Schatten IT & Shadow AI: Erkennung, Risiken und KI-Sicherheit für Unternehmen.

Zwei-Tages-Kurs für IT-Experten: Schatten IT und Shadow AI erkennen, analysieren und mit wirksamen Maßnahmen absichern.

Seminar	9 Termine verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	16 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 29230

Stand: 23.09.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29230

Schatten IT entsteht, wenn KI-Dienste, SaaS-Anwendungen, Browser-Erweiterungen oder weitere Tools außerhalb der kontrollierten IT-Infrastruktur genutzt werden. Das Seminar zeigt praxisnah, wie Sie Schatten-IT- und Shadow-AI-Aktivitäten erkennen, Risiken bewerten und mit CASB, DLP, EDR, Zero Trust sowie sicheren Enterprise-AI-Strukturen absichern.

Nutzen

• Sie erkennen typische Formen von Schatten IT und Shadow AI in Browser-, SaaS-, API- und Endpoint-Umgebungen.
• Sie analysieren verdächtige Nutzungsmuster in Proxy-, Firewall-, SIEM- und Identity-Daten systematisch und bewerten daraus entstehende Schatten IT Risiken.
• Sie verstehen, warum klassische Sicherheitsmechanismen bei verschlüsseltem KI-Traffic und externen LLM-Diensten nur eingeschränkt greifen.
• Sie identifizieren Risiken durch unautorisierte OAuth-Freigaben, Browser-Erweiterungen und nicht genehmigte KI-Wrapper.
• Sie lernen, wie sich sensible Datenabflüsse über generative KI mit CASB-, DLP-, EDR- und Zero-Trust-Maßnahmen technisch eindämmen lassen.
• Sie erhalten praxisnahe Ansätze für Incident-Response- und SOAR-Workflows bei Shadow-AI-Vorfällen.

Zielgruppe

Das Seminar richtet sich an IT- und Security-Experten mit fortgeschrittenen technischen Kenntnissen, die Schatten IT und Shadow AI erkennen, analysieren und wirksam eindämmen möchten – z. B. IT-Security-Spezialisten, SOC-Analysten, Netzwerk- und Systemadministratoren, Cloud-Security-Spezialisten, Incident-Response-Spezialisten, IT-Architekten oder DevSecOps-Experten. Ebenso richtet sich der Kurs an leitende IT- und Informationssicherheitsverantwortliche, Security Architects, ISOs und CISOs, die sichere Enterprise-KI-Strukturen etablieren und bestehende Sicherheitsarchitekturen um KI- und Cloud-spezifische Schutzmechanismen erweitern möchten.

Voraussetzungen

Teilnehmende sollten über grundlegende Kenntnisse in der Nutzung und im Betrieb von KI-Systemen sowie von Cloud- und SaaS-Diensten verfügen. Offenheit für digitale Themen und Interesse an neuen Arbeitsweisen mit KI und Cloud sind von Vorteil.

Abschluss

Teilnahmebescheinigung

Sie erhalten eine Teilnahmebescheinigung der TÜV Rheinland Akademie GmbH.

Inhalte des Seminars

Tag 1: Schatten IT & Shadow AI erkennen und bewerten (Detection & Visibility)

Schatten IT und Shadow AI als Informationssicherheitsrisiko
• Abgrenzung von Schatten IT, Shadow SaaS und Shadow AI sowie typische Nutzungsszenarien.
• Risiken für sensible Daten, Geschäftsgeheimnisse, Identitäten und geistiges Eigentum.
• Bedeutung für ISMS sowie Rollen und Verantwortlichkeiten von IT- und Security-Fachkräften, ISO und CISO.

Risikoanalyse & Governance
• Identifikation, Bewertung und Behandlung von Shadow-AI- und Shadow-IT-Risiken.
• Richtlinien, Freigabeprozesse und Verantwortlichkeiten für KI- und SaaS-Dienste.

Detection & Visibility
• Erkennung nicht autorisierter KI- und SaaS-Dienste über Proxy, Firewall, CASB/SSE, EDR, SIEM, Least Privilege und Least Cability.

• Analyse von OAuth-Berechtigungen, Browser-Erweiterungen und API-Kommunikation.

Praxis: Analyse von Shadow-AI-Aktivitäten
• Analyse ausgewählter Log- und Security-Ereignisse.
• Risikobewertung und Ableitung geeigneter Maßnahmen und Eskalationswege.

Tag 2: Shadow AI absichern & Enterprise AI etablieren (Containment & Architecture)

Prävention & technische Schutzmaßnahmen
• Einsatz von CASB/SSE, DLP, EDR und Application Control zur Kontrolle nicht autorisierter KI-Dienste.
• Netzwerk-, Endpoint- und identitätsbasierte Kontrollen nach Zero-Trust-Prinzipien.

Managed Enterprise AI
• Aufbau kontrollierter Alternativen zu Shadow AI: Enterprise-LLMs, sichere APIs, AI Gateways und lokale Modelle.
• Security-by-Design, IAM, Datenklassifizierung und Logging für KI-Anwendungen.

Incident Response bei Shadow-AI-Vorfällen
• Vorgehen bei Abfluss von Sourcecode, personenbezogenen Daten oder Geschäftsgeheimnissen.
• Zusammenspiel von SOC, ISO, CISO, Datenschutz und Management bei Erkennung, Eindämmung und Aufarbeitung.

Shadow-AI-Security aus Sicht von IT- und Security-Fachkräften, ISO & CISO
• Aufbau eines nachhaltigen Kontroll- und Governance-Modells für Shadow AI und Schatten IT.
• Integration in ISMS, Risikomanagement, Security Monitoring und Management-Reporting.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29230 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.