AI-Security Engineer (m./w./d.)

BERUFSBESCHREIBUNG

Mit der zunehmenden Nutzung von Künstlicher Intelligenz (KI) in sicherheitskritischen Bereichen wie z. B. Finanzdienstleistungen, Gesundheitswesen oder öffentlicher Verwaltung gewinnt die Sicherheit von KI-Systemen stark an Bedeutung. Neben klassischen Bereichen der Informationssicherheit müssen dabei auch KI-spezifischen Bedrohungen berücksichtigt werden.

AI-Security Engineers (m./w./d.) schützen KI-Systeme, Modelle, Datenbestände und die zugrundeliegende Infrastruktur vor Angriffen und Manipulationen. Ihr Ziel ist es, Risiken frühzeitig zu erkennen und technische und organisatorische Schutzmaßnahmen zu entwickeln. Dazu analysieren sie potenzielle Bedrohungen wie Data Poisoning, Model Theft, Prompt Injection, Datenlecks oder andere Angriffe auf KI-Systeme.

Zu ihren Aufgaben zählen insbesondere:

- Schwachstellen von KI-Modelle und KI-Pipelines analysieren
- Bedrohungen modellieren und Risiko bewerten
- Robustheit und Sicherheit von KI-Anwendungen testen
- Schutzmaßnahmen entwickeln und umsetzen
- produktive KI-Systeme überwachen
- Notfall- und Reaktionspläne für Sicherheitsvorfälle entwickeln
- bei Complaince und Governance-Anforderungen unterstützen

AI-Security Engineers identifizieren bereits während der Entwicklung und des Trainings von KI-Modellen potenziell Risiken und tragen dazu bei, deren Sicherheit, Robustheit und Vertrauenswürdigkeit zu erhöhen. Sie arbeiten dazu eng mit Cybersecurity-Spezialist*innen, Softwareentwickler*innen, Data Scientists (m./w./d.) und IT-Architekt*innen zusammen.

Sie arbeiten in für Unternehmen, die KI-Lösungen entwickeln oder direkt in Banken, Versicherungen, öffentlichen Einrichtungen sowie Unternehmen aller Branchen, die datenintensive oder sicherheitskritische KI-Systeme einsetzen.

Ausbildung

Für den Beruf AI-Security Engineer (m./w./d.) ist in der Regel ein abgeschlossenes Universitäts- oder Fachhochschulstudium erforderlich, beispielsweise in den Bereichen Informatik, Softwareentwicklung, Data Science, Künstliche Intelligenz/Artificial Intelligence, Cyber Security usw.

© ibw-Institut für Bildungsforschung der Wirtschaft