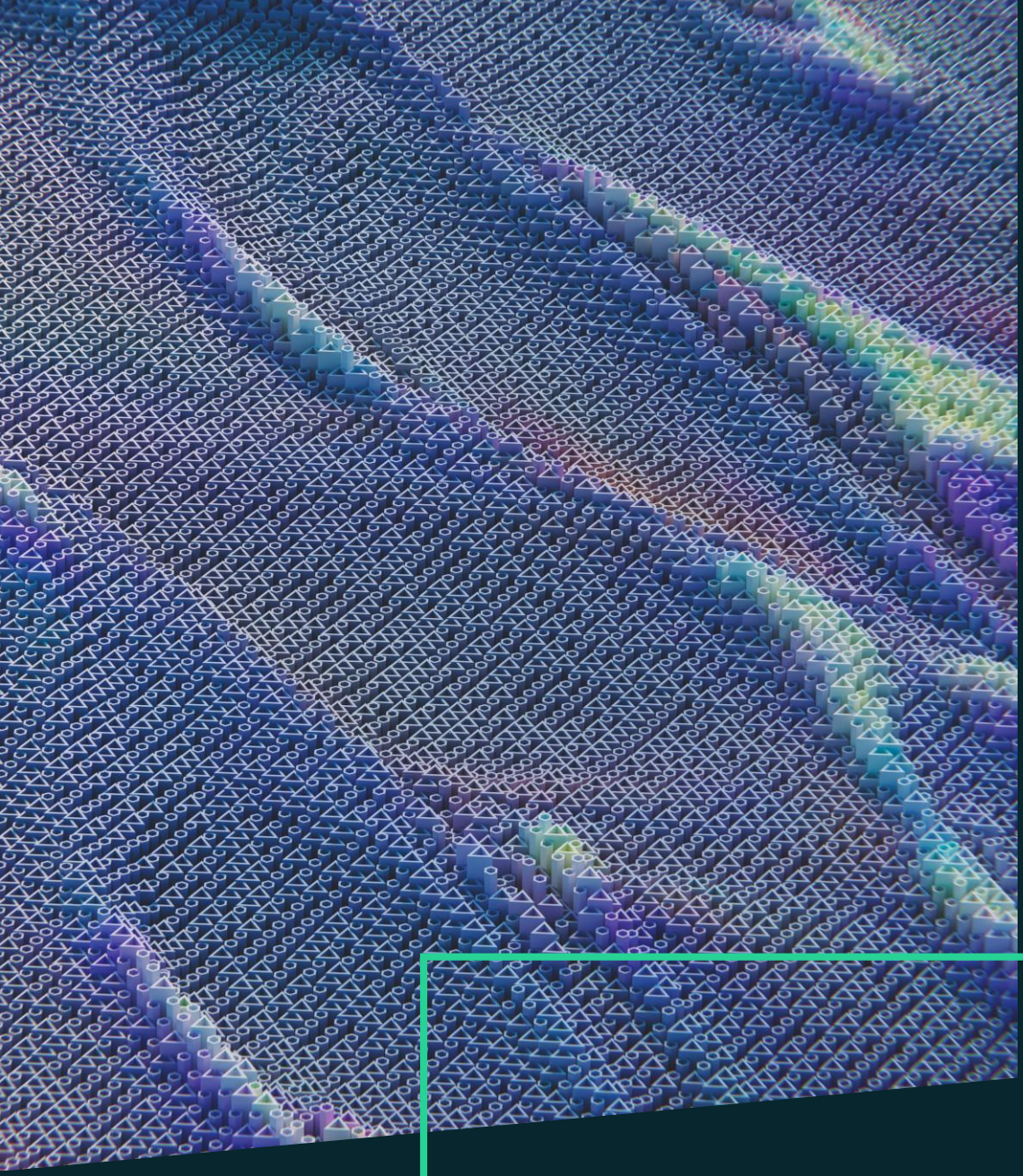


bitkom
akademie

Cybersecurity 2.0: KI in der IT-Sicherheit

Zertifikatslehrgang

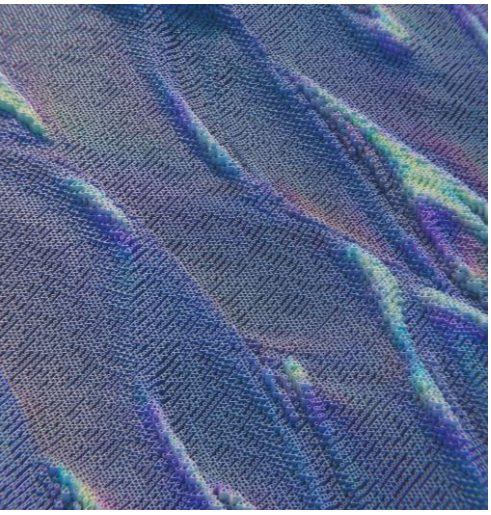
Cybersecurity 2.0: KI in der IT-Sicherheit

Cyberangriffe mit Künstlicher Intelligenz vorhersagen, abwehren und vorbeugen

Kurzbeschreibung

Künstliche Intelligenz verändert die IT-Sicherheit grundlegend: Sie ermöglicht neue Formen der Angriffserkennung, automatisiert Analyseprozesse und eröffnet völlig neue Verteidigungsansätze. Gleichzeitig entstehen durch KI neue Verwundbarkeiten, Manipulationsmöglichkeiten und Risiken, die klassische Sicherheitsmechanismen nicht ausreichend berücksichtigen.

Im Seminar Cybersecurity 2.0: KI in der IT-Sicherheit erhalten Sie einen umfassenden Überblick über die **Chancen und Herausforderungen KI-basierter Sicherheitssysteme**. Sie lernen, wie Angreifer KI einsetzen, welche neuen **Bedrohungsformen** dadurch entstehen und wie Sie selbst **KI** gezielt zur **Stärkung Ihrer Sicherheitsarchitektur** nutzen können. Darüber hinaus erfahren Sie, **wie KI sicher in bestehende Governance- und Compliance-Strukturen integriert wird** – inklusive Einordnung in NIS 2, ISO 27001, ISO 42001, EU AI Act und DORA – und entwickeln die Grundlage für eine moderne, zukunftsfähige KI-Security-Strategie.



Inhalt

- Verständnis moderner KI-Technologien und ihrer Bedeutung für die Cyberabwehr
- Analyse zentraler KI-basierten Bedrohungen wie Data Poisoning, Prompt Injection und modellbasierten Angriffen
- Einsatz von Predictive AI und KI-gestützter Threat Detection im SOC
- KI als Werkzeug für Angreifer: automatisierte Reconnaissance, Social Engineering und Deepfake-Szenarien
- Absicherung von KI-Modellen: Robustness, Monitoring, SecMLOps und Schutz vor Manipulation
- Praktische Anwendung von KI in Incident Detection, Analyse und Response
- Governance- und Compliance-Anforderungen (NIS 2, ISO 27001, ISO 42001, EU AI Act, DORA) im KI-Kontext

Was lernen Sie in diesem Seminar?

Sie erhalten ein fundiertes Verständnis darüber, wie moderne KI-Systeme funktionieren und welche Auswirkungen sie auf die IT-Sicherheitslandschaft haben. Sie lernen zentrale KI-spezifische Risiken wie Data Poisoning, Prompt Injection und modellbasierte Angriffe kennen und verstehen, wie Angreifer KI für automatisierte und personalisierte Attacken nutzen. Sie erfahren, wie KI in der Verteidigung eingesetzt werden kann – etwa in der Anomalieerkennung, Threat Intelligence oder im SOC – und wie sich KI-Modelle technisch und organisatorisch absichern lassen. Darüber hinaus lernen Sie, KI sicher in bestehende Governance-, Compliance- und ISMS-Strukturen einzuordnen und ein zielgerichtetes KI-Sicherheitskonzept zu entwickeln.

bitkom akademie

Cybersecurity 2.0: KI in der IT-Sicherheit

Cyberangriffe mit Künstlicher Intelligenz vorhersagen, abwehren und vorbeugen

Zielgruppe

Der Lehrgang Cybersecurity 2.0: KI in der IT-Sicherheit richtet sich an Fach- und Führungskräfte, die KI sicher, verantwortungsvoll und strategisch im Unternehmenskontext einsetzen wollen. Er eignet sich besonders für:

- Sicherheitsverantwortliche, die verstehen möchten, wie KI-basierte Angriffe funktionieren und wie KI für moderne Abwehrstrategien eingesetzt werden kann.
- CISOs, ISOs und IT-Manager:innen, die KI-Technologien in ihre bestehende Sicherheitsarchitektur integrieren oder bewerten müssen.
- Security Engineers, SOC-Analyst:innen und Threat-Intelligence-Teams, die KI-gestützte Detection-, Analyse- und Response-Mechanismen in der Praxis anwenden wollen.
- Führungskräfte aus Governance, Risk & Compliance, die KI in regulatorische Anforderungen wie NIS-2, ISO 27001, ISO 42001 oder den EU AI Act einordnen müssen.

Didaktischer Aufbau

Der Lehrgang verbindet fundierte technische Grundlagen mit praxisnahen Sicherheitsanwendungen. Nach einer verständlichen Einführung in KI-Technologien und ihre sicherheitsrelevanten Besonderheiten zeigt der Referent anhand realitätsnaher Beispiele, wie KI sowohl von Angreifern als auch in der Verteidigung genutzt wird. Praxisblöcke, Gruppenübungen und Live-Demonstrationen sorgen dafür, dass die Teilnehmenden KI-basierte Angriffe, Manipulationsversuche und moderne Detection-Ansätze unmittelbar erleben und einordnen können. Durch die Arbeit an Fallstudien und einem abschließenden KI-Sicherheitskonzept vertiefen die Teilnehmenden Ihr Verständnis dafür, wie KI verantwortungsvoll, sicher und compliant im Unternehmen eingesetzt werden kann.

Zertifizierung

Der Lehrgang schließt mit einer Prüfung ab, die an einem separaten Termin stattfindet. Mit Bestehen der Prüfung erhalten Sie ein **Zertifikat**, das Ihre Fachkenntnisse im Bereich Cybersecurity und Künstliche Intelligenz nachweist. Die Zertifizierung beruht auf einem Qualitätsstandard, den sich die Bitkom Akademie und ihre Partner als Qualitätssiegel für ihre Ausbildungslehrgänge gesetzt haben.

bitkom akademie

Cybersecurity 2.0: KI in der IT-Sicherheit

Cyberangriffe mit Künstlicher Intelligenz vorhersagen, abwehren und vorbeugen

Zusatzinformationen

- Das Seminar hat eine begrenzte **Teilnehmerzahl von 16 Personen**. Unser Referent kann dadurch gezielt auf individuelle Fragestellungen eingehen. Die Mindestteilnehmerzahl beträgt 5.
- Die Bitkom Akademie ist anerkannter Bildungsträger in Baden-Württemberg und Nordrhein-Westfalen. Teilnehmende haben im Rahmen des Bildungszeitgesetzes die Möglichkeit, Bildungsurlaub bzw. eine Bildungsfreistellung zu beantragen. Auf Anfrage erstellen wir Anträge auf Anerkennung unserer Seminar-Veranstaltungen auch in anderen Bundesländern.
- Dieser Online-Workshop wird mit Zoom durchgeführt. Systemvoraussetzungen und unterstützte Betriebssysteme können Sie hier einsehen. Für die Einwahl in Zoom über die verschiedenen Anwendungen (Desktop Client, App oder Web-Client) bietet Ihnen diese Tabelle einen zusätzlichen Vergleich zu den jeweiligen Eigenschaften.
- Wir erklären ausdrücklich, dass beim Bitkom – Unterzeichner der Charta der Vielfalt – jede Person, unabhängig von Geschlecht, Nationalität, ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter, sexueller Orientierung und Identität willkommen ist.

bitkom akademie

Seminarprogramm

Cybersecurity 2.0: KI in der IT-Sicherheit

Tag 1

Einordnung von KI und Grundlagen der Technologie
- Historische Entwicklung der KI und aktuelle Bedeutung
- Machine Learning, Deep Learning & neuronale Netze
- Zentrale Lernmechanismen (supervised, unsupervised, reinforcement)

Ethik & Verantwortungsfragen in der KI
- Grundlagen verantwortungsvoller KI-Nutzung
- Risiken durch Verzerrungen und fehlende Transparenz
- Warum Ethik ein Sicherheitsfaktor ist

KI-Modelle und moderne KI-Systeme verstehen
- Was ist GPT? Funktionsweise und Besonderheiten großer Sprachmodelle
- Was ist ein GAN? Überblick über generative Modelle
- Chancen und Risiken im Security-Kontext

Cybersecurity 2.0 & KI-Strategie im Unternehmen
- Traditionelle Cybersecurity vs. KI-gestützte Ansätze (KI vs. KI)
- Einordnung von AI Agents & Hypecheck
- Strategische Grundlagen für den Einsatz von KI in der Sicherheit

Tag 2

Phishing 2.0 & Deepfakes in der Praxis
- Erstellung moderner KI-basierter Phishing- und Deepfake-Angriffe
- Wie einfach sich realistische Manipulationen heute erzeugen lassen
- Methoden zur Erkennung und Entlarvung KI-generierter Inhalte

Sicheres Prompt Engineering & Abwehr von Prompt Injections
- Grundlagen für strukturierte, reproduzierbare und sichere Prompts
- Angriffsszenarien durch Prompt Injection & indirekte Manipulation
- Techniken zur Härtung eigener KI-Anwendungen gegen Misuse

Risiken & Herausforderungen eigenentwickelter KI-Systeme
- Modellrisiken, Trainingsdatenqualität und technische Verwundbarkeiten
- OWASP Top 10 für KI & typische Schwachstellen in KI-Pipelines
- Sicherheitsanforderungen an AIMS & Verzahnung mit ISMS

KI-Compliance & regulatorische Anforderungen
- Einordnung in ISO 42001, ISO 27001 und EU AI Act
- Datenschutzanforderungen (GDPR) im Kontext von KI-Systemen
- Aufbau und Struktur einer wirksamen AI Policy im Unternehmen

bitkom akademie

Seminarprogramm

Cybersecurity 2.0: KI in der IT-Sicherheit

Tag 3

Modellrisiken: Halluzinationen, Bias & Datenmanipulation

- Ursachen und Auswirkungen von Halluzinationen, Verzerrungen und Fehlvorhersagen
- Poisoned Data, manipulierte Modelle und Model Drift als Sicherheitsrisiken
- Strategien zur Erkennung und systematischen Reduktion von Modellfehlern

Gegenmaßnahmen gegen KI-Modellrisiken

- Validierung, Monitoring & kontinuierliche Überwachung von KI-Systemen
- Techniken zur Härtung gegen Datenvergiftung & Modellmanipulation
- Einsatz von System Prompts und Guardrails zur Stabilisierung von LLM-Verhalten

KI-gestützte Cyberabwehr: SOC-Integration & APT-Analyse

- Rolle von KI in Threat Detection, Log-Analyse und Alert-Triage
- Nutzung von KI zur Erkennung komplexer Angriffsketten (APT)
- Hype Check: Grenzen von SOC-Automatisierung & Predictive AI

Threat Intelligence & moderne Detection-Ansätze

- KI-gestützte Analyse von Bedrohungsdaten & Angriffsmustern
- Automatisierte Mustererkennung in Threat Intelligence Feeds
- Realistische Einsatzszenarien vs. aktuelle technische Machbarkeit

Tag 4

KI-Risikomanagement & Bewertung von KI-Systemen

- Methoden zur Identifikation, Bewertung und Priorisierung von KI-Risiken
- Besonderheiten im Risikomanagement für LLMs und datengetriebene Modelle
- Umgang mit Echtzeitdaten, externen Wissensquellen und dynamischen Risiken

LLM-Entwicklung & Integration in CI/CD-Pipelines

- Grundprinzipien des sicheren LLM-Lebenszyklus
- Anforderungen an Datenqualität, Testprozesse & Modellvalidierung
- Einbettung von KI-Modellen in moderne CI/CD- und MLOps-Prozesse

KI-Communities & professionelle Netzwerke

- Austauschformate, Arbeitskreise & relevante Security- und KI-Communities
- Nutzen von Best Practices, Benchmarking & Peer Learning
- Rolle der Community in Innovation, Sicherheit & Compliance

Weiterbildung & Zertifizierungen im KI-Kontext

- Überblick über professionelle KI- und AI-Security-Zertifikate
- Einordnung nach Rolle, Zielgruppe & Kompetenzstufe
- Orientierung für individuelle Entwicklungswege und Teamqualifizierung

bitkom akademie

Ihr Referent

Kevin Engelhardt

Cybersecurity Innovation Consultant
pcbs Cybersecurity Consulting

Kevin Engelhardt ist Cybersecurity- und KI-Governance-Experte mit umfassender Erfahrung in der sicheren Einführung, Bewertung und Regulierung von KI-Systemen in Unternehmen. Sein Schwerpunkt liegt auf KI-gestützter Security, Security Governance, ISMS-Integration sowie modernen Sicherheitsarchitekturen in Cloud- und SaaS-Umgebungen.
Er begleitet Unternehmen bei der Umsetzung von NIS-2-Pflichten, ISO-27001- und ISO-42001-Anforderungen, beim Aufbau von KI-Risikomanagement sowie bei der strategischen Einführung von KI-Technologien im Security-Kontext. Durch seine Arbeit in Energie, Technologie, Automotive und Scale-ups verbindet er technische Tiefe mit einem klaren Blick für regulatorische, organisatorische und operative Anforderungen.
Neben seiner Tätigkeit als Berater ist er Dozent an der DHBW im Bereich Secure Software & Security by Design und besitzt zahlreiche Zertifizierungen wie ISO 27001 Lead Implementer, ISO 42001 Lead Implementer, CISSP und zahlreiche Cloud- und Sicherheitszertifizierungen.
Seine praxisnahe Arbeitsweise und breite Erfahrung – von SOC-Integration über Threat Detection bis hin zu KI-Strategie und Policy-Entwicklung – machen ihn zu einem vielseitigen Experten, der Sicherheit, Innovation und moderne KI-Anwendungen miteinander verbindet.

Shortfacts

Termine, Veranstaltungsort und Preise

Die aktuellen Informationen entnehmen Sie bitte der ↗ Website der Bitkom Akademie.

Kontaktieren Sie uns – wir beraten Sie gern.

Bitkom Akademie | Albrechtstraße 10 | 10117 Berlin
T 030 27576-540 | info@bitkom-akademie.de
Weitere Seminare finden Sie unter **www.bitkom-akademie.de**

bitkom akademie