CAS AI powered CyberTech

Future Skills: Mastering AI Safety, Prompt Engineering und AI-Assessments

AI befeuert den Kampf zum Schutz von digitalen Werten. ICT-Fachkräfte müssen mit den Angreifern mithalten und setzen AI geschickt für die Abwehr von Attacken ein.

Tauchen Sie ein in die Welt der Künstlichen Intelligenz und des Machine Learning, verstehen Sie deren Einfluss auf die Cybersicherheit und werden Sie Expert*in in AI Safety. Lernen Sie, AI-basierte Cybersecurity-Technologien strategisch zu bewerten, erkennen und beurteilen Sie die Risiken von KI-unterstützten Angriffen. Dieser Lehrgang rüstet Sie mit dem Wissen aus, um Cloud- und Datensicherheitsmaßnahmen im Zeitalter der KI zu beurteilen und führt Sie in die fortschrittlichen Methoden der AI-gestützten IT-Forensik ein. Machen Sie den nächsten Schritt und führen Sie Ihre Organisation sicher in die digitale Zukunft.

Ziele

Die Absolventinnen und Absolventen…

- kennen die Grundlagen und Funktionsweise von AI/ML/DL und wenden diese im Kontext von Artificial Intelligence Safety und Cybersecurity an.
- kennen strategische Methoden und Modelle zur Bewertung von neuen AI getriebenen Cybersecurity Technologien.
- kennen und beurteilen Cloud- und Data-Security unter dem Aspekt AI.
- kennen und beurteilen aktuelle AI gestützte Hacking-Methoden.
- kennen und bewerten die Gefahren durch Angriffe auf AI-Applikationen.
- kennen und beurteilen AI gestützte Methoden der IT-Forensik.

Inhalte	**Modul 1: AI Safety & Trust** Begrifflichkeiten wie AI, ML, Deep Learning etc., Prompt Engineering EU AI Act, OECD AI Principles, SAE J3016, AI-Compliance/Datenschutz Roboter- und Maschinenethik, Zero Trust Network Access ZTNA Risk & Security Management: IT und EmTech **Modul 2: AI CyberTech Assessment** Cyber Security Framework: Integration von AI und weiteren Technologien Cyber Defence Center: Integration und Automatisierung mit AI Continuous Threat Exposure Management (CTEM) Predictive Security Analytics, Machine Learning in Threat Intelligence **Modul 3: Cloud-Security & Data-Security** CASB und AI / SASE und AI Intelligente Netzwerksicherheit in hybriden Clouds IAM, CIAM und Re-Authentisierung mit AI, DRM und DLD mit AI AI-gestützte Kryptoanalyse und Quantum Machine Learning (QML) **Modul 4: AI Hacking** AI-gesteuertes Hacking, Social Engineering & Deep Fakes Mobile-Device und IoT Hacking, Attack AI und Hacking der AI Secure Streaming, Netzwerk-Kameras, NGAM (ML-basiert), Drohnen Demo von AI-getriebenen Hacking-Angriffen **Modul 5: IT-Forensik** Digitale Forensik mit AI und AI Cybercrime Detection AI-gestützte Strafverfolgung im Internet und AI Cyberforensik Forensische Cloud- und Daten-Analyse mit AI, Rapportierung Maschinelles Lernen für IKT-Integritätsprüfungen
Zielpublikum	Chief Informationsecurity Officer IT-Security Fachkräfte ICT Fach- und Führungskräfte
Abschluss	CAS AI powered CyberTech / 15 ECTS-Credits
Daten	Start: 3. März 2025 Ende: 3. Juli 2025
Ort	Campus Brugg-Windisch und Online
Kosten	CHF 7500.- / Preisänderung ab 1. Januar 2025.
Programmleitung	Prof. Martina Dalla Vecchia martina.dallavecchia@fhnw.ch
Co-Leitung	Rainer Kessler rainer.kessler@fhnw.ch
Koordination	Franziska Toth franziska.toth@fhnw.ch