Cybersecurity-KI-Spezialist (TÜV).

Planung und Implementierung KI-gestützter Cyberabwehrmaßnahmen – Intelligente Verteidigung für moderne Bedrohungslagen

Seminar	3 Termine verfügbar	Zertifikat
Präsenz / Virtual Classroom	24 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 31600

Stand: 04.07.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31600

Cyberangriffe entwickeln sich rasant weiter – insbesondere durch KI-basierte Angriffsmethoden. Dieses Seminar befähigt Sie, moderne Cyberrisiken zu verstehen, Sicherheitsmaßnahmen zu planen und KI sowohl als Risiko wie auch als Schutzinstrument professionell einzusetzen.

Nutzen

- Sie kennen die aktuellen Cyberbedrohungen sowie die Funktionsweise moderner, KI-basierter Angriffe.
- Sie werden in die Lage versetzt, tragfähige Sicherheitsstrategien zu entwickeln und KI-gestützte Abwehrmaßnahmen zielgerichtet in die bestehende Sicherheitsarchitektur einzuordnen
- Sie wissen, wie eine wirksame Cybersecurity-Organisation aufgebaut, gesteuert und kontinuierlich verbessert wird.
- Sie können Risiken fundiert bewerten, praxisnahe Krisenübungen durchführen und moderne regulatorische Anforderungen wie den EU AI Act und NIS2 sicher anwenden

Zielgruppe

- Fachkräfte
- IT-Verantwortliche
- Mitarbeiter im Informationssicherheits- und Compliance-Umfeld
- Personen, die Cybersecurity und KI-Risiken im Unternehmen koordinieren sollen.

Voraussetzungen

Grundkenntnisse in IT oder Informationssicherheit sind hilfreich, jedoch nicht zwingend erforderlich.

Inhalte des Seminars

Cybersecurity-Grundlagen

- Bedrohungslage, Schutzziele, Rollen; neue KI-Gefahren: KI-gestützte Angriffe, automatisiertes Social Engineering.

IT-Infrastrukturen & Systeme

- Systemlandschaften in Unternehmen;Schwachstellen; Angriffspunkte für KI-basierte Attacken.

KI als Risiko (Deepfakes, KI-Phishing, Social Engineering)

- Deepfakes (Audio/Video), KI-generierte Phishing-Kampagnen, automatisierte Social-Engineering-Skripte, Prompt Injection.

KI als Verteidigungswerkzeug

- Anomalieerkennung, Fraud Detection, KI im SOC, Mustererkennung, KI-gestützte Angriffsdetektion.

Regulatorische Anforderungen

- EU AI Act, DSGVO, NIS2, BAIT/VAIT, DORA; Anforderungen an KI-Sicherheit und Datenverarbeitung.

KI-sicheres Organisationskonzept

- KI-Policies, Zero Trust, ISMS, Lieferkettenrisiken; Schutz vor Deepfake-Angriffen und KI-Missbrauch.

Praxisteil & Krisenübungen

- Simulierte KI-Phishing-Angriffe, Deepfake-Erkennung, Log-Analyse, Incident Response.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31600 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.