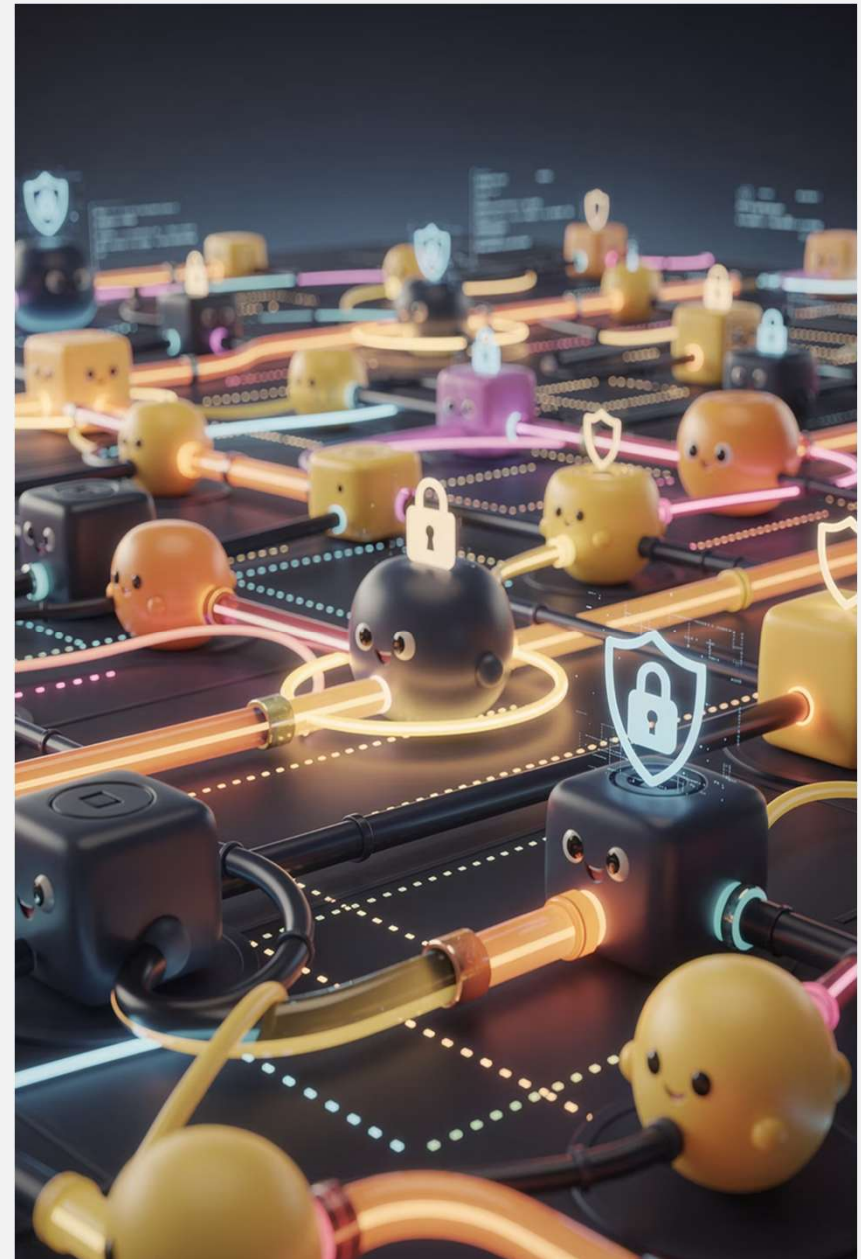


Cybersecurity & Informationssicherheit

Kick-off Veranstaltung zur Weiterbildung mit NIS-2, ISMS & KI-Integration



Ihre Reise durch die Weiterbildung

01

Begrüßung & Kennenlernen

Wir stellen uns vor und teilen unsere Erwartungen für diesen Kurs

02

Weiterbildungsangebot

Cybersecurity, NIS-2 & ISMS

03


Kursinhalte im Detail

8 Lektionen für Ihre Zukunft

04

Offene Fragen

Raum für Austausch und Klärung

 Unser Treffen lebt von Ihrer aktiven Teilnahme – fühlen Sie sich eingeladen, Fragen zu stellen und Ihre Gedanken zu teilen!

Offene Vorstellungsrunde



Lernen wir uns kennen!

Jede und jeder Teilnehmende stellt sich kurz vor. Teilen Sie gerne mit uns:

- Ihren Namen und beruflichen Hintergrund
- Was Sie zu diesem Kurs motiviert hat
- Welche Erwartungen und Wünsche Sie mitbringen
- Was Sie sich von der gemeinsamen Zeit erhoffen

Ziel ist es, einander kennenzulernen und eine vertrauensvolle Atmosphäre zu schaffen, in der wir voneinander lernen können.

Tobias Apel

Allgemeines

- Geschäftsführer apro.gmbh
- Senior IT-Sicherheitsberater
- 17 Jahre Berufserfahrung

Skills

- BSI-Standard 200-1 bis 200-4
- BSI-Grundschutz Kompendium
- ISO/IEC 27001/27002
- ISO/IEC 27005
- ISO 22301

Skills

- BSI-Praktiker
- Lead Auditor 27001
- Zusätzliche Prüfverfahrens-Kompetenz für § 8a (3)
BSIG
- ISO 27001 Professional



Cybersecurity & Informationssicherheit

Eine Weiterbildung für die digitale Zukunft mit NIS-2, ISMS & KI-Integration



Was Sie in dieser Weiterbildung erwartet

Die Weiterbildung vermittelt praxisorientierte Kenntnisse und Fähigkeiten in den Bereichen Cybersecurity, Informationssicherheits-Management (ISMS), Umsetzung der europäischen NIS-2-Richtlinie sowie Integration von Künstlicher Intelligenz in Sicherheitsstrategien.



**Sicherheitskonzepte
entwickeln**



**Bedrohungen
analysieren**



Compliance erfüllen



**KI-Technologien
einsetzen**

Arbeitsmarktrelevanz: Warum jetzt?

Cybersecurity- und Informationssicherheitskompetenzen zählen zu den zentralen Schlüsselqualifikationen in einer zunehmend digitalisierten Wirtschaft. Mit Inkrafttreten der NIS-2-Richtlinie steigt der Bedarf an Fachkräften massiv.

Unternehmen suchen dringend Expertinnen und Experten, die sowohl regulatorische Anforderungen umsetzen als auch moderne technische Sicherheitslösungen einführen können.

300K

Fehlende Fachkräfte

in der IT-Sicherheit in Deutschland

85%

Mehr Cyberangriffe

auf Unternehmen seit 2020

Ihre beruflichen Perspektiven

Absolventinnen und Absolventen der Weiterbildung eröffnen sich vielfältige Karrierechancen:

Sicherheitsmaßnahmen strategisch planen

Entwickeln Sie umfassende Sicherheitskonzepte für Organisationen

ISMS etablieren

Implementieren Sie Informationssicherheits-Managementssysteme nach ISO 27001

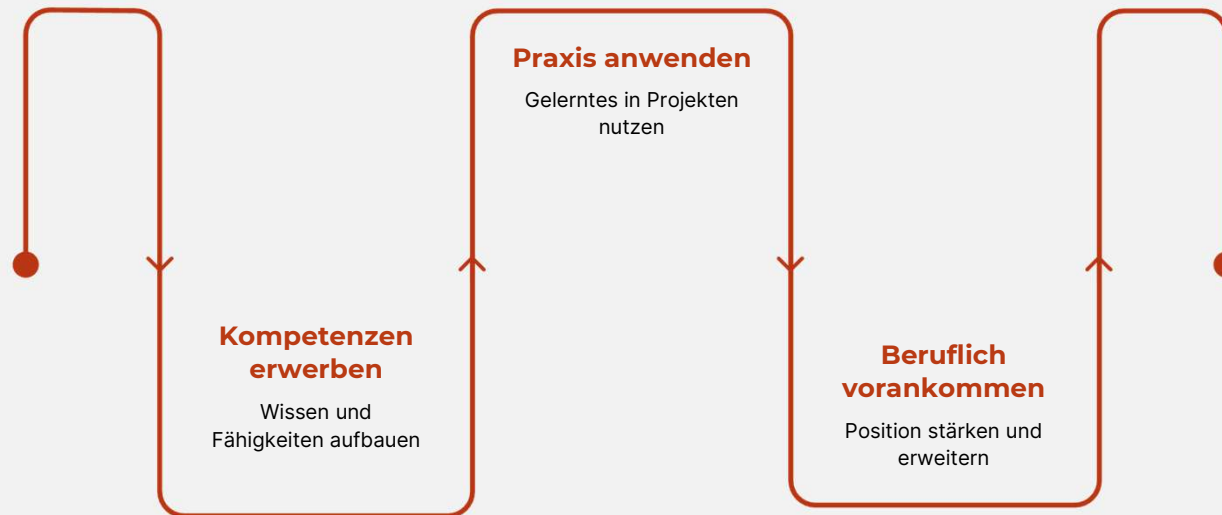
KI-basierte Lösungen einsetzen

Nutzen Sie moderne Technologien zur Bedrohungserkennung

Digitale Resilienz erhöhen

Stärken Sie die Widerstandsfähigkeit von Unternehmen nachhaltig

Nachhaltige Stärkung Ihrer Position



Die Weiterbildung befähigt Sie, Ihre berufliche Position nachhaltig zu stärken und neue Tätigkeitsfelder zu erschließen.

Was Sie erreichen

- Rechtliche Vorgaben (z.B. NIS-2) sicher einhalten
- Prozesse zur Risikominimierung erfolgreich einführen
- KI-Technologien in Sicherheitsarchitekturen einbinden
- Qualifizierung für Rollen in IT-Sicherheit, Compliance und Risikomanagement

Unser didaktisches Konzept

Die Weiterbildung wird online durchgeführt und kombiniert verschiedene Lehrmethoden für optimalen Lernerfolg:



Fachvorträge

Fundierte theoretisches Wissen



Fallstudien

Praxisorientierte Anwendung



Gruppendiskussionen

Interaktiver Austausch



Individuelle Betreuung

Persönliche Unterstützung



Ziele der Weiterbildung

Die Maßnahme vermittelt praxisnahes Fachwissen und zentrale Handlungskompetenzen für den Aufbau, die Umsetzung und Weiterentwicklung von Cybersecurity- und Informationssicherheitsstrategien.

Kursinformationen im Überblick

Weiterbildung zum Cybersecurity & Informationssicherheit

mit NIS-2, ISMS & KI-Integration

Bildungsträger	Seminarkontor GmbH
Standort	Markomannenstrasse 11, 70771 Leinfelden-Echterdingen
UE Gesamt	400 Unterrichtseinheiten
Dauer	26 Wochen
Abschluss	Trägerinternes Zertifikat
Anbieter-Nr.	304731

Besonderheiten unserer Weiterbildung

Flexibler Einstieg

Jederzeit möglich – starten Sie, wenn es für Sie passt

Freie Zeiteinteilung

Lernen Sie in Ihrem eigenen Tempo

Praxisorientierung

Viele praktische Übungen für direkten Transfer

Persönliche Betreuung

Individuelle Unterstützung durch erfahrene Trainer



Die 8 Lektionen im Detail

400 Unterrichtseinheiten strukturiert in thematische Module

Grundlagen der Informationssicherheit

Was Sie lernen

Sie verstehen die grundlegenden Schutzziele der Informationssicherheit, typische Bedrohungsszenarien und relevante Rechtsrahmen. Sie sind in der Lage, diese Aspekte zu bewerten und auf Ihr eigenes berufliches Umfeld zu übertragen.

Schutzziele

Vertraulichkeit, Integrität,
Verfügbarkeit

Bedrohungen

Cyberbedrohungen und
Angriffsvektoren

Architekturen

IT-Sicherheitsarchitekturen
und Schutzmechanismen

Rechtsrahmen

DSGVO, NIS-2 und weitere
Normen

LEKTION 2

NIS-2 verstehen & umsetzen

60 Unterrichtseinheiten

Sie entwickeln ein umfassendes Verständnis der europäischen NIS-2-Richtlinie und können deren Anforderungen praxisnah auf betriebliche Kontexte anwenden.



NIS-2: Ihre Kompetenzen

1

Risiken erfassen

Systematische
Dokumentation von
Bedrohungen

2

Governance aufbauen

Strukturen zur
Sicherstellung von
Compliance

3

Meldepflichten umsetzen

Reporting und Incident-
Management

4

Best Practices anwenden

Analyse aktueller
Fallbeispiele

NIS-2: Praktische Übungen

Durch praxisnahe Aufgaben stellen wir den unmittelbaren Transfer in Ihre berufliche Realität sicher:

- Bewertung von Unternehmensprofilen hinsichtlich NIS-2-Pflichten
- Entwicklung eines Risikoregisters mit Maßnahmenplanung
- Simulation von Meldepflicht-Situationen
- Vergleich verschiedener Governance-Modelle
- Diskussion zu Chancen und Herausforderungen für KMU



ISO 27001: Kernkompetenzen

Grundlagen & Annex A

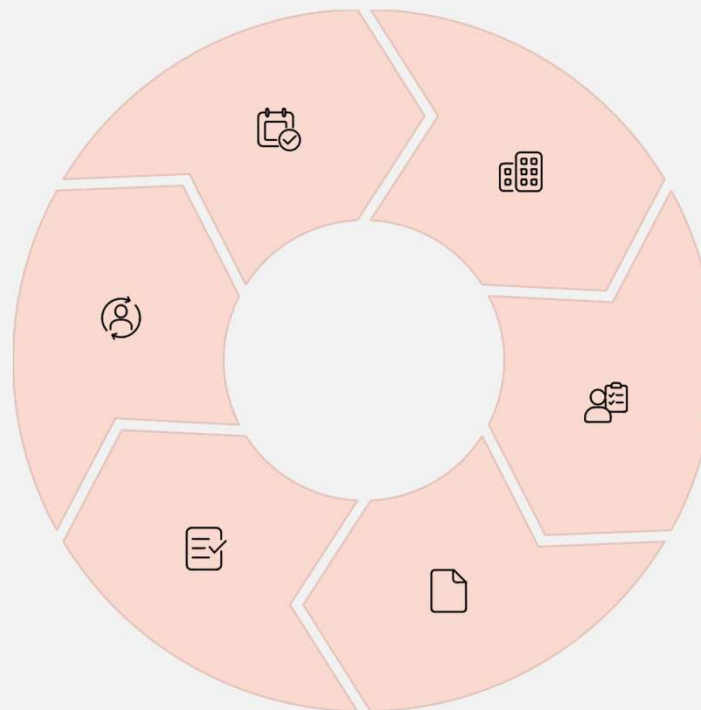
Überblick über Standards und Controls

PDCA-Zyklus

Kontinuierliche Verbesserung

Audit-Vorbereitung

Externe Zertifizierungen



ISMS aufbauen

Einführung im Unternehmen

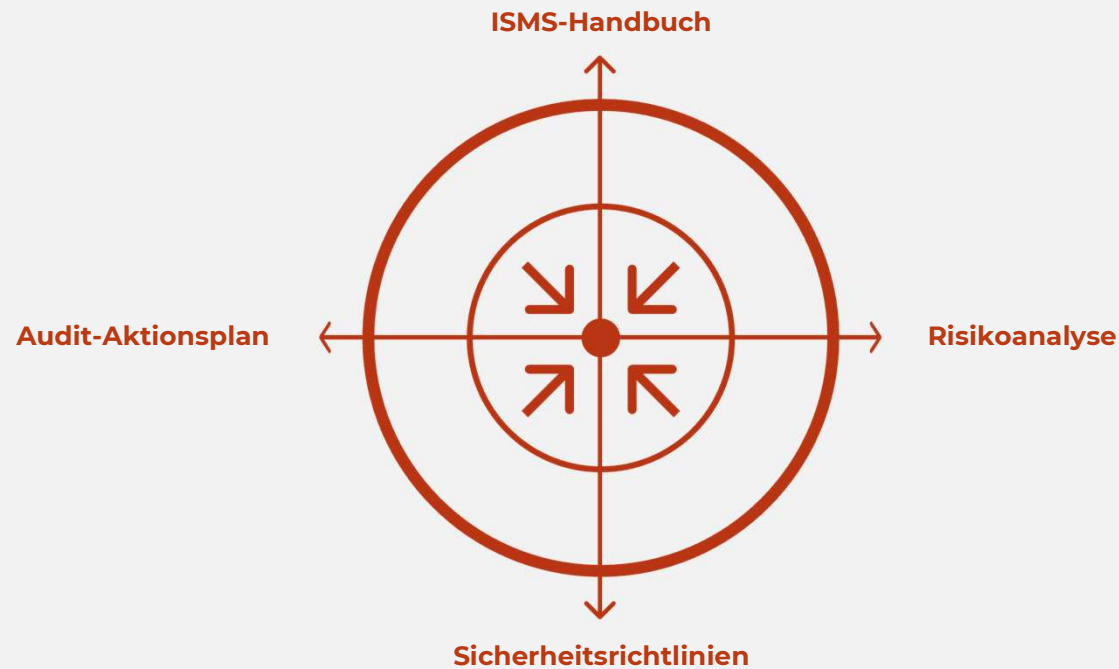
Risiken analysieren

Risikobehandlung in der Praxis

Dokumentation

Policies erstellen und pflegen

ISO 27001: Praxistransfer



Ihre Ergebnisse

Die Teilnehmenden erarbeiten beispielhaft folgende Dokumente:

1. Struktur eines ISMS-Handbuchs
2. Risikoanalyse mit Behandlungsplänen
3. Unternehmensspezifische Policies
4. Maßnahmenplan zur Audit-Vorbereitung

Alle Inhalte werden durch praxisnahe Fallstudien, Gruppenarbeiten und individuelle Aufgaben vertieft.

LEKTION 4

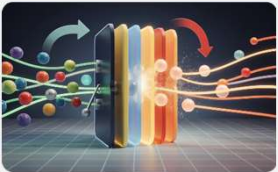
Technische & organisatorische Maßnahmen

70 Unterrichtseinheiten

Sie erwerben praxisorientierte Kompetenzen im Umgang mit technischen und organisatorischen Schutzmaßnahmen.



Technische Sicherheitsmaßnahmen



Netzwerksicherheit & Firewalls

Konfiguration und Verwaltung



Endpoint-Security

EDR und SOC-Konzepte



Backup & Recovery

Desaster-Recovery-Konzepte



Identity & Access Management

Zugriffskontrolle und Berechtigungen



Kryptographie

Verschlüsselung sensibler Daten



Notfallmanagement

Business Continuity Planning

Praktische Übungen: Technische Maßnahmen

Hands-on Erfahrung

Sie setzen Ihr Wissen direkt in praktischen Szenarien um:

- Einrichtung und Konfiguration einer Firewall
- Analyse von Endpoint-Security-Maßnahmen
- Entwicklung eines Backup-Plans für kritische Systeme
- Konzeption von Identity- & Access-Management
- Verschlüsselung mit praxisnahen Tools
- Notfallmanagement anhand von Fallstudien



LEKTION 5

Awareness & Security Culture

50 Unterrichtseinheiten

Sie entwickeln eigenständig zielgerichtete Awareness-Kampagnen und bauen eine nachhaltige Sicherheitskultur im Unternehmen auf.



Awareness: Von der Theorie zur Praxis

Social Engineering erkennen

Methoden und Schutzmaßnahmen

Schulungskonzepte entwickeln

Awareness-Kampagnen gestalten

Change Management

Sicherheitskultur etablieren

Simulationen durchführen

Reale Angriffsszenarien üben

Der Mensch als Sicherheitsfaktor

Die beste Technologie nützt wenig, wenn Mitarbeitende nicht sensibilisiert sind. Sie lernen, wie Sie eine lebendige Sicherheitskultur schaffen.

Incident Response & Forensik

50 Unterrichtseinheiten

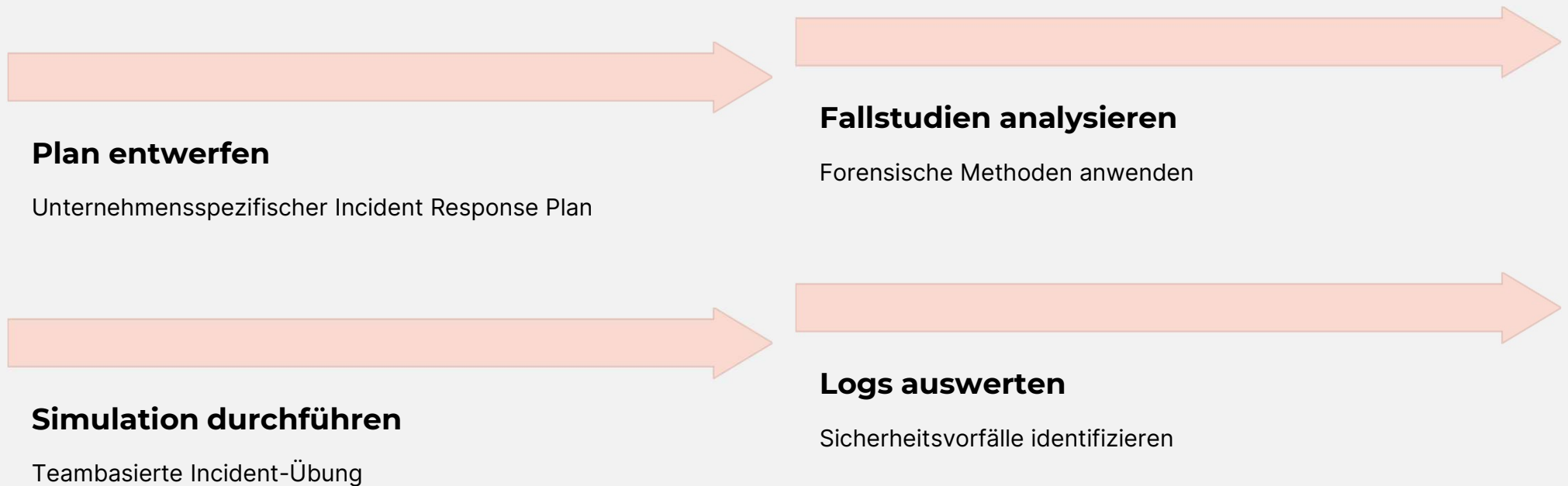


Professionelle Reaktion auf Vorfälle

Sie entwickeln einen vollständigen Incident Response Plan und erwerben Grundlagen in Monitoring, SIEM und forensischer Analyse.

- Aufbau und Struktur eines Incident Response Plans
- Monitoring-Strategien & SIEM-Systeme
- Forensische Grundlagen und Spurensicherung
- Incident-Simulationen mit Auswertung

Incident Response: Praktische Umsetzung



LEKTION 7

Künstliche Intelligenz & Compliance

50 Unterrichtseinheiten

Sie verstehen die rechtlichen Rahmenbedingungen für den Einsatz von KI im Unternehmen und können KI-Anwendungen datenschutzkonform einsetzen.



KI im Compliance-Kontext

Rechtliche Grundlagen

Der sichere Umgang mit KI erfordert fundiertes Wissen über aktuelle Regulierungen:

- Einführung in die europäische KI-Verordnung (AI Act)
- Rechtliche Anforderungen und Schnittstellen zur DSGVO
- Strategische Integration von KI in Unternehmensprozesse
- Praxisbeispiele aus dem Mittelstand

Fallbeispiel-Analyse

Bewertung von KI-Anwendungen

Checkliste entwickeln

Rechtssichere KI-Einführung

Chancen & Grenzen

AI Act für KMU diskutieren



LEKTION 8

Projektarbeit & Transfer

20 Unterrichtseinheiten

Sie wenden Ihr erworbenes Wissen praktisch an und entwickeln ein eigenständiges Projekt für ein realistisches Szenario.

Ihr Abschlussprojekt



Beispiele für Projektarbeiten



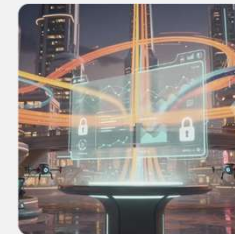
ISMS-Plan erstellen

Für ein mittelständisches Unternehmen



NIS-2-Roadmap entwickeln

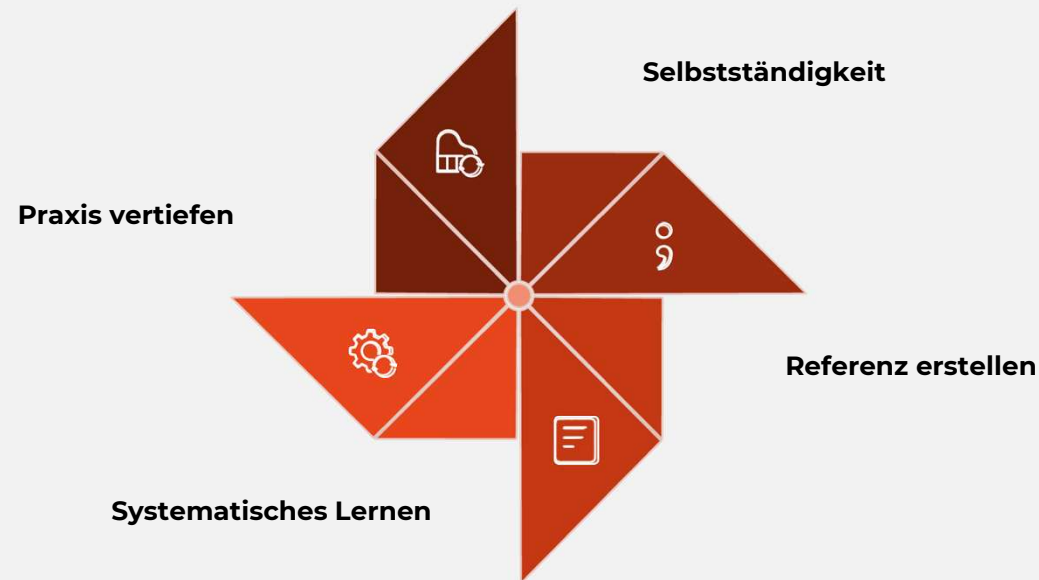
Zur Umsetzung regulatorischer Anforderungen



KI-gestützten Sicherheitsansatz konzipieren

Zur Bedrohungserkennung oder Prozessoptimierung

Nutzen der Projektarbeit



Die Projektarbeit ermöglicht eine vertiefte Auseinandersetzung mit praxisrelevanten Fragestellungen.

Was Sie gewinnen

- Selbstständiges Arbeiten trainieren
- Systematisches Vorgehen einüben
- Theoretisches Wissen in Handlungskonzepte überführen
- Argumentations- und Präsentationskompetenz stärken
- Referenzprojekt für Bewerbungen erstellen

Ihre Ziele in diesem Kurs



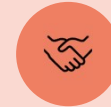
Persönliche Weiterentwicklung

Entdecken Sie Ihre Stärken und bauen Sie neue Kompetenzen auf, die Sie sowohl privat als auch beruflich weiterbringen.



Praktische Anwendung

Das Gelernte direkt umsetzen – mit konkreten Übungen und Projekten für den Alltag.



Aktiver Austausch

Profitieren Sie von gegenseitiger Unterstützung, Feedback und den Erfahrungen der Gruppe.

"Bildung ist nicht das Befüllen von Fässern, sondern das Entzünden von Flammen." – Heraklit

Ihr Kursportal – Zugang & Inhalte

Alles an einem Ort

Das Kursportal ist Ihre zentrale Anlaufstelle für alle Kursinhalte. Hier finden Sie:



Kursmaterialien

Alle Unterlagen, Präsentationen und Handouts zum Download



Video-Bibliothek

Aufzeichnungen der Live-Sessions und ergänzende Lernvideos



Aufgaben & Übungen

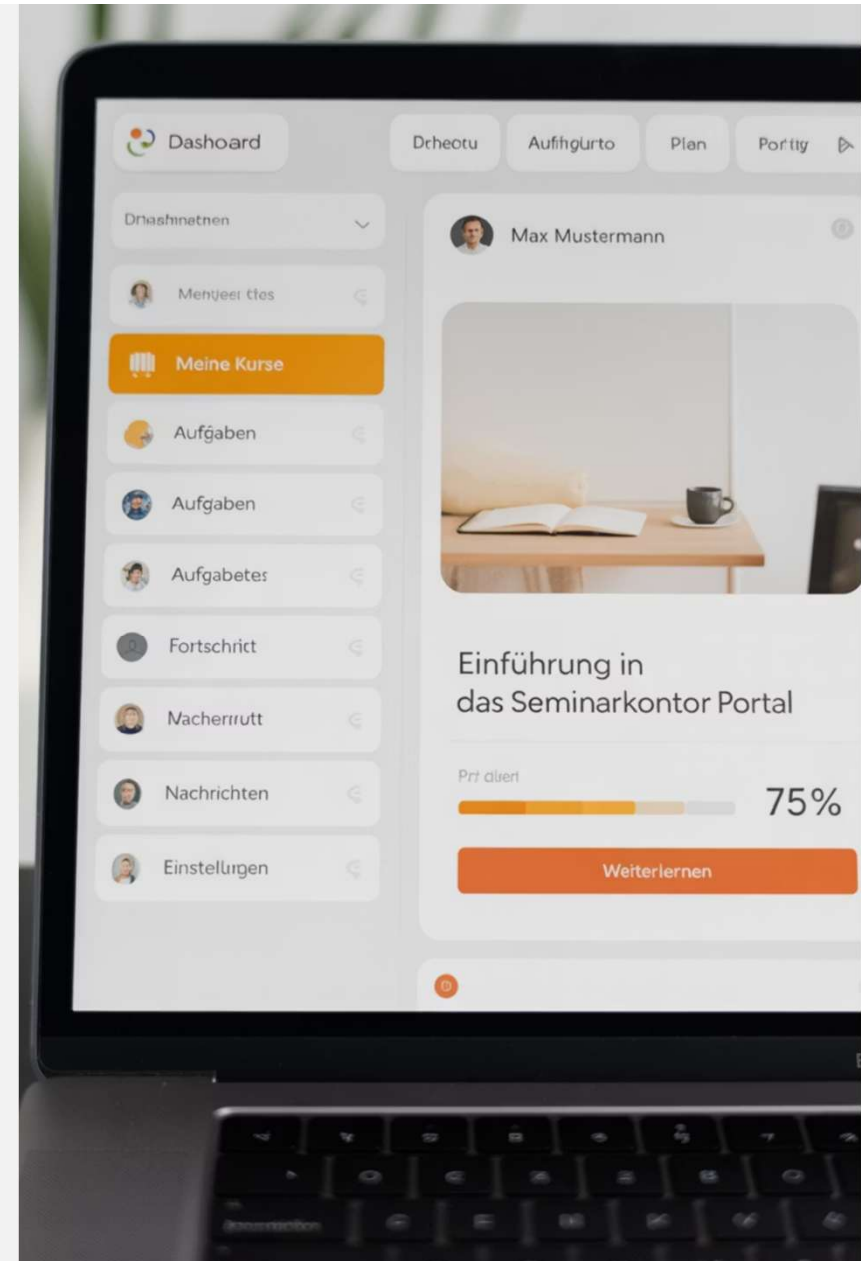
Praktische Aufgaben zur Vertiefung des Gelernten



Feedback & Support

Direkter Kontakt zu den Kursleitenden und Feedback zu Ihren Arbeiten

Tipp für den optimalen Start: Machen Sie sich gleich heute mit dem Portal vertraut und aktivieren Sie die Benachrichtigungen, damit Sie keine wichtigen Updates verpassen!



Ihre Live Sessions

Montag

9:00 – 13:00 Uhr

Live-Unterricht Präsentation zu den Lektionen, Q&A,
Präsentation der Hausarbeiten/Übungen

Hier geht es zum Montags-Kursraum:

[Jetzt an der Besprechung teilnehmen](#)

*Dazwischen: Bin ich per E-Mail oder Telefon
für Sie erreichbar*

Dienstag


9:00 – 13:00 Uhr

Live-Unterricht Präsentation zu den Lektionen, Q&A,
Präsentation der Hausarbeiten/Übungen

Einzelcoaching für individuelle Fragen und persönliche
Entwicklungsgespräche

Hier geht es zum Dienstags-Kursraum:

[Jetzt an der Besprechung teilnehmen](#)

-  Planen Sie sich die Termine am besten direkt fest in Ihren Kalender ein – die Live-Sessions werden nicht aufgezeichnet.

Ihr Dozent

Tobias Apel

Senior IT-Sicherheitsberater / Geschäftsführer

apro.gmbh – Erfurter Landstraße 9/10 –
99095 Erfurt

Tel.: [+49 36204 1248 11](tel:+4936204124811)

E-Mail: apel@apro.gmbh

[Termine buchen Sie direkt online](#)

URL: www.apro.gmbh

