AICCI AI Security Analyst

3 Tage Intensivschulung mit Zertifizierungsmöglichkeit (AICCI)

Der **AI Security Analyst** Kurs vermittelt die Fähigkeiten, KI-gestützte Systeme zu analysieren, Bedrohungen zu erkennen und gezielt Gegenmaßnahmen zu entwickeln. Teilnehmende lernen, wie sich Security-by-Design in den KI-Entwicklungsprozess integrieren lässt, welche regulatorischen Anforderungen zu beachten sind und wie ein effektives Incident Response für KI-Systeme aussieht. So werden sie zur zentralen Schnittstelle zwischen Cybersecurity und KI-Entwicklung.

Zielgruppe
Die Schulung richtet sich an (angehende) KI-Beauftragte und AI Compliance Officer, an KI-Koordinatorinnen und -Manager sowie an Mitarbeitende, die ein KI-Managementsystem einführen oder betreiben. Darüber hinaus spricht sie Fach- und Führungskräfte an, die einen rechtssicheren und verantwortungsvollen Umgang mit KI etablieren möchten.

Voraussetzungen
Die Teilnahme setzt keine besonderen Voraussetzungen voraus.
Empfohlen: Erfahrung mit IT-Infrastruktur und/oder Anwendungssicherheit.
Ein vorheriger Besuch der AICCI AI Foundation erleichtert den Einstieg.

Sprache
Deutsch oder Englisch

Format
Online oder Inhouse
(auf Anfrage)

Zertifizierung (optional)
AICCI
"AI Security Analyst"

Modul 1 - Einführung in KI-Sicherheit
- ✓ Überblick: KI-Technologien und ihre sicherheitsrelevanten Besonderheiten
- ✓ Unterschiede zwischen klassischer IT-Security und KI-Security
- ✓ Bedrohungsmodelle für KI-Systeme
- ✓ Aktuelle Fallbeispiele für KI-Sicherheitsvorfälle

Modul 2 - Angriffsarten auf KI-Systeme
- ✓ Datenmanipulation & Data Poisoning
- ✓ Adversarial Attacks (z. B. Bild- und Texterkennung täuschen)
- ✓ Modell-Extraktion & Modell-Inversion
- ✓ Prompt Injection & Jailbreaks bei generativen Modellen
- ✓ Supply-Chain-Angriffe in KI-Entwicklungsumgebungen

Modul 3 - Security-by-Design für KI
- ✓ Sicherheitsanforderungen im KI-Entwicklungsprozess verankern
- ✓ Datenschutz- und Compliance-Aspekte berücksichtigen
- ✓ Sicheres Datenmanagement (Data Governance, Zugriffskontrollen, Verschlüsselung)
- ✓ Integration in bestehende Sicherheitsarchitekturen

Modul 4 - Sicherheitsstandards & ISO/IEC 42001
- ✓ Überblick: ISO/IEC 42001 (AI Management System) und sicherheitsrelevante Anforderungen
- ✓ Verbindung zu ISO/IEC 27001 (Informationssicherheitsmanagement)
- ✓ NIST AI Risk Management Framework
- ✓ Regulatorische Vorgaben (EU AI Act, branchenspezifische Standards)

Modul 5 - Incident Detection & Response für KI
- ✓ Monitoring von KI-Systemen im Betrieb
- ✓ Erkennen und Melden von Angriffen
- ✓ Incident-Response-Pläne für KI-bezogene Vorfälle
- ✓ Forensische Analyse und Lessons Learned

Modul 6 - Zukunftstrends & Emerging Threats
- ✓ Automatisierte Angriffe mit KI
- ✓ KI-gestützte Abwehrsysteme (Defensive AI)
- ✓ Ethische und geopolitische Aspekte von KI-Security
- ✓ Prognosen zu Sicherheitsstandards und Best Practices

Praxis-Workshop
- ✓ 3 Praktische Übungen
- ✓ Diskussionsrunde

Prüfungsvorbereitung
- ✓ Musterprüfung

AICCI

Bactrya

Aktuelle Termine und weitere Informationen finden Sie hier:
https://www.bactrya.com/trainings/aicci-ai-security-analyst