Weiterbildender Masterstudiengang

Künstliche Intelligenz in der Cybersicherheit

tech global university

tech global university

Weiterbildender Masterstudiengang
Künstliche Intelligenz in der Cybersicherheit

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Global University**
- Akkreditierung: **90 ECTS**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: **www.techtitute.com/de/kunstliche-intelligenz/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-kunstliche-intelligenz-cybersicherheit**

Index

01

Präsentation des Programms

Die Cybersicherheit hat sich in den letzten Jahren aufgrund der zunehmenden Komplexität der Cyber-Bedrohungen erheblich verändert. Angesichts der zunehmenden Zahl ausgefeilter Angriffe sind herkömmliche Verteidigungstechniken unzureichend. In diesem Zusammenhang hat sich die künstliche Intelligenz als grundlegendes Instrument zur Verbesserung der Erkennung von Angriffen, der Vorhersage von Bedrohungen und der Reaktion auf Vorfälle erwiesen. Daher müssen Experten die ausgefeiltesten Techniken des maschinellen Lernens beherrschen, um die digitale Infrastruktur von Organisationen zu schützen. Um ihnen diese Arbeit zu erleichtern, führt TECH einen innovativen Universitätsabschluss ein, der sich auf den Einsatz von künstlicher Intelligenz in der Cybersicherheit konzentriert. Und das alles im bequemen Online-Modus!

Dank dieses zu 100% online angebotenen weiterbildenden Masterstudiengangs werden Sie robuste Schutzsysteme auf der Grundlage künstlicher Intelligenz entwickeln, um die Privatsphäre und Authentizität von Daten zu gewährleisten“

Laut einem neuen Bericht der Vereinten Nationen waren Unternehmen im vergangenen Jahr mehr als 50 Millionen Cyberangriffen ausgesetzt, was einem Anstieg von 50% gegenüber dem Vorjahr entspricht. Vor diesem Hintergrund spielt die künstliche Intelligenz eine entscheidende Rolle bei der Weiterentwicklung der Cybersicherheit. Beispielsweise ermöglichen Technologien wie maschinelles Lernen und prädiktive Analytik Unternehmen, potenzielle Bedrohungen zu erkennen, bevor sie eintreten. In diesem Szenario benötigen Fachleute ein umfassendes Verständnis der Anwendungen intelligenter Systeme, um den digitalen Schutz zu optimieren.

Vor diesem Hintergrund bietet TECH einen hochmodernen Weiterbildenden Masterstudiengang in Künstliche Intelligenz für Cybersicherheit an. Der von Spezialisten auf diesem Gebiet konzipierte Studiengang wird sich mit Themen befassen, die vom Datenlebenszyklus oder innovativen Techniken des maschinellen Lernens bis hin zur Verwendung von Software der neuesten Generation wie TensorFlow reichen. Auf diese Weise erwerben die Studenten fortgeschrittene Fähigkeiten, um prädiktive Analysetechniken zu integrieren, digitale Infrastrukturen gegen ausgefeilte Angriffe zu stärken und multidisziplinäre Teams bei der Schaffung autonomer Sicherheitssysteme zu leiten.

Was die Methodik dieses Universitätsprogramms betrifft, so stützt sich TECH auf ihr revolutionäres *Relearning*-System. Diese Methode besteht in der schrittweisen Wiederholung der wichtigsten Konzepte, um sicherzustellen, dass die Absolventen ein umfassendes Verständnis der wesentlichen Inhalte des Lehrplans erlangen. Darüber hinaus benötigen die Fachkräfte für den Zugang zu allen Lernressourcen lediglich ein elektronisches Gerät mit Internetanschluss (z. B. Mobiltelefon, Tablet oder Computer). Sie werden also auf den virtuellen Campus zugreifen und eine immersive Erfahrung machen können, die es ihnen ermöglicht, ihre tägliche klinische Praxis deutlich zu optimieren.

Dieser **Weiterbildender Masterstudiengang in Künstliche Intelligenz in der Cybersicherheit** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für künstliche Intelligenz in der Cybersicherheit vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren wissenschaftlichen und praktischen Informationen
- Praktische Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens genutzt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Lektionen, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugangs zu Inhalten von jedem festen oder tragbaren Gerät mit Internetanschluss

> *Sie werden Techniken der künstlichen Intelligenz einsetzen, um Angriffe und Betrug zu verhindern“*

Sie werden Ihre strategische Entscheidungsfindung durch prädiktive Analysen und den Einsatz fortschrittlicher Modelle beim Management von Cyberangriffen optimieren“

Sie werden Sicherheitsvorfälle mithilfe künstlicher Intelligenz effizient verwalten.

Das bahnbrechende Relearning-System von TECH reduziert die langen Lernzeiten, die bei anderen Lehrmethoden so häufig vorkommen. Sie werden Spaß am progressiven Lernen haben!

Der Lehrkörper des Programms besteht aus Experten des Sektors, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie aus renommierten Fachkräften von führenden Gesellschaften und angesehenen Universitäten.

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

02

Warum an der TECH studieren?

TECH ist die größte digitale Universität der Welt. Mit einem beeindruckenden Katalog von über 14.000 Hochschulprogrammen, die in 11 Sprachen angeboten werden, ist sie mit einer Vermittlungsquote von 99% führend im Bereich der Beschäftigungsfähigkeit. Darüber hinaus verfügt sie über einen beeindruckenden Lehrkörper mit mehr als 6.000 Professoren von höchstem internationalem Prestige.

Studieren Sie an der größten digitalen Universität der Welt und sichern Sie sich Ihren beruflichen Erfolg. Die Zukunft beginnt bei TECH“

Die beste Online-Universität der Welt laut FORBES

Das renommierte, auf Wirtschaft und Finanzen spezialisierte Magazin Forbes hat TECH als „beste Online-Universität der Welt" ausgezeichnet. Dies wurde kürzlich in einem Artikel in der digitalen Ausgabe des Magazins festgestellt, in dem die Erfolgsgeschichte dieser Einrichtung „dank ihres akademischen Angebots, der Auswahl ihrer Lehrkräfte und einer innovativen Lernmethode, die auf die Ausbildung der Fachkräfte der Zukunft abzielt", hervorgehoben wird.

Die besten internationalen Top-Lehrkräfte

Der Lehrkörper der TECH besteht aus mehr als 6.000 Professoren von höchstem internationalen Ansehen. Professoren, Forscher und Führungskräfte multinationaler Unternehmen, darunter Isaiah Covington, Leistungstrainer der Boston Celtics, Magda Romanska, leitende Forscherin am Harvard MetaLAB, Ignacio Wistumba, Vorsitzender der Abteilung für translationale Molekularpathologie am MD Anderson Cancer Center, und D.W. Pine, Kreativdirektor des TIME Magazine, um nur einige zu nennen.

Die größte digitale Universität der Welt

TECH ist die weltweit größte digitale Universität. Wir sind die größte Bildungseinrichtung mit dem besten und umfangreichsten digitalen Bildungskatalog, der zu 100% online ist und die meisten Wissensgebiete abdeckt. Wir bieten weltweit die größte Anzahl eigener Abschlüsse sowie offizieller Grund- und Aufbaustudiengänge an. Insgesamt sind wir mit mehr als 14.000 Hochschulabschlüssen in elf verschiedenen Sprachen die größte Bildungseinrichtung der Welt.

Die umfassendsten Lehrpläne in der Universitätslandschaft

TECH bietet die vollständigsten Lehrpläne in der Universitätslandschaft an, mit Lehrplänen, die grundlegende Konzepte und gleichzeitig die wichtigsten wissenschaftlichen Fortschritte in ihren spezifischen wissenschaftlichen Bereichen abdecken. Darüber hinaus werden diese Programme ständig aktualisiert, um den Studenten die akademische Avantgarde und die gefragtesten beruflichen Kompetenzen zu garantieren. Auf diese Weise verschaffen die Abschlüsse der Universität ihren Absolventen einen bedeutenden Vorteil, um ihre Karriere erfolgreich voranzutreiben.

Eine einzigartige Lernmethode

TECH ist die erste Universität, die *Relearning* in allen ihren Studiengängen einsetzt. Es handelt sich um die beste Online-Lernmethodik, die mit internationalen Qualitätszertifikaten renommierter Bildungseinrichtungen ausgezeichnet wurde. Darüber hinaus wird dieses disruptive akademische Modell durch die „Fallmethode" ergänzt, wodurch eine einzigartige Online-Lehrstrategie entsteht. Es werden auch innovative Lehrmittel eingesetzt, darunter ausführliche Videos, Infografiken und interaktive Zusammenfassungen.

Die offizielle Online-Universität der NBA

TECH ist die offizielle Online-Universität der NBA. Durch eine Vereinbarung mit der größten Basketball-Liga bietet sie ihren Studenten exklusive Universitätsprogramme sowie eine breite Palette von Bildungsressourcen, die sich auf das Geschäft der Liga und andere Bereiche der Sportindustrie konzentrieren. Jedes Programm hat einen einzigartig gestalteten Lehrplan und bietet außergewöhnliche Gastredner: Fachleute mit herausragendem Sporthintergrund, die ihr Fachwissen zu den wichtigsten Themen zur Verfügung stellen.

Führend in Beschäftigungsfähigkeit

TECH ist es gelungen, die führende Universität im Bereich der Beschäftigungsfähigkeit zu werden. 99% der Studenten finden innerhalb eines Jahres nach Abschluss eines Studiengangs der Universität einen Arbeitsplatz in dem von ihnen studierten Fachgebiet. Ähnlich viele erreichen einen unmittelbaren Karriereaufstieg. All dies ist einer Studienmethodik zu verdanken, die ihre Wirksamkeit auf den Erwerb praktischer Fähigkeiten stützt, die für die berufliche Entwicklung absolut notwendig sind.

Google Partner Premier

Der amerikanische Technologieriese hat TECH mit dem Logo Google Partner Premier ausgezeichnet. Diese Auszeichnung, die nur 3% der Unternehmen weltweit erhalten, unterstreicht die effiziente, flexible und angepasste Erfahrung, die diese Universität den Studenten bietet. Die Anerkennung bestätigt nicht nur die maximale Präzision, Leistung und Investition in die digitalen Infrastrukturen der TECH, sondern positioniert diese Universität auch als eines der modernsten Technologieunternehmen der Welt.

Die von ihren Studenten am besten bewertete Universität

Die Studenten haben TECH auf den wichtigsten Bewertungsportalen als die am besten bewertete Universität der Welt eingestuft, mit einer Höchstbewertung von 4,9 von 5 Punkten, die aus mehr als 1.000 Bewertungen hervorgeht. Diese Ergebnisse festigen die Position der TECH als internationale Referenzuniversität und spiegeln die Exzellenz und die positiven Auswirkungen ihres Bildungsmodells wider.

03

Lehrplan

Die Lehrmaterialien dieses Studiengangs werden die Grundlagen der künstlichen Intelligenz im Bereich der Cybersicherheit vertiefen. Auf diese Weise wird der Lehrplan Bereiche wie *Data Mining*, Algorithmentraining und fortgeschrittene Techniken der Verarbeitung natürlicher Sprache behandeln. Dadurch werden die Studenten fortgeschrittene Fähigkeiten entwickeln, um autonome Sicherheitssysteme zu entwerfen, Präventionslösungen auf der Grundlage des maschinellen Lernens zu implementieren und neue Technologien zum Schutz digitaler Infrastrukturen anzuwenden.

Sie werden Sicherheitsvorschriften und -standards in der Cybersicherheit anwenden, wodurch Sie die Einhaltung der geltenden internationalen Vorschriften sicherstellen können"

Modul 1. Grundlagen der künstlichen Intelligenz

1.1. Geschichte der künstlichen Intelligenz
- 1.1.1. Ab wann spricht man von künstlicher Intelligenz?
- 1.1.2. Referenzen im Film
- 1.1.3. Bedeutung der künstlichen Intelligenz
- 1.1.4. Technologien, die künstliche Intelligenz ermöglichen und unterstützen

1.2. Künstliche Intelligenz in Spielen
- 1.2.1. Spieltheorie
- 1.2.2. *Minimax* und Alpha-Beta-Beschneidung
- 1.2.3. Simulation: Monte Carlo

1.3. Neuronale Netzwerke
- 1.3.1. Biologische Grundlagen
- 1.3.2. Berechnungsmodell
- 1.3.3. Überwachte und nicht überwachte neuronale Netzwerke
- 1.3.4. Einfaches Perzeptron
- 1.3.5. Mehrlagiges Perzeptron

1.4. Genetische Algorithmen
- 1.4.1. Geschichte
- 1.4.2. Biologische Grundlage
- 1.4.3. Problem-Kodierung
- 1.4.4. Erzeugung der Ausgangspopulation
- 1.4.5. Hauptalgorithmus und genetische Operatoren
- 1.4.6. Bewertung von Personen: Fitness

1.5. Thesauri, Vokabularien, Taxonomien
- 1.5.1. Wortschatz
- 1.5.2. Taxonomie
- 1.5.3. Thesauri
- 1.5.4. Ontologien
- 1.5.5. Wissensrepräsentation: Semantisches Web

1.6. Semantisches Web
- 1.6.1. Spezifizierungen: RDF, RDFS und OWL
- 1.6.2. Schlussfolgerung/Begründung
- 1.6.3. *Linked Data*

1.7. Expertensysteme und DSS
- 1.7.1. Expertensysteme
- 1.7.2. Systeme zur Entscheidungshilfe

1.8. *Chatbots* und virtuelle Assistenten
- 1.8.1. Arten von Assistenten: sprach- und textbasierte Assistenten
- 1.8.2. Grundlegende Bestandteile für die Entwicklung eines Assistenten: *Intents*, Entitäten und Dialogablauf
- 1.8.3. Integrationen: Web, *Slack*, Whatsapp, Facebook
- 1.8.4. Tools für die Entwicklung von Assistenten: *Dialog Flow*, *Watson Assistant*

1.9. Strategie zur Implementierung der künstlichen Intelligenz

1.10. Die Zukunft der künstlichen Intelligenz
- 1.10.1. Wir wissen, wie man mit Algorithmen Emotionen erkennt
- 1.10.2. Eine Persönlichkeit schaffen: Sprache, Ausdrücke und Inhalt
- 1.10.3. Tendenzen der künstlichen Intelligenz
- 1.10.4. Reflexionen

Modul 2. Datentypen und Datenlebenszyklus

2.1. Die Statistik
- 2.1.1. Statistik: Deskriptive Statistik, statistische Schlussfolgerungen
- 2.1.2. Population, Stichprobe, Individuum
- 2.1.3. Variablen: Definition und Mess-Skalen

2.2. Arten von statistischen Daten
- 2.2.1. Je nach Typ
  - 2.2.1.1. Quantitativ: kontinuierliche Daten und diskrete Daten
  - 2.2.1.2. Qualitativ: Binomialdaten, nominale Daten und ordinale Daten
- 2.2.2. Je nach Form
  - 2.2.2.1. Numerisch
  - 2.2.2.2. Text
  - 2.2.2.3. Logisch
- 2.2.3. Je nach Quelle
  - 2.2.3.1. Primär
  - 2.2.3.2. Sekundär

2.3. Lebenszyklus der Daten
  2.3.1. Etappen des Zyklus
  2.3.2. Meilensteine des Zyklus
  2.3.3. FAIR-Prinzipien
2.4. Die ersten Phasen des Zyklus
  2.4.1. Definition von Zielen
  2.4.2. Ermittlung des Ressourcenbedarfs
  2.4.3. Gantt-Diagramm
  2.4.4. Struktur der Daten
2.5. Datenerhebung
  2.5.1. Methodik der Erhebung
  2.5.2. Erhebungsinstrumente
  2.5.3. Kanäle für die Erhebung
2.6. Datenbereinigung
  2.6.1. Phasen der Datenbereinigung
  2.6.2. Qualität der Daten
  2.6.3. Datenmanipulation (mit R)
2.7. Datenanalyse, Interpretation und Bewertung der Ergebnisse
  2.7.1. Statistische Maßnahmen
  2.7.2. Beziehungsindizes
  2.7.3. *Data Mining*
2.8. Datenlager (*Datawarehouse*)
  2.8.1. Elemente, aus denen sie bestehen
  2.8.2. Design
  2.8.3. Zu berücksichtigende Aspekte
2.9. Verfügbarkeit von Daten
  2.9.1. Zugang
  2.9.2. Nutzen
  2.9.3. Sicherheit
2.10. Regulatorische Aspekte
  2.10.1. Datenschutzgesetz
  2.10.2. Bewährte Verfahren
  2.10.3. Andere regulatorische Aspekte

Modul 3. Daten in der künstlichen Intelligenz

3.1. Datenwissenschaft
  3.1.1. Datenwissenschaft
  3.1.2. Fortgeschrittene Tools für den Datenwissenschaftler
3.2. Daten, Informationen und Wissen
  3.2.1. Daten, Informationen und Wissen
  3.2.2. Datentypen
  3.2.3. Datenquellen
3.3. Von Daten zu Informationen
  3.3.1. Datenanalyse
  3.3.2. Arten der Analyse
  3.3.3. Extraktion von Informationen aus einem *Dataset*
3.4. Extraktion von Informationen durch Visualisierung
  3.4.1. Visualisierung als Analyseinstrument
  3.4.2. Visualisierungsmethoden
  3.4.3. Visualisierung eines Datensatzes
3.5. Qualität der Daten
  3.5.1. Datenqualität
  3.5.2. Datenbereinigung
  3.5.3. Grundlegende Datenvorverarbeitung
3.6. *Dataset*
  3.6.1. *Dataset*-Anreicherung
  3.6.2. Der Fluch der Dimensionalität
  3.6.3. Ändern unseres Datensatzes
3.7. Ungleichgewicht
  3.7.1. Ungleichgewicht der Klassen
  3.7.2. Techniken zur Begrenzung von Ungleichgewichten
  3.7.3. *Dataset*-Abgleich
3.8. Unüberwachte Modelle
  3.8.1. Unüberwachtes Modell
  3.8.2. Methoden
  3.8.3. Klassifizierung mit unüberwachten Modellen

3.9. Überwachte Modelle
- 3.9.1. Überwachtes Modell
- 3.9.2. Methoden
- 3.9.3. Klassifizierung mit überwachten Modellen

3.10. Tools und bewährte Verfahren
- 3.10.1. Bewährte Praktiken für einen Datenwissenschaftler
- 3.10.2. Das beste Modell
- 3.10.3. Nützliche Tools

Modul 4. *Data Mining*. Auswahl, Vorverarbeitung und Transformation

4.1. Statistische Inferenz
- 4.1.1. Deskriptive Statistik vs. statistische Inferenz
- 4.1.2. Parametrische Verfahren
- 4.1.3. Nichtparametrische Verfahren

4.2. Explorative Analyse
- 4.2.1. Deskriptive Analyse
- 4.2.2. Visualisierung
- 4.2.3. Vorbereitung der Daten

4.3. Vorbereitung der Daten
- 4.3.1. Datenintegration und -bereinigung
- 4.3.2. Normalisierung der Daten
- 4.3.3. Attribute umwandeln

4.4. Verlorene Werte
- 4.4.1. Umgang mit verlorenen Werten
- 4.4.2. *Maximum-Likelihood*-Imputationsmethoden
- 4.4.3. Imputation verlorener Werte durch maschinelles Lernen

4.5. Datenrauschen
- 4.5.1. Lärmklassen und Attribute
- 4.5.2. Rauschfilterung
- 4.5.3. Rauscheffekt

4.6. Der Fluch der Dimensionalität
- 4.6.1. *Oversampling*
- 4.6.2. *Undersampling*
- 4.6.3. Multidimensionale Datenreduktion

4.7. Kontinuierliche zu diskreten Attributen
- 4.7.1. Kontinuierliche versus diskrete Daten
- 4.7.2. Prozess der Diskretisierung

4.8. Daten
- 4.8.1. Datenauswahl
- 4.8.2. Perspektiven und Auswahlkriterien
- 4.8.3. Methoden der Auswahl

4.9. Auswahl der Instanzen
- 4.9.1. Methoden für die Instanzauswahl
- 4.9.2. Auswahl von Prototypen
- 4.9.3. Erweiterte Methoden für die Instanzauswahl

4.10. Vorverarbeitung von Daten in *Big-Data*-Umgebungen

Modul 5. Algorithmik und Komplexität in der künstlichen Intelligenz

5.1. Einführung in Algorithmus-Design-Strategien
- 5.1.1. Rekursion
- 5.1.2. Aufteilen und erobern
- 5.1.3. Andere Strategien

5.2. Effizienz und Analyse von Algorithmen
- 5.2.1. Maßnahmen zur Steigerung der Effizienz
- 5.2.2. Messung der Eingabegröße
- 5.2.3. Messung der Ausführungszeit
- 5.2.4. Schlimmster, bester und durchschnittlicher Fall
- 5.2.5. Asymptotische Notation
- 5.2.6. Kriterien für die mathematische Analyse von nicht-rekursiven Algorithmen
- 5.2.7. Mathematische Analyse von rekursiven Algorithmen
- 5.2.8. Empirische Analyse von Algorithmen

5.3. Sortieralgorithmen
- 5.3.1. Konzept der Sortierung
- 5.3.2. Sortieren der Blase
- 5.3.3. Sortieren nach Auswahl
- 5.3.4. Reihenfolge der Insertion
- 5.3.5. Sortierung zusammenführen (*Merge_Sort*)
- 5.3.6. Schnelle Sortierung (*Quick_Sort*)

5.4. Algorithmen mit Bäumen
- 5.4.1. Konzept des Baumes
- 5.4.2. Binäre Bäume
- 5.4.3. Baumpfade
- 5.4.4. Ausdrücke darstellen
- 5.4.5. Geordnete binäre Bäume
- 5.4.6. Ausgeglichene binäre Bäume

5.5. Algorithmen mit *Heaps*
- 5.5.1. *Heaps*
- 5.5.2. Der *Heapsort*-Algorithmus
- 5.5.3. Prioritätswarteschlangen

5.6. Graph-Algorithmen
- 5.6.1. Vertretung
- 5.6.2. Lauf in Breite
- 5.6.3. Lauf in Tiefe
- 5.6.4. Topologische Anordnung

5.7. *Greedy*-Algorithmen
- 5.7.1. Die *Greedy*-Strategie
- 5.7.2. Elemente der *Greedy*-Strategie
- 5.7.3. Währungsumtausch
- 5.7.4. Das Problem des Reisenden
- 5.7.5. Problem mit dem Rucksack

5.8. Minimale Pfadsuche
- 5.8.1. Das Problem des minimalen Pfades
- 5.8.2. Negative Bögen und Zyklen
- 5.8.3. Dijkstra-Algorithmus

5.9. *Greedy*-Algorithmen auf Graphen
- 5.9.1. Der minimal aufspannende Baum
- 5.9.2. Algorithmus von Prim
- 5.9.3. Algorithmus von Kruskal
- 5.9.4. Komplexitätsanalyse

5.10. *Backtracking*
- 5.10.1. Das *Backtracking*
- 5.10.2. Alternative Techniken

Modul 6. Intelligente Systeme

6.1. Agententheorie
- 6.1.1. Geschichte des Konzepts
- 6.1.2. Definition von Agent
- 6.1.3. Agenten in der künstlichen Intelligenz
- 6.1.4. Agenten in der Softwareentwicklung

6.2. Agent-Architekturen
- 6.2.1. Der Denkprozess eines Agenten
- 6.2.2. Reaktive Agenten
- 6.2.3. Deduktive Agenten
- 6.2.4. Hybride Agenten
- 6.2.5. Vergleich

6.3. Informationen und Wissen
- 6.3.1. Unterscheidung zwischen Daten, Informationen und Wissen
- 6.3.2. Bewertung der Datenqualität
- 6.3.3. Methoden der Datenerfassung
- 6.3.4. Methoden der Informationsbeschaffung
- 6.3.5. Methoden zum Wissenserwerb

6.4. Wissensrepräsentation
- 6.4.1. Die Bedeutung der Wissensrepräsentation
- 6.4.2. Definition der Wissensrepräsentation durch ihre Rollen
- 6.4.3. Merkmale einer Wissensrepräsentation

6.5. Ontologien
- 6.5.1. Einführung in Metadaten
- 6.5.2. Philosophisches Konzept der Ontologie
- 6.5.3. Computergestütztes Konzept der Ontologie
- 6.5.4. Bereichsontologien und Ontologien auf höherer Ebene
- 6.5.5. Wie erstellt man eine Ontologie?

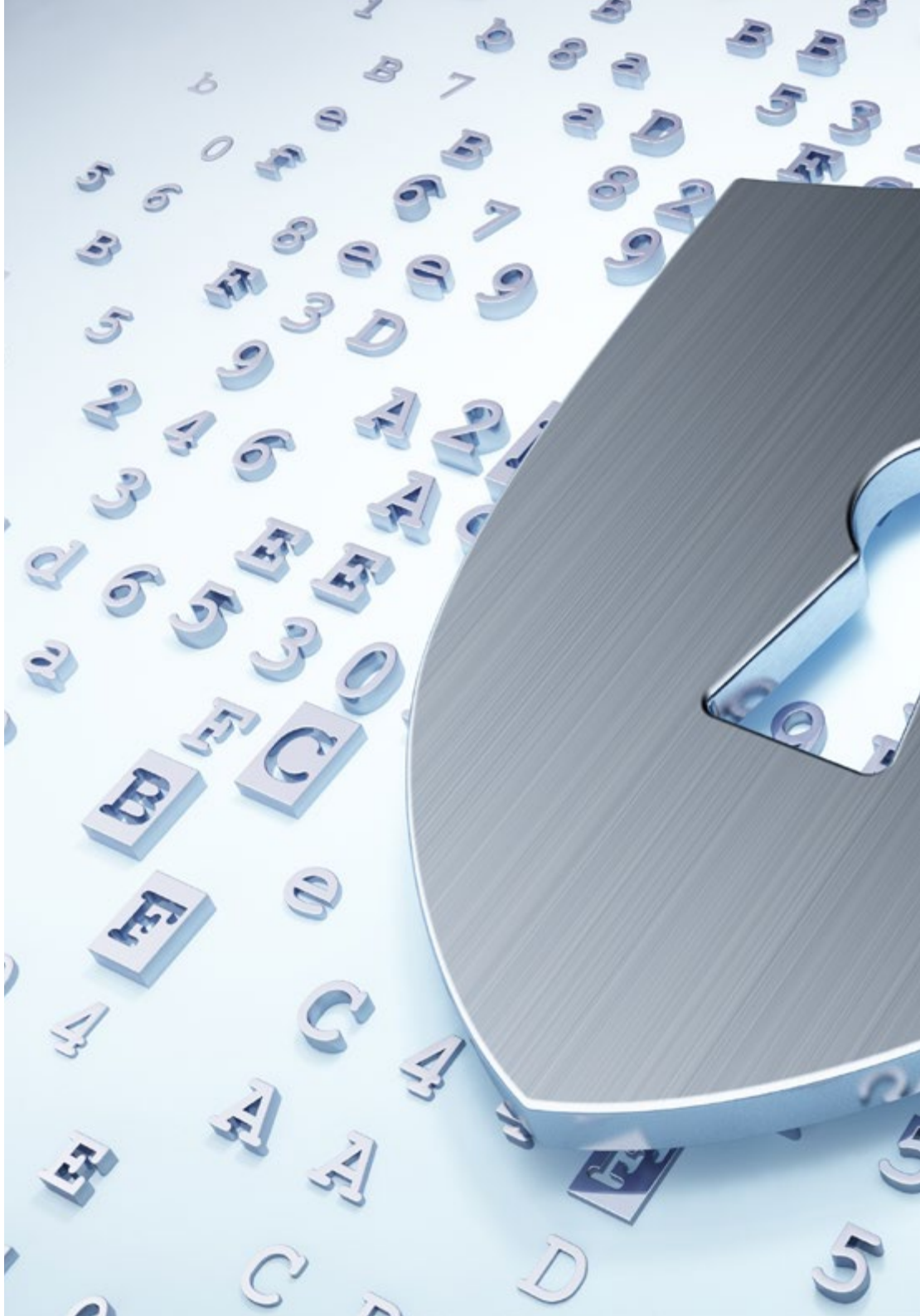
6.6. Ontologiesprachen und Software für die Erstellung von Ontologien
- 6.6.1. RDF-Tripel, *Turtle* und N
- 6.6.2. RDF-Schema
- 6.6.3. OWL
- 6.6.4. SPARQL
- 6.6.5. Einführung in die verschiedenen Tools für die Erstellung von Ontologien
- 6.6.6. Installation und Verwendung von *Protégé*

6.7. Das semantische Web
- 6.7.1. Der aktuelle Stand und die Zukunft des semantischen Webs
- 6.7.2. Anwendungen des semantischen Webs

6.8. Andere Modelle der Wissensdarstellung
- 6.8.1. Wortschatz
- 6.8.2. Globale Sicht
- 6.8.3. Taxonomie
- 6.8.4. Thesauri
- 6.8.5. Folksonomien
- 6.8.6. Vergleich
- 6.8.7. *Mind Maps*

6.9. Bewertung und Integration von Wissensrepräsentationen
- 6.9.1. Logik nullter Ordnung
- 6.9.2. Logik erster Ordnung
- 6.9.3. Beschreibende Logik
- 6.9.4. Beziehung zwischen verschiedenen Arten von Logik
- 6.9.5. *Prolog*: Programmierung auf Basis der Logik erster Ordnung

6.10. Semantische *Reasoner*, wissensbasierte Systeme und Expertensysteme
- 6.10.1. Konzept des *Reasoners*
- 6.10.2. Anwendungen eines *Reasoners*
- 6.10.3. Wissensbasierte Systeme
- 6.10.4. MYCIN, Geschichte der Expertensysteme
- 6.10.5. Elemente und Architektur von Expertensystemen
- 6.10.6. Erstellung von Expertensystemen



Modul 7. Maschinelles Lernen und *Data Mining*

7.1. Einführung in die Prozesse der Wissensentdeckung und in die grundlegenden Konzepte des maschinellen Lernens
- 7.1.1. Schlüsselkonzepte von Prozessen der Wissensentdeckung
- 7.1.2. Historische Perspektive der Wissensentdeckungsprozesse
- 7.1.3. Phasen des Wissensentdeckungsprozesses
- 7.1.4. Techniken, die bei der Wissensentdeckung eingesetzt werden
- 7.1.5. Merkmale guter Modelle für maschinelles Lernen
- 7.1.6. Arten von Informationen zum maschinellen Lernen
- 7.1.7. Grundlegende Lernkonzepte
- 7.1.8. Grundlegende Konzepte des unüberwachten Lernens

7.2. Datenexploration und Vorverarbeitung
- 7.2.1. Datenverarbeitung
- 7.2.2. Datenverarbeitung im Datenanalysefluss
- 7.2.3. Datentypen
- 7.2.4. Datenumwandlung
- 7.2.5. Anzeige und Untersuchung von kontinuierlichen Variablen
- 7.2.6. Anzeige und Erkundung kategorialer Variablen
- 7.2.7. Korrelationsmaßnahmen
- 7.2.8. Die häufigsten grafischen Darstellungen
- 7.2.9. Einführung in die multivariate Analyse und Dimensionsreduktion

7.3. Entscheidungsbaum
- 7.3.1. ID-Algorithmus
- 7.3.2. Algorithmus C
- 7.3.3. Übertraining und Beschneidung
- 7.3.4. Analyse der Ergebnisse

7.4. Bewertung von Klassifikatoren
- 7.4.1. Konfusionsmatrizen
- 7.4.2. Numerische Bewertungsmatrizen
- 7.4.3. Kappa-Statistik
- 7.4.4. Die ROC-Kurve

7.5. Klassifizierungsregeln
- 7.5.1. Maßnahmen zur Bewertung von Regeln
- 7.5.2. Einführung in die grafische Darstellung
- 7.5.3. Sequentieller Überlagerungsalgorithmus

7.6. Neuronale Netze
- 7.6.1. Grundlegende Konzepte
- 7.6.2. Einfache neuronale Netze
- 7.6.3. *Backpropagation*-Algorithmus
- 7.6.4. Einführung in rekurrente neuronale Netze

7.7. Bayessche Methoden
- 7.7.1. Grundlegende Konzepte der Wahrscheinlichkeit
- 7.7.2. Bayes-Theorem
- 7.7.3. Naive Bayes
- 7.7.4. Einführung in Bayessche Netzwerke

7.8. Regressions- und kontinuierliche Antwortmodelle
- 7.8.1. Einfache lineare Regression
- 7.8.2. Multiple lineare Regression
- 7.8.3. Logistische Regression
- 7.8.4. Regressionsbäume
- 7.8.5. Einführung in *Support Vector Machines* (SVM)
- 7.8.6. Maße für die Anpassungsgüte

7.9. *Clustering*
- 7.9.1. Grundlegende Konzepte
- 7.9.2. Hierarchisches *Clustering*
- 7.9.3. Probabilistische Methoden
- 7.9.4. EM-Algorithmus
- 7.9.5. *B-Cubed*-Methode
- 7.9.6. Implizite Methoden

7.10. *Text Mining* und natürliche Sprachverarbeitung (NLP)
- 7.10.1. Grundlegende Konzepte
- 7.10.2. Erstellung eines Korpus
- 7.10.3. Deskriptive Analyse
- 7.10.4. Einführung in die Stimmungsanalyse

Modul 8. Neuronale Netze, die Grundlage von *Deep Learning*

8.1. Tiefes Lernen
- 8.1.1. Arten von tiefem Lernen
- 8.1.2. Anwendungen von tiefem Lernen
- 8.1.3. Vor- und Nachteile von tiefem Lernen

8.2. Operationen
- 8.2.1. Addition
- 8.2.2. Produkt
- 8.2.3. Transfer

8.3. Ebenen
- 8.3.1. Eingangsebene
- 8.3.2. Ausgeblendete Ebene
- 8.3.3. Ausgangsebene

8.4. Schichtenverbund und Operationen
- 8.4.1. Design-Architekturen
- 8.4.2. Verbindung zwischen Ebenen
- 8.4.3. Vorwärtsausbreitung

8.5. Aufbau des ersten neuronalen Netzes
- 8.5.1. Entwurf des Netzes
- 8.5.2. Festlegen der Gewichte
- 8.5.3. Training des Netzes

8.6. Trainer und Optimierer
- 8.6.1. Auswahl des Optimierers
- 8.6.2. Festlegen einer Verlustfunktion
- 8.6.3. Festlegung einer Metrik

8.7. Anwendung der Prinzipien des neuronalen Netzes
- 8.7.1. Aktivierungsfunktionen
- 8.7.2. Rückwärtsausbreitung
- 8.7.3. Einstellung der Parameter

8.8. Von biologischen zu künstlichen Neuronen
- 8.8.1. Funktionsweise eines biologischen Neurons
- 8.8.2. Wissensübertragung auf künstliche Neuronen
- 8.8.3. Herstellung von Beziehungen zwischen den beiden

8.9. Implementierung von MLP (Mehrlagiges Perzeptron) mit Keras
- 8.9.1. Definition der Netzstruktur
- 8.9.2. Modell-Kompilierung
- 8.9.3. Modell-Training

8.10. *Fine Tuning* der Hyperparameter von neuronalen Netzen
- 8.10.1. Auswahl der Aktivierungsfunktion
- 8.10.2. Einstellung der *Learning Rate*
- 8.10.3. Einstellung der Gewichte

Modul 9. Training Tiefer Neuronaler Netze

9.1. Gradienten-Probleme
- 9.1.1. Techniken der Gradientenoptimierung
- 9.1.2. Stochastische Gradienten
- 9.1.3. Techniken zur Initialisierung der Gewichte

9.2. Wiederverwendung von vortrainierten Schichten
- 9.2.1. *Transfer Learning Training*
- 9.2.2. Merkmalsextraktion
- 9.2.3. Tiefes Lernen

9.3. Optimierer
- 9.3.1. Stochastische Gradientenabstiegs-Optimierer
- 9.3.2. Adam- und *RMSprop*-Optimierer
- 9.3.3. Moment-Optimierer

9.4. Planen der Lernrate
- 9.4.1. Automatische Steuerung der Lernrate
- 9.4.2. Lernzyklen
- 9.4.3. Bedingungen für die Glättung

9.5. Überanpassung
- 9.5.1. Kreuzvalidierung
- 9.5.2. Regulierung
- 9.5.3. Bewertungsmetriken

9.6. Praktische Leitlinien
- 9.6.1. Entwurf des Modells
- 9.6.2. Auswahl der Metriken und Bewertungsparameter
- 9.6.3. Testen von Hypothesen

9.7. *Transfer Learning*
- 9.7.1. *Transfer Learning Training*
- 9.7.2. Merkmalsextraktion
- 9.7.3. Tiefes Lernen

9.8. *Data Augmentation*
- 9.8.1. Bildtransformationen
- 9.8.2. Generierung synthetischer Daten
- 9.8.3. Textumwandlung

9.9. Praktische Anwendung von *Transfer Learning*
- 9.9.1. *Transfer Learning Training*
- 9.9.2. Merkmalsextraktion
- 9.9.3. Tiefes Lernen

9.10. Regulierung
- 9.10.1. L und L
- 9.10.2. Maximale Entropie-Regularisierung
- 9.10.3. *Dropout*

Modul 10. Anpassung von Modellen und Training mit *TensorFlow*

10.1. TensorFlow
- 10.1.1. Verwendung der TensorFlow-Bibliothek
- 10.1.2. Modelltraining mit TensorFlow
- 10.1.3. Graphische Operationen in TensorFlow

10.2. TensorFlow und NumPy
- 10.2.1. NumPy-Berechnungsumgebung für TensorFlow
- 10.2.2. Verwendung von NumPy-Arrays mit TensorFlow
- 10.2.3. NumPy-Operationen für TensorFlow-Graphiken

10.3. Anpassung von Modellen und Trainingsalgorithmen
- 10.3.1. Eigene Modelle mit TensorFlow erstellen
- 10.3.2. Verwaltung von Trainingsparametern
- 10.3.3. Verwendung von Optimierungstechniken für das Training

10.4. TensorFlow-Funktionen und Graphiken
- 10.4.1. Funktionen mit TensorFlow
- 10.4.2. Verwendung von Graphen für das Modelltraining
- 10.4.3. Graphikoptimierung mit TensorFlow-Operationen

10.5. Laden und Vorverarbeiten von Daten mit TensorFlow
- 10.5.1. Laden von Datensätzen mit TensorFlow
- 10.5.2. Vorverarbeitung von Daten mit TensorFlow
- 10.5.3. Verwendung von TensorFlow-Werkzeugen zur Datenmanipulation

10.6. Die tfdata-API
- 10.6.1. Verwendung der tfdata-API für die Datenverarbeitung
- 10.6.2. Konstruktion von Datenströmen mit tfdata
- 10.6.3. Verwendung der tfdata-API für das Modelltraining

10.7. Das Format TFRecord
- 10.7.1. Verwendung der TFRecord-API zur Serialisierung von Daten
- 10.7.2. Laden von TFRecord-Dateien mit TensorFlow
- 10.7.3. Verwendung von TFRecord-Dateien für das Modelltraining

10.8. Keras Vorverarbeitungsschichten
- 10.8.1. Verwendung der Keras-API für die Vorverarbeitung
- 10.8.2. Aufbau der Vorverarbeitung in Pipelines mit Keras
- 10.8.3. Verwendung der Keras Vorverarbeitungs-API für das Modelltraining

10.9. Das TensorFlow Datasets-Projekt
- 10.9.1. Verwendung von TensorFlow Datasets zum Laden von Daten
- 10.9.2. Vorverarbeitung von Daten mit TensorFlow Datasets
- 10.9.3. Verwendung von TensorFlow Datasets für das Modelltraining

10.10. Konstruktion einer Deep Learning-Anwendung mit TensorFlow
- 10.10.1. Praktische Anwendung
- 10.10.2. Konstruktion einer Deep Learning-Anwendung mit TensorFlow
- 10.10.3. Modelltraining mit TensorFlow
- 10.10.4. Verwendung der Anwendung für die Vorhersage von Ergebnissen

Modul 11. *Deep Computer Vision* mit *Convolutional Neural Networks*

11.1. Die *Visual-Cortex*-Architektur
- 11.1.1. Funktionen des visuellen Kortex
- 11.1.2. Theorien des rechnergestützten Sehens
- 11.1.3. Modelle der Bildverarbeitung

11.2. Faltungsschichten
- 11.2.1. Wiederverwendung von Gewichten bei der Faltung
- 11.2.2. Faltung D
- 11.2.3. Aktivierungsfunktionen

11.3. Gruppierungsschichten und Implementierung von Gruppierungsschichten mit Keras
- 11.3.1. *Pooling* und *Striding*
- 11.3.2. *Flattening*
- 11.3.3. Arten des *Pooling*

11.4. CNN-Architektur
- 11.4.1. VGG-Architektur
- 11.4.2. *AlexNet*-Architektur
- 11.4.3. *ResNet*-Architektur

11.5. Implementierung eines *ResNet*-CNN mit Keras
- 11.5.1. Initialisierung der Gewichte
- 11.5.2. Definition der Eingabeschicht
- 11.5.3. Definition der Ausgabe

11.6. Verwendung von vortrainierten Keras-Modellen
- 11.6.1. Merkmale der vortrainierten Modelle
- 11.6.2. Verwendung von vortrainierten Modellen
- 11.6.3. Vorteile von vortrainierten Modellen

11.7. Vortrainierte Modelle für das Transferlernen
- 11.7.1. Transferlernen
- 11.7.2. Prozess des Transferlernens
- 11.7.3. Vorteile des Transferlernens

11.8. Klassifizierung und Lokalisierung in *Deep Computer Vision*
- 11.8.1. Klassifizierung von Bildern
- 11.8.2. Objekte in Bildern lokalisieren
- 11.8.3. Objekterkennung

11.9. Objekterkennung und Objektverfolgung
- 11.9.1. Methoden zur Objekterkennung
- 11.9.2. Algorithmen zur Objektverfolgung
- 11.9.3. Verfolgungs- und Lokalisierungstechniken

11.10. Semantische Segmentierung
- 11.10.1. *Deep Learning* für semantische Segmentierung
- 11.10.2. Kantenerkennung
- 11.10.3. Regelbasierte Segmentierungsmethoden

Modul 12. Natürliche Sprachverarbeitung (NLP) mit rekurrenten neuronalen Netzen (RNN) und Aufmerksamkeit

12.1. Textgenerierung mit RNN
- 12.1.1. Training eines RNN für die Texterzeugung
- 12.1.2. Generierung natürlicher Sprache mit RNN
- 12.1.3. Anwendungen zur Texterzeugung mit RNN

12.2. Erstellung von Trainingsdatensätzen
- 12.2.1. Vorbereitung der Daten für das RNN-Training
- 12.2.2. Speicherung des Trainingsdatensatzes
- 12.2.3. Bereinigung und Transformation der Daten
- 12.2.4. Sentiment-Analyse

12.3. Ranking von Meinungen mit RNN
- 12.3.1. Erkennung von Themen in Kommentaren
- 12.3.2. Stimmungsanalyse mit *Deep-Learning*-Algorithmen

12.4. *Encoder-Decoder*-Netz für neuronale maschinelle Übersetzung
- 12.4.1. Training eines RNN für maschinelle Übersetzung
- 12.4.2. Verwendung eines *Encoder-Decoder*-Netzes für die maschinelle Übersetzung
- 12.4.3. Verbesserung der Genauigkeit der maschinellen Übersetzung mit RNNs

12.5. Aufmerksamkeitsmechanismen
- 12.5.1. Implementierung von Aufmerksamkeitsmechanismen in RNN
- 12.5.2. Verwendung von Betreuungsmechanismen zur Verbesserung der Modellgenauigkeit
- 12.5.3. Vorteile von Betreuungsmechanismen in neuronalen Netzen

12.6. *Transformer*-Modelle
- 12.6.1. Verwendung von *Transformer*-Modellen für die Verarbeitung natürlicher Sprache
- 12.6.2. Anwendung von *Transformer*-Modellen für die Sicht
- 12.6.3. Vorteile von *Transformer*-Modellen

12.7. *Transformers* für die Sicht
- 12.7.1. Verwendung von *Transformer* für die Sicht
- 12.7.2. Vorverarbeitung von Bilddaten
- 12.7.3. Training eines *Transformer*-Modells für die Sicht

12.8. *Hugging Face Transformer*-Bibliothek
- 12.8.1. Verwendung der *Hugging Face Transformer*-Bibliothek
- 12.8.2. Anwendung der *Hugging Face Transformer*-Bibliothek
- 12.8.3. Vorteile der *Hugging Face Transformer*-Bibliothek

12.9. Andere *Transformer*-Bibliotheken. Vergleich
- 12.9.1. Vergleich zwischen den verschiedenen *Transformer*-Bibliotheken
- 12.9.2. Verwendung der anderen *Transformer*-Bibliotheken
- 12.9.3. Vorteile der anderen *Transformer*-Bibliotheken

12.10. Entwicklung einer NLP-Anwendung mit RNN und Aufmerksamkeit. Praktische Anwendung
- 12.10.1. Entwicklung einer Anwendung zur Verarbeitung natürlicher Sprache mit RNN und Aufmerksamkeit
- 12.10.2. Verwendung von RNN, Aufmerksamkeitsmechanismen und *Transformer*-Modellen in der Anwendung
- 12.10.3. Bewertung der praktischen Umsetzung

Modul 13. *Autoencoder, GANs* und Diffusionsmodelle

13.1. Effiziente Datendarstellungen
- 13.1.1. Reduzierung der Dimensionalität
- 13.1.2. Tiefes Lernen
- 13.1.3. Kompakte Repräsentationen

13.2. Realisierung von PCA mit einem unvollständigen linearen automatischen Kodierer
- 13.2.1. Trainingsprozess
- 13.2.2. Python-Implementierung
- 13.2.3. Verwendung von Testdaten

13.3. Gestapelte automatische Kodierer
- 13.3.1. Tiefe neuronale Netze
- 13.3.2. Konstruktion von Kodierungsarchitekturen
- 13.3.3. Verwendung der Regularisierung

13.4. Faltungs-Autokodierer
- 13.4.1. Entwurf eines Faltungsmodells
- 13.4.2. Training von Faltungsmodellen
- 13.4.3. Auswertung der Ergebnisse

13.5. Automatische Entrauschung des Encoders
- 13.5.1. Anwendung von Filtern
- 13.5.2. Entwurf von Kodierungsmodellen
- 13.5.3. Anwendung von Regularisierungstechniken

13.6. Automatische Verteilkodierer
- 13.6.1. Steigerung der Kodierungseffizienz
- 13.6.2. Minimierung der Anzahl von Parametern
- 13.6.3. Verwendung von Regularisierungstechniken

13.7. Automatische Variationskodierer
- 13.7.1. Verwendung der Variationsoptimierung
- 13.7.2. Unüberwachtes tiefes Lernen
- 13.7.3. Tiefe latente Repräsentationen

13.8. Modische MNIST-Bilderzeugung
- 13.8.1. Mustererkennung
- 13.8.2. Bilderzeugung
- 13.8.3. Training Tiefer Neuronaler Netze

13.9. *Generative Adversarial Networks* und Diffusionsmodelle
- 13.9.1. Bildbasierte Inhaltsgenerierung
- 13.9.2. Modellierung von Datenverteilungen
- 13.9.3. Verwendung von *Adversarial Networks*

13.10. Implementierung der Modelle
- 13.10.1. Praktische Anwendung
- 13.10.2. Implementierung der Modelle
- 13.10.3. Verwendung von realen Daten
- 13.10.4. Auswertung der Ergebnisse

Modul 14. Bio-inspiriertes Computing

14.1. Einführung in das bio-inspirierte Computing
- 14.1.1. Einführung in das bio-inspirierte Computing

14.2. Algorithmen zur sozialen Anpassung
- 14.2.1. Bioinspiriertes Computing auf der Grundlage von Ameisenkolonien
- 14.2.2. Varianten von Ameisenkolonie-Algorithmen
- 14.2.3. Cloud-basiertes Computing auf Partikelebene

14.3. Genetische Algorithmen
- 14.3.1. Allgemeine Struktur
- 14.3.2. Implementierungen der wichtigsten Operatoren

14.4. Explorations-Ausbeutungsraum-Strategien für genetische Algorithmen
- 14.4.1. CHC-Algorithmus
- 14.4.2. Multimodale Probleme

14.5. Evolutionäre Berechnungsmodelle (I)
- 14.5.1. Evolutionäre Strategien
- 14.5.2. Evolutionäre Programmierung
- 14.5.3. Algorithmen auf der Grundlage der differentiellen Evolution

14.6. Evolutionäre Berechnungsmodelle (II)
- 14.6.1. Evolutionäre Modelle auf der Grundlage der Schätzung von Verteilungen (EDA)
- 14.6.2. Genetische Programmierung

14.7. Evolutionäre Programmierung angewandt auf Lernprobleme
- 14.7.1. Regelbasiertes Lernen
- 14.7.2. Evolutionäre Methoden bei Instanzauswahlproblemen

14.8. Multi-Objektive Probleme
- 14.8.1. Konzept der Dominanz
- 14.8.2. Anwendung evolutionärer Algorithmen auf multikriterielle Probleme

14.9. Neuronale Netze (I)
- 14.9.1. Einführung in neuronale Netze
- 14.9.2. Praktisches Beispiel mit neuronalen Netzen

14.10. Neuronale Netze
- 14.10.1. Anwendungsbeispiele für neuronale Netze in der medizinischen Forschung
- 14.10.2. Anwendungsbeispiele für neuronale Netze in der Wirtschaft
- 14.10.3. Anwendungsfälle für neuronale Netze in der industriellen Bildverarbeitung

Modul 15. Künstliche Intelligenz: Strategien und Anwendungen

15.1. Finanzdienstleistungen
- 15.1.1. Die Auswirkungen von künstlicher Intelligenz auf Finanzdienstleistungen. Chancen und Herausforderungen
- 15.1.2. Anwendungsbeispiele
- 15.1.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.1.4. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.2. Auswirkungen von künstlicher Intelligenz im Gesundheitswesen
- 15.2.1. Auswirkungen von künstlicher Intelligenz im Gesundheitswesen. Chancen und Herausforderungen
- 15.2.2. Anwendungsbeispiele

15.3. Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz im Gesundheitswesen
- 15.3.1. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.3.2. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.4. *Retail*
- 15.4.1. Auswirkungen von künstlicher Intelligenz im *Retail*. Chancen und Herausforderungen
- 15.4.2. Anwendungsbeispiele
- 15.4.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.4.4. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.5. Industrie
- 15.5.1. Auswirkungen von künstlicher Intelligenz in der Industrie. Chancen und Herausforderungen
- 15.5.2. Anwendungsbeispiele

15.6. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz in der Industrie
- 15.6.1. Anwendungsbeispiele
- 15.6.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.6.3. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.7. Öffentliche Verwaltung
- 15.7.1. Auswirkungen von künstlicher Intelligenz in der Öffentlichen Verwaltung. Chancen und Herausforderungen
- 15.7.2. Anwendungsbeispiele
- 15.7.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.7.4. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.8. Bildung
- 15.8.1. Auswirkungen von künstlicher Intelligenz in der Bildung. Chancen und Herausforderungen
- 15.8.2. Anwendungsbeispiele
- 15.8.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.8.4. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.9. Forst- und Landwirtschaft
- 15.9.1. Auswirkungen von künstlicher Intelligenz in der Forst- und Landwirtschaft. Chancen und Herausforderungen
- 15.9.2. Anwendungsbeispiele
- 15.9.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.9.4. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

15.10. Personalwesen
- 15.10.1. Auswirkungen von künstlicher Intelligenz im Personalwesen. Chancen und Herausforderungen
- 15.10.2. Anwendungsbeispiele
- 15.10.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz
- 15.10.4. Mögliche zukünftige Entwicklungen/Nutzungen von künstlicher Intelligenz

Modul 16. Cybersicherheit und Analyse moderner Bedrohungen mit ChatGPT

16.1. Einführung in die Cybersicherheit: aktuelle Bedrohungen und die Rolle der künstlichen Intelligenz
- 16.1.1. Definition und grundlegende Konzepte der Cybersicherheit
- 16.1.2. Arten von modernen Cyber-Bedrohungen
- 16.1.3. Rolle der künstlichen Intelligenz bei der Entwicklung der Cybersicherheit

16.2. Vertraulichkeit, Integrität und Verfügbarkeit (CIA) im Zeitalter der künstlichen Intelligenz
  16.2.1. Grundlagen des CIA-Modells in der Cybersicherheit
  16.2.2. Im Kontext der künstlichen Intelligenz angewandte Sicherheitsgrundsätze
  16.2.3. Herausforderungen und Überlegungen zur CIA in KI-gesteuerten Systemen
16.3. Verwendung von ChatGPT für Risikoanalysen und Bedrohungsszenarien
  16.3.1. Grundlagen der Risikoanalyse in der Cybersicherheit
  16.3.2. Fähigkeit von ChatGPT, Bedrohungsszenarien zu identifizieren und zu bewerten
  16.3.3. Vorteile und Grenzen der Risikoanalyse mit künstlicher Intelligenz
16.4. ChatGPT bei der Erkennung kritischer Schwachstellen
  16.4.1. Grundsätze der Erkennung von Schwachstellen in Informationssystemen
  16.4.2. Funktionalitäten von ChatGPT zur Unterstützung der Schwachstellenerkennung
  16.4.3. Ethische und sicherheitstechnische Überlegungen beim Einsatz von künstlicher Intelligenz bei der Schwachstellenerkennung
16.5. KI-gestützte Analyse von *Malware* und *Ransomware*
  16.5.1. Grundlegende Prinzipien der Analyse von *Malware* und *Ransomware*
  16.5.2. Techniken der künstlichen Intelligenz, die bei der Identifizierung von bösartigem Code eingesetzt werden
  16.5.3. Technische und operative Herausforderungen bei der KI-gestützten Analyse von *Malware*
16.6. Identifizierung von häufigen Angriffen mit Hilfe von KI: *Phishing*, *Social Engineering* und *Exploit*
  16.6.1. Klassifizierung von Angriffen: *Phishing*, *Social Engineering* und *Exploit*
  16.6.2. Techniken der künstlichen Intelligenz für die Identifizierung und Analyse von häufigen Angriffen
  16.6.3. Schwierigkeiten und Grenzen von Modellen der künstlichen Intelligenz bei der Angriffserkennung
16.7. ChatGPT in der Fortbildung und der Simulation von Cyber-Bedrohungen
  16.7.1. Grundlagen der Bedrohungssimulation für die Fortbildung im Bereich Cybersicherheit
  16.7.2. ChatGPT-Funktionen für den Entwurf von Simulationsszenarien
  16.7.3. Vorteile der Bedrohungssimulation als Fortbildungstool
16.8. Richtlinien zur Cybersicherheit mit Empfehlungen der künstlichen Intelligenz
  16.8.1. Grundsätze für die Formulierung von Cybersicherheitsstrategien
  16.8.2. Rolle der künstlichen Intelligenz bei der Erstellung von Sicherheitsempfehlungen
  16.8.3. Schlüsselkomponenten einer KI-orientierten Sicherheitspolitik
16.9. Sicherheit in IoT-Geräten und die Rolle der künstlichen Intelligenz
  16.9.1. Grundlagen der Sicherheit im Internet der Dinge (IoT)
  16.9.2. Fähigkeiten der künstlichen Intelligenz zur Entschärfung von Schwachstellen in IoT-Geräten
  16.9.3. Besondere Herausforderungen und Überlegungen zur künstlichen Intelligenz für die IoT-Sicherheit
16.10. Bewertung von Bedrohungen und Reaktionen mit Hilfe von KI-Tools
  16.10.1. Grundsätze der Bewertung von Cyber-Bedrohungen
  16.10.2. Merkmale KI-gestützter automatisierter Reaktionen
  16.10.3. Kritische Faktoren für die Wirksamkeit von Cyber-Reaktionen mit künstlicher Intelligenz

Modul 17. Erkennung und Vorbeugung von Angriffen mit Modellen der generativen künstlichen Intelligenz

17.1. Grundlagen von IDS/IPS-Systemen und die Rolle der künstlichen Intelligenz
  17.1.1. Definition und Grundprinzipien von IDS- und IPS-Systemen
  17.1.2. Haupttypen und Konfigurationen von IDS/IPS
  17.1.3. Beitrag der künstlichen Intelligenz zur Entwicklung von Erkennungs- und Präventionssystemen
17.2. Einsatz von Gemini zur Erkennung von Netzwerkanomalien
  17.2.1. Konzepte und Arten von Netzverkehrsanomalien
  17.2.2. Merkmale von Gemini für die Analyse von Netzwerkdaten
  17.2.3. Vorteile der Erkennung von Anomalien bei der Prävention von Angriffen
17.3. Gemini und die Identifizierung von *Intrusion Patterns*
  17.3.1. Grundsätze der Identifizierung und Klassifizierung von *Intrusion Patterns*
  17.3.2. Techniken der künstlichen Intelligenz, die bei der Erkennung von *Intrusion Patterns* angewendet werden
  17.3.3. Arten von Mustern und anomalem Verhalten in der Netzsicherheit
17.4. Anwendung von generativen Modellen in der Angriffssimulation
  17.4.1. Grundlagen der generativen Modelle in der künstlichen Intelligenz
  17.4.2. Anwendung von generativen Modellen zur Nachbildung von Angriffsszenarien
  17.4.3. Vorteile und Grenzen der Angriffssimulation mit generativer künstlicher Intelligenz

17.5. *Clustering* und Ereignisklassifizierung mittels künstlicher Intelligenz
- 17.5.1. Grundlagen des *Clustering* und der Klassifizierung in der *Intrusion Detection*
- 17.5.2. Übliche *Clustering*-Algorithmen, die in der Cybersicherheit eingesetzt werden
- 17.5.3. Rolle der künstlichen Intelligenz bei der Verbesserung von Methoden zur Ereignisklassifizierung

17.6. Gemini bei der Erstellung von Verhaltensprofilen
- 17.6.1. Konzepte zur Erstellung von Nutzer- und Geräteprofilen
- 17.6.2. Anwendung von generativen Modellen bei der Profilerstellung
- 17.6.3. Vorteile der Verhaltensprofilierung bei der Erkennung von Bedrohungen

17.7. *Big-Data*-Analyse zur Vorbeugung von Angriffen
- 17.7.1. Die Bedeutung von *Big Data* bei der Erkennung von Sicherheitsmustern
- 17.7.2. Methoden zur Verarbeitung großer Datenmengen in der Cybersicherheit
- 17.7.3. Anwendungen der künstlichen Intelligenz in der Analyse und Prävention auf der Grundlage von *Big Data*

17.8. Datenreduktion und Auswahl relevanter Merkmale mit künstlicher Intelligenz
- 17.8.1. Prinzipien der Dimensionalitätsreduktion bei großen Datenmengen
- 17.8.2. Auswahl von Merkmalen zur Verbesserung der Effizienz der Analyse durch künstliche Intelligenz
- 17.8.3. In der Cybersicherheit angewandte Datenreduktionstechniken

17.9. Bewertung von Modellen der künstlichen Intelligenz bei der Erkennung von Angriffen
- 17.9.1. Bewertungskriterien für Modelle der künstlichen Intelligenz in der Cybersicherheit
- 17.9.2. Leistungs- und Genauigkeitsindikatoren der Modelle
- 17.9.3. Bedeutung der fortlaufenden Validierung und Bewertung in der künstlichen Intelligenz

17.10. Implementierung eines durch generative künstliche Intelligenz unterstützten Systems zur Erkennung von Eindringlingen
- 17.10.1. Grundlagen der Implementierung von *Intrusion-Detection*-Systemen
- 17.10.2. Integration von generativer künstlicher Intelligenz in IDS/IPS-Systeme
- 17.10.3. Schlüsselaspekte für die Konfiguration und Wartung von KI-basierten Systemen

Modul 18. Moderne Kryptographie mit ChatGPT-Unterstützung beim Datenschutz

18.1. Grundprinzipien der Kryptographie mit KI-Anwendungen
- 18.1.1. Grundlegende Konzepte der Kryptographie: Vertraulichkeit und Authentizität
- 18.1.2. Die wichtigsten kryptographischen Algorithmen und ihre aktuelle Bedeutung
- 18.1.3. Rolle der künstlichen Intelligenz bei der Modernisierung der Kryptographie

18.2. ChatGPT in Lehre und Praxis der symmetrischen und asymmetrischen Kryptographie
- 18.2.1. Einführung in die symmetrische und asymmetrische Kryptographie
- 18.2.2. Vergleich zwischen symmetrischer und asymmetrischer Verschlüsselung
- 18.2.3. Verwendung von ChatGPT beim Erlernen kryptographischer Methoden

18.3. Fortgeschrittene Verschlüsselung (AES, RSA) und KI-generierte Empfehlungen
- 18.3.1. Grundlagen der AES- und RSA-Algorithmen in der Datenverschlüsselung
- 18.3.2. Stärken und Schwächen dieser Algorithmen im aktuellen Kontext
- 18.3.3. Generierung von Sicherheitsempfehlungen in der fortgeschrittenen Kryptographie mit künstlicher Intelligenz

18.4. Künstliche Intelligenz in der Verwaltung und Authentifizierung von Schlüsseln
- 18.4.1. Grundsätze der kryptographischen Schlüssel
- 18.4.2. Die Bedeutung einer sicheren Schlüsselauthentifizierung
- 18.4.3. Anwendung von künstlicher Intelligenz zur Optimierung der Prozesse der Schlüsselverwaltung und -authentifizierung

18.5. *Hashing*-Algorithmen und ChatGPT bei der Integritätsbewertung
- 18.5.1. Grundlegende Konzepte und Anwendungen von *Hashing*-Algorithmen
- 18.5.2. *Hash*-Funktionen in der Prüfung der Datenintegrität
- 18.5.3. Analyse und Überprüfung der Datenintegrität mit Hilfe von ChatGPT

18.6. ChatGPT bei der Erkennung von anomalen Verschlüsselungsmustern
- 18.6.1. Einführung in die Erkennung kryptographischer anomaler Muster
- 18.6.2. ChatGPTs Fähigkeit, Unregelmäßigkeiten in verschlüsselten Daten zu erkennen
- 18.6.3. Grenzen von Sprachmodellen bei der Erkennung anomaler Verschlüsselungen

18.7. Einführung in die Post-Quanten-Kryptographie mit KI-Simulationen
- 18.7.1. Grundlagen der Post-Quanten-Kryptographie und ihre Bedeutung
- 18.7.2. Die wichtigsten Post-Quanten-Algorithmen in der Forschung
- 18.7.3. Einsatz von künstlicher Intelligenz in Simulationen für die Untersuchung der Post-Quanten-Kryptographie

18.8. *Blockchain* und ChatGPT bei der Überprüfung von sicheren Transaktionen
- 18.8.1. Grundlegende Konzepte der *Blockchain* und ihrer Sicherheitsstruktur
- 18.1.2. Rolle der Kryptographie bei der *Blockchain*-Integrität
- 18.1.3. Anwendung von ChatGPT zur Erklärung und Analyse sicherer Transaktionen

18.9. Schutz der Privatsphäre und Verbundlernen
- 18.9.1. Definition und Prinzipien des Verbundlernens
- 18.9.2. Bedeutung des Datenschutzes beim dezentralen Lernen
- 18.9.3. Vorteile und Herausforderungen des Verbundlernens für die Datensicherheit

18.10. Entwicklung eines generativen, auf künstlicher Intelligenz basierenden Verschlüsselungssystems
- 18.10.1. Grundprinzipien bei der Erstellung von Verschlüsselungssystemen
- 18.10.2. Vorteile der generativen künstlichen Intelligenz bei der Entwicklung von Verschlüsselungssystemen
- 18.10.3. Komponenten und Anforderungen an ein KI-gestütztes Verschlüsselungssystem

Modul 19. Digitale Forensik und KI-gestützte Reaktion auf Vorfälle

19.1. Forensische Prozesse mit ChatGPT zur Identifizierung von Beweisen
- 19.1.1. Grundlegende Konzepte der forensischen Analyse in digitalen Umgebungen
- 19.1.2. Etappen der Identifizierung und Sammlung von Beweismitteln
- 19.1.3. Rolle von ChatGPT bei der Unterstützung der forensischen Identifizierung

19.2. Gemini und ChatGPT bei der Identifizierung und Datenextraktion
- 19.2.1. Grundlagen des *Data Mining* für die forensische Analyse
- 19.2.2. Techniken zur Identifizierung von relevanten Daten
- 19.2.3. Beitrag der künstlichen Intelligenz zur Automatisierung des Extraktionsprozesses

19.3. *Log*-Analyse und Ereigniskorrelation mit künstlicher Intelligenz
- 19.3.1. Bedeutung der *Logs* bei der Ereignisanalyse
- 19.3.2. Techniken der Ereigniskorrelation zur Rekonstruktion von Vorfällen
- 19.3.3. Einsatz von künstlicher Intelligenz zur Erkennung von Mustern in der *Log*-Korrelation

19.4. Daten- und Systemwiederherstellung mit künstlicher Intelligenz
- 19.4.1. Prinzipien der Datenwiederherstellung und ihre Bedeutung in der digitalen Forensik
- 19.4.2. Techniken zur Wiederherstellung kompromittierter Systeme
- 19.4.3. Anwendung von künstlicher Intelligenz zur Verbesserung von Wiederherstellungs- und Restaurierungsprozessen

19.5. *Machine Learning* für die Erkennung und Rekonstruktion von Vorfällen
- 19.5.1. Einführung in das *Machine Learning* bei der Erkennung von Vorfällen
- 19.5.2. Techniken zur Rekonstruktion von Vorfällen mit Modellen der künstlichen Intelligenz
- 19.5.3. Ethische und praktische Überlegungen bei der Ereigniserkennung

19.6. Rekonstruktion und Simulation von Ereignissen mit ChatGPT
- 19.6.1. Grundlagen der Ereignisrekonstruktion in der forensischen Analyse
- 19.6.2. ChatGPTs Fähigkeit, Vorfallsimulationen zu erstellen
- 19.6.3. Beschränkungen und Herausforderungen bei der Simulation komplexer Vorfälle

19.7. Erkennung von bösartigen Aktivitäten auf mobilen Geräten
- 19.7.1. Merkmale und Herausforderungen bei der forensischen Analyse von mobilen Geräten
- 19.7.2. Wichtige bösartige Aktivitäten in mobilen Umgebungen
- 19.7.3. Anwendung von künstlicher Intelligenz zur Identifizierung von Bedrohungen auf mobilen Geräten

19.8. Automatisierte Reaktion auf Vorfälle mit *Workflows* der künstlichen Intelligenz
- 19.8.1. Grundsätze der Reaktion auf Cybersicherheitsvorfälle
- 19.8.2. Bedeutung der Automatisierung bei der schnellen Reaktion auf Vorfälle
- 19.8.3. Vorteile von KI-gestützten Arbeitsabläufen bei der Schadensbegrenzung

19.9. Ethik und Transparenz bei der forensischen Analyse durch generative künstliche Intelligenz
- 19.9.1. Ethische Grundsätze beim Einsatz von künstlicher Intelligenz in der forensischen Analyse
- 19.9.2. Transparenz und Erklärbarkeit von generativen Modellen in der Forensik
- 19.9.3. Überlegungen zum Datenschutz und zur Verantwortlichkeit in der Analyse

19.10. Forensische Analyse und Labor zur Wiederherstellung von Vorfällen mit ChatGPT und Gemini
- 19.10.1. Struktur und Ziele eines Labors für forensische Analysen
- 19.10.2. Vorteile von kontrollierten Umgebungen für die forensische Praxis
- 19.10.3. Schlüsselkomponenten für die Einrichtung eines Simulationslabors

Modul 20. Prädiktive Modelle für die proaktive Verteidigung in der Cybersicherheit mit ChatGPT

20.1. Prädiktive Analyse in der Cybersicherheit: Techniken und Anwendungen mit künstlicher Intelligenz
- 20.1.1. Grundlegende Konzepte der prädiktiven Analyse in der Sicherheit
- 20.1.2. Prädiktive Techniken im Bereich der Cybersicherheit
- 20.1.3. Anwendung von künstlicher Intelligenz bei der Vorhersage von Cyber-Bedrohungen

20.2. Von ChatGPT unterstützte Regressions- und Klassifikationsmodelle
- 20.2.1. Grundsätze der Regression und Klassifizierung bei der Vorhersage von Bedrohungen
- 20.2.2. Arten von Klassifikationsmodellen in der Cybersicherheit
- 20.2.3. Unterstützung durch ChatGPT bei der Interpretation von prädiktiven Modellen

20.3. Identifizierung neuer Bedrohungen mit ChatGPT-Vorhersagen
- 20.3.1. Konzepte zur Erkennung aufkommender Bedrohungen
- 20.3.2. Techniken zur Erkennung neuer Angriffsmuster
- 20.3.3. Beschränkungen und Vorsichtsmaßnahmen bei der Vorhersage neuer Bedrohungen

20.4. Neuronale Netze zur Vorhersage von Cyberangriffen
- 20.4.1. Grundlagen der neuronalen Netze für die Cybersicherheit
- 20.4.2. Übliche Architekturen für die Erkennung und Vorhersage von Angriffen
- 20.4.3. Herausforderungen bei der Implementierung von neuronalen Netzen in der Cyberverteidigung

20.5. Verwendung von ChatGPT für Simulationen von Bedrohungsszenarien
- 20.5.1. Grundlegende Konzepte der Bedrohungssimulation in der Cybersicherheit
- 20.5.2. ChatGPT-Fähigkeiten zur Entwicklung prädiktiver Simulationen
- 20.5.3. Faktoren, die bei der Gestaltung von simulierten Szenarien zu berücksichtigen sind

20.6. Algorithmen des Verstärkungslernens für die Optimierung der Verteidigung
- 20.6.1. Einführung in das Verstärkungslernen in der Cybersicherheit
- 20.6.2. Algorithmen des Verstärkungslernens, angewandt auf Verteidigungsstrategien
- 20.6.3. Vorteile und Herausforderungen des Verstärkungslernens in Umgebungen der Cybersicherheit

20.7. Simulation von Bedrohungen und Reaktionen mit ChatGPT
- 20.7.1. Prinzipien der Bedrohungssimulation und ihre Bedeutung für die Cyberabwehr
- 20.7.2. Automatisierte und optimierte Reaktionen auf simulierte Angriffe
- 20.7.3. Vorteile der Simulation für die Verbesserung der Cyber-Bereitschaft

20.8. Bewertung der Genauigkeit und Wirksamkeit von prädiktiven KI-Modellen
- 20.8.1. Schlüsselindikatoren für die Bewertung von prädiktiven Modellen
- 20.8.2. Methodologien zur Bewertung der Genauigkeit von Modellen der Cybersicherheit
- 20.8.3. Kritische Faktoren für die Effektivität von Modellen der künstlichen Intelligenz in der Cybersicherheit

20.9. Künstliche Intelligenz im Management von Vorfällen und automatisierte Reaktionen
- 20.9.1. Grundlagen des Managements von Vorfällen in der Cybersicherheit
- 20.9.2. Rolle der künstlichen Intelligenz bei der Entscheidungsfindung in Echtzeit
- 20.9.3. Herausforderungen und Möglichkeiten der Automatisierung von Reaktionen

20.10. Aufbau eines prädiktiven Verteidigungssystems mit ChatGPT-Unterstützung
- 20.10.1. Entwurfsprinzipien für ein proaktives Verteidigungssystem
- 20.10.2. Integration von prädiktiven Modellen in Umgebungen der Cybersicherheit
- 20.10.3. Schlüsselkomponenten für ein KI-basiertes prädiktives Verteidigungssystem

Sie werden Sicherheitsarchitekturen auf der Grundlage des maschinellen Lernens implementieren und sicherstellen, dass die Lösungen effektiv in die Infrastrukturen der Organisationen integriert werden“

04

Lehrziele

Durch diesen Hochschulabschluss erwerben die Fachkräfte fortgeschrittene Kompetenzen zur Leitung von auf künstlicher Intelligenz basierenden Projekten im Bereich der Cybersicherheit. In diesem Sinne werden die Studenten in der Lage sein, Vorhersagemodelle zu entwerfen, fortschrittliche Algorithmen zu implementieren und wirksame Strategien zum Schutz von Systemen und Daten zu entwickeln. Darüber hinaus werden die Absolventen in der Lage sein, Bedrohungen proaktiv zu erkennen, digitale forensische Analysetechniken anzuwenden und technologische Ressourcen in hochkomplexen Umgebungen zu optimieren.

Sie werden Algorithmen anpassen, um sicherzustellen, dass Sicherheitslösungen bei der Prävention und Erkennung von Cyberbedrohungen wirksam sind"

Allgemeine Ziele

- Beherrschen der Grundprinzipien der künstlichen Intelligenz und ihrer Anwendung in der Cybersicherheit
- Analysieren des Datenlebenszyklus und seiner Auswirkungen auf die Implementierung intelligenter Systeme
- Entwickeln fortgeschrittener maschineller Lernmodelle zur Erkennung und Abwehr von Bedrohungen
- Implementieren von tiefen neuronalen Netzen und *Deep-Learning*-Systemen in Cybersicherheitsprojekten
- Anwenden von *Data Mining* und Techniken zur Verarbeitung natürlicher Sprache auf die Risikoanalyse
- Entwickeln von KI-basierten Strategien für den proaktiven Schutz kritischer Infrastrukturen
- Integrieren von bio-inspirierten intelligenten Systemen für die Lösung komplexer Probleme in digitalen Umgebungen
- Optimieren von Algorithmen und Tools wie TensorFlow zur Anpassung von Sicherheitslösungen
- Implementieren KI-gestützter digitaler forensischer Analysemethoden
- Entwerfen innovativer Lösungen in der modernen Kryptographie zur Gewährleistung der Datenintegrität
- Bewerten der Wirksamkeit von prädiktiven und generativen Modellen für die Cyberabwehr
- Fördern von Innovationen bei der Entwicklung KI-gestützter Tools zur Bekämpfung neuer Bedrohungen

Spezifische Ziele

Modul 1. Grundlagen der künstlichen Intelligenz

- Analysieren der historischen Entwicklung der künstlichen Intelligenz, von ihren Anfängen bis zu ihrem heutigen Stand, Identifizierung der wichtigsten Meilensteine und Entwicklungen
- Verstehen der Funktionsweise von neuronalen Netzen und ihrer Anwendung in Lernmodellen der künstlichen Intelligenz
- Untersuchen der Grundsätze und Anwendungen von genetischen Algorithmen und Analysieren ihrer Nützlichkeit bei der Lösung komplexer Probleme
- Analysieren der Bedeutung von Thesauri, Vokabularen und Taxonomien bei der Strukturierung und Verarbeitung von Daten für KI-Systeme

Modul 2. Datentypen und Datenlebenszyklus

- Identifizieren und Klassifizieren der verschiedenen Arten von statistischen Daten, von quantitativen bis zu qualitativen Daten
- Analysieren des Lebenszyklus von Daten, von der Erzeugung bis zur Entsorgung, und Identifizieren der wichtigsten Phasen
- Erkunden der ersten Phasen des Lebenszyklus von Daten, wobei die Bedeutung der Datenplanung und der Datenstruktur hervorgehoben wird
- Untersuchen der Prozesse der Datenerfassung, einschließlich Methodik, Tools und Erfassungskanäle
- Untersuchen des *Datawarehouse*-Konzepts mit Schwerpunkt auf den Elementen des *Datawarehouse* und seinem Design
- Analysieren der rechtlichen Aspekte im Zusammenhang mit der Datenverwaltung, der Einhaltung von Datenschutz- und Sicherheitsvorschriften sowie bewährter Verfahren

Modul 3. Daten in der künstlichen Intelligenz

- Beherrschen der Grundlagen der Datenwissenschaft, einschließlich der Werkzeuge, Typen und Quellen für die Informationsanalyse
- Erforschen des Prozesses der Umwandlung von Daten in Informationen mithilfe von *Data Mining* und Datenvisualisierungstechniken
- Untersuchen der Struktur und der Eigenschaften von *Datasets* und Verstehen ihrer Bedeutung für die Aufbereitung und Nutzung von Daten für KI-Modelle
- Verwenden spezifischer Tools und bewährter Verfahren für die Datenverarbeitung, um Effizienz und Qualität bei der Implementierung von künstlicher Intelligenz zu gewährleisten

Modul 4. *Data Mining*. Auswahl, Vorverarbeitung und Transformation

- Beherrschen statistischer Inferenztechniken, um statistische Methoden im *Data Mining* zu verstehen und anzuwenden
- Durchführen detaillierter explorativer Analysen von Datensätzen, um relevante Muster, Anomalien und Trends zu erkennen
- Entwickeln von Fähigkeiten zur Datenaufbereitung, einschließlich Datenbereinigung, -integration und -formatierung für die Verwendung im *Data Mining*
- Implementieren effektiver Strategien für den Umgang mit fehlenden Werten in Datensätzen, indem je nach Kontext Imputations- oder Eliminierungsmethoden angewendet werden
- Identifizieren und Entschärfen von Datenrauschen, durch Anwendung von Filter- und Glättungsverfahren, um die Qualität des Datensatzes zu verbessern
- Eingehen auf die Datenvorverarbeitung in *Big-Data*-Umgebungen

Modul 5. Algorithmik und Komplexität in der künstlichen Intelligenz

- Einführen von Strategien zum Entwurf von Algorithmen, die ein solides Verständnis der grundlegenden Ansätze zur Problemlösung vermitteln
- Untersuchen und Anwenden von Sortieralgorithmen, Verstehen ihrer Leistung und Vergleichen ihrer Effizienz in verschiedenen Kontexten
- Untersuchen von Algorithmen mit *Heaps*, Analysieren ihrer Implementierung und ihrer Nützlichkeit bei der effizienten Datenmanipulation
- Analysieren graphenbasierter Algorithmen, wobei ihre Anwendung bei der Darstellung und Lösung von Problemen mit komplexen Beziehungen untersucht wird
- Untersuchen von *Greedy*-Algorithmen, Verständnis ihrer Logik und Anwendungen bei der Lösung von Optimierungsproblemen
- Untersuchen und Anwenden der *Backtracking*-Technik für die systematische Problemlösung und Analysieren ihrer Effektivität in verschiedenen Szenarien

Modul 6. Intelligente Systeme

- Erforschen der Agententheorie, Verstehen der grundlegenden Konzepte ihrer Funktionsweise und ihrer Anwendung in der künstlichen Intelligenz und der Softwaretechnik
- Analysieren des Konzepts des semantischen Webs und seiner Auswirkungen auf die Organisation und den Abruf von Informationen in digitalen Umgebungen
- Evaluieren und Vergleichen verschiedener Wissensrepräsentationen und deren Integration zur Verbesserung der Effizienz und Genauigkeit von intelligenten Systemen
- Studieren semantischer *Reasoner*, wissensbasierter Systeme und Expertensysteme und Verstehen ihrer Funktionalität und Anwendungen in der intelligenten Entscheidungsfindung

Modul 7. Maschinelles Lernen und *Data Mining*

- Einführen in die Prozesse der Wissensentdeckung und in die grundlegenden Konzepte des maschinellen Lernens
- Bewerten von Klassifikatoren anhand spezifischer Techniken, um ihre Leistung und Genauigkeit bei der Datenklassifizierung zu messen
- Studieren neuronaler Netze und Verstehen ihrer Funktionsweise und Architektur, um komplexe Probleme des maschinellen Lernens zu lösen
- Erforschen von Bayesschen Methoden und deren Anwendung im maschinellen Lernen, einschließlich Bayesscher Netze und Klassifikatoren
- Analysieren von Regressions- und kontinuierlichen Antwortmodellen zur Vorhersage von numerischen Werten aus Daten
- Erforschen von *Text Mining* und natürlicher Sprachverarbeitung (NLP), um zu verstehen, wie maschinelle Lerntechniken zur Analyse und zum Verständnis von Texten eingesetzt werden

Modul 8. Neuronale Netze, die Grundlage von *Deep Learning*

- Beherrschen der Grundlagen des tiefen Lernens und Verstehen seiner wesentlichen Rolle beim *Deep Learning*
- Erkunden der grundlegenden Operationen in neuronalen Netzen und Verstehen ihrer Anwendung bei der Konstruktion von Modellen
- Analysieren der verschiedenen Schichten, die in neuronalen Netzen verwendet werden, und lernen, wie man sie richtig auswählt
- Verstehen der effektiven Verknüpfung von Schichten und Operationen, um komplexe und effiziente neuronale Netzarchitekturen zu entwerfen
- Erforschen der Verbindung zwischen biologischen und künstlichen Neuronen für ein tieferes Verständnis des Modelldesigns
- Anpassen von Hyperparametern für das *Fine Tuning* neuronaler Netze, um ihre Leistung bei bestimmten Aufgaben zu optimieren

Modul 9. Training Tiefer Neuronaler Netze

- Lösen von Problemen im Zusammenhang mit Gradienten beim Training von tiefen neuronalen Netzen
- Anwenden praktischer Richtlinien, um ein effizientes und effektives Training von tiefen neuronalen Netzen zu gewährleisten
- Implementieren von *Transfer Learning* als fortgeschrittene Technik zur Verbesserung der Modellleistung bei bestimmten Aufgaben
- Erforschen und Anwenden von Techniken der *Data Augmentation* zur Anreicherung von Datensätzen und Verbesserung der Modellgeneralisierung
- Entwickeln praktischer Anwendungen mit *Transfer Learning* zur Lösung realer Probleme
- Verstehen und Anwenden von Regularisierungstechniken zur Verbesserung der Generalisierung und zur Vermeidung von *Overfitting* in tiefen neuronalen Netzen

Modul 10. Anpassung von Modellen und Training mit *TensorFlow*

- Beherrschen der Grundlagen von *TensorFlow* und seiner Integration mit NumPy für effiziente Datenverwaltung und Berechnungen
- Anpassen von Modellen und Trainingsalgorithmen mit den fortgeschrittenen Fähigkeiten von *TensorFlow*
- Implementieren des Formats TFRecord, um große Datensätze in *TensorFlow* zu speichern und darauf zuzugreifen
- Verwenden von Keras-Vorverarbeitungsschichten zur Erleichterung der Konstruktion eigener Modelle
- Erforschen des *TensorFlow Datasets* Projekts, um auf vordefinierte Datensätze zuzugreifen und die Entwicklungseffizienz zu verbessern
- Entwickeln einer *Deep-Learning*-Anwendung mit *TensorFlow* unter Einbeziehung der im Modul erworbenen Kenntnisse

Modul 11. *Deep Computer Vision* mit *Convolutional Neural Networks*

- Verstehen der Architektur des visuellen Kortex und ihrer Bedeutung für *Deep Computer Vision*
- Erforschen und Anwenden von Faltungsschichten, um wichtige Merkmale aus Bildern zu extrahieren
- Implementieren von *Clustering*-Schichten und ihre Verwendung in *Deep Computer Vision*-Modellen mit Keras
- Analysieren verschiedener Architekturen von *Convolutional Neural Networks* (CNN) und deren Anwendbarkeit in verschiedenen Kontexten
- Entwickeln und Implementieren eines CNN ResNet unter Verwendung der Keras-Bibliothek, um die Effizienz und Leistung des Modells zu verbessern
- Verwenden von vorab trainierten Keras-Modellen, um das Transfer-Lernen für bestimmte Aufgaben zu nutzen
- Untersuchen der Strategien zur Objekterkennung und -verfolgung mit *Convolutional Neural Networks*
- Implementieren von Techniken der semantischen Segmentierung, um Objekte in Bildern im Detail zu verstehen und zu klassifizieren

Modul 12. Natürliche Sprachverarbeitung (NLP) mit rekurrenten neuronalen Netzen (RNN) und Aufmerksamkeit

- Entwickeln von Fähigkeiten zur Texterstellung mit rekurrenten neuronalen Netzen (RNN)
- Anwenden von RNNs bei der Meinungsklassifizierung zur Stimmungsanalyse in Texten
- Verstehen und Anwenden von Aufmerksamkeitsmechanismen in Modellen zur Verarbeitung natürlicher Sprache
- Analysieren und Verwenden von *Transformers*-Modellen in spezifischen NLP-Aufgaben
- Eingehen auf die Anwendung von *Transformers*-Modellen im Kontext von Bildverarbeitung und Computer Vision
- Kennenlernen der *Hugging Face Transformers*-Bibliothek für die effiziente Implementierung fortgeschrittener Modelle
- Vergleichen der verschiedenen *Transformers*-Bibliotheken, um ihre Eignung für bestimmte Aufgaben zu bewerten
- Entwickeln einer praktischen Anwendung von NLP, die RNN- und Aufmerksamkeitsmechanismen integriert, um reale Probleme zu lösen

Modul 13. *Autoencoder, GANs* und Diffusionsmodelle

- Entwickeln effizienter Datenrepräsentationen mit *Autoencodern, GANs* und Diffusionsmodellen
- Durchführen einer PCA unter Verwendung eines unvollständigen linearen *Autoencoders* zur Optimierung der Datendarstellung
- Vertiefen und Anwenden von *Convolutional Autoencoders* für effiziente visuelle Datendarstellungen
- Generieren von Modebildern aus dem MNIST-Datensatz mit Hilfe von *Autoencoders*
- Verstehen des Konzepts der *Generative Adversarial Networks* (GANs) und Diffusionsmodelle
- Implementieren und Vergleichen der Leistung von Diffusionsmodellen und *GANs* bei der Datengenerierung

Modul 14. Bio-inspiriertes Computing

- Einführen in die grundlegenden Konzepte des bio-inspirierten Computings
- Analysieren sozialer Anpassungsalgorithmen als wichtiger Ansatz im bio-inspirierten Computing
- Untersuchen von Modellen des evolutionären Rechnens im Kontext der Optimierung
- Bewältigen der Komplexität von Multi-Objektiv-Problemen im Rahmen des bio-inspirierten Computings
- Erforschen der Anwendung von neuronalen Netzen im Bereich des bio-inspirierten Computings
- Vertiefen der Implementierung und des Nutzens von neuronalen Netzen im Bereich des bio-inspirierten Computings

Modul 15. Künstliche Intelligenz: Strategien und Anwendungen

- Entwickeln von Strategien für die Implementierung von künstlicher Intelligenz in Finanzdienstleistungen
- Analysieren der Auswirkungen von künstlicher Intelligenz auf die Erbringung von Dienstleistungen im Gesundheitswesen
- Identifizieren und Bewerten der Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz im Gesundheitssektor
- Bewerten der potenziellen Risiken im Zusammenhang mit dem Einsatz von künstlicher Intelligenz in der Industrie

- Anwenden von Techniken der künstlichen Intelligenz in der Industrie zur Verbesserung der Produktivität
- Entwerfen von Lösungen der künstlichen Intelligenz zur Optimierung von Prozessen in der öffentlichen Verwaltung
- Bewerten des Einsatzes von KI-Technologien im Bildungssektor
- Anwenden von Techniken der künstlichen Intelligenz in der Forst- und Landwirtschaft zur Verbesserung der Produktivität

Modul 16. Cybersicherheit und Analyse moderner Bedrohungen mit ChatGPT

- Verstehen der grundlegenden Konzepte der Cybersicherheit, einschließlich moderner Bedrohungen und des CIA-Modells
- Verwenden von ChatGPT zur Risikoanalyse, Schwachstellenerkennung und Simulation von Bedrohungsszenarien
- Entwickeln von Fähigkeiten zur Gestaltung effektiver Cybersicherheitsrichtlinien und zum Schutz von IoT-Geräten mithilfe von künstlicher Intelligenz
- Implementieren fortschrittlicher Strategien zum Bedrohungsmanagement unter Verwendung generativer künstlicher Intelligenz, um potenzielle Angriffe zu antizipieren
- Bewerten der Auswirkungen moderner Bedrohungen auf kritische Infrastrukturen mithilfe von KI-gestützten Simulationstechniken
- Entwickeln maßgeschneiderter Lösungen für den Schutz von Unternehmensnetzwerken auf der Grundlage fortschrittlicher Werkzeuge der künstlichen Intelligenz

Modul 17. Erkennung und Vorbeugung von Angriffen mit Modellen der generativen künstlichen Intelligenz

- Beherrschen von Techniken zur Erkennung von Anomalien und Eindringungsmustern mit Tools wie Gemini
- Anwenden generativer Modelle zur Simulation von Cyberangriffen und zur Verbesserung der Prävention von Angriffen
- Implementieren fortschrittlicher IDS/IPS-Systeme, die mit künstlicher Intelligenz optimiert sind, Verhaltensprofile entwickeln und Big Data in Echtzeit analysieren
- Entwerfen von KI-integrierten Sicherheitsarchitekturen für den Schutz von Mehrbenutzerumgebungen und verteilten Systemen
- Verwenden generativer Modelle zur Vorhersage gezielter Angriffe und zur Entwicklung von Gegenmaßnahmen in Echtzeit
- Integrieren von prädiktiven Analysen in Erkennungssysteme für ein dynamisches Management von neu auftretenden Bedrohungen

Modul 18. Moderne Kryptographie mit ChatGPT-Unterstützung beim Datenschutz

- Beherrschen der Grundlagen fortgeschrittener Kryptographie, einschließlich Algorithmen wie AES, RSA und Post-Quanten-Algorithmen
- Verwenden von ChatGPT zum Erlernen, Üben und Optimieren kryptographischer Methoden
- Entwerfen und Verwalten von KI-gestützten Verschlüsselungssystemen, die den Datenschutz und die Authentizität von Daten gewährleisten
- Bewerten der Widerstandsfähigkeit von kryptographischen Algorithmen gegen simulierte Angriffsszenarien mit generativer künstlicher Intelligenz
- Entwickeln optimierter Ver- und Entschlüsselungsstrategien zum Schutz kritischer Infrastrukturen und sensibler Daten
- Implementieren von Lösungen der Post-Quanten-Kryptographie, um zukünftige Risiken in KI-basierten Systemen zu minimieren

Modul 19. Digitale Forensik und KI-gestützte Reaktion auf Vorfälle

- Lernen, digitale Beweise mit Hilfe von KI-Tools zu identifizieren, zu extrahieren und zu analysieren
- Verwenden von künstlicher Intelligenz zur Automatisierung der Datenwiederherstellung und Rekonstruktion von Sicherheitsvorfällen
- Entwerfen und Anwenden von automatisierten Reaktionsabläufen, die eine schnelle und effektive Eindämmung von Vorfällen gewährleisten
- Integrieren fortschrittlicher forensischer Analysetools für die Untersuchung komplexer Cyberangriffe
- Entwickeln von KI-basierten Techniken zur Ereignisrekonstruktion für Audits nach Vorfällen
- Erstellen von automatisierten Protokollen für die Reaktion auf Vorfälle, wobei der Betriebskontinuität und der Schadensbegrenzung Priorität eingeräumt wird

Modul 20. Prädiktive Modelle für die proaktive Verteidigung in der Cybersicherheit mit ChatGPT

- Entwickeln fortgeschrittener Vorhersagemodelle auf der Grundlage von neuronalen Netzen und Verstärkungslernen
- Implementieren von Simulationen von Bedrohungsszenarien, um Teams zu trainieren und die Bereitschaft für Vorfälle zu verbessern
- Bewerten und Optimieren proaktiver Verteidigungssysteme unter Einbeziehung generativer künstlicher Intelligenz in die Entscheidungsfindung und Reaktionsautomatisierung
- Entwickeln von *Frameworks* für die prädiktive Verteidigung, die an kritische Infrastrukturen und Unternehmenssysteme angepasst werden können
- Verwenden von prädiktiver Analytik, um aufkommende Schwachstellen zu erkennen, bevor sie ausgenutzt werden
- Integrieren von generativer künstlicher Intelligenz in strategische Entscheidungsprozesse zur kontinuierlichen Verbesserung von Verteidigungssystemen

Mit den Lernmitteln von TECH, zu denen unter anderem Lehrvideos und interaktive Zusammenfassungen gehören, werden Sie Ihre Ziele erreichen“

05

Karrieremöglichkeiten

Durch dieses Programm in Künstliche Intelligenz in der Cybersicherheit werden die Spezialisten ihre Berufsaussichten deutlich verbessern. Berufsaussichten deutlich verbessern.
Auf diese Weise werden die Absolventen hochqualifiziert sein, um Zugang zu strategischen Rollen von größerer Bedeutung zu erhalten, wie z. B. der Leitung von Cybersicherheit mit künstlicher Intelligenz. Auf diese Weise werden die Studenten die Implementierung digitaler Sicherheitslösungen auf der Grundlage intelligenter Systeme leiten und innovative Tools zum Schutz von Systemen in globalen Organisationen entwickeln.

Möchten Sie als Analyst für Cybersicherheit in der künstlichen Intelligenz arbeiten? Dieser Universitätsabschluss wird Ihnen die notwendigen Kenntnisse vermitteln, um dies in nur wenigen Monaten zu erreichen“

Profil des Absolventen

Der Absolvent dieses Hochschulprogramms wird ein Experte für die Integration von künstlicher Intelligenz und Cybersicherheit sein, um innovative Lösungen für digitale Bedrohungen zu entwickeln. Er wird über fundierte Kenntnisse fortschrittlicher Tools, Prognosemodelle und moderner Kryptographie verfügen und sich durch seine Fähigkeit auszeichnen, wirksame Strategien zum Schutz kritischer Daten und Systeme umzusetzen. Dieses Profil verbindet technische Exzellenz mit praktischem Weitblick und stellt sicher, dass er einen Beitrag zum Wandel des digitalen Umfelds leistet.

Sie werden in der Lage sein, große Datenmengen im Zusammenhang mit der Cybersicherheit zu analysieren, um ungewöhnliche Verhaltensmuster zu erkennen.

- **Kritisches Denken und Problemlösung:** Fähigkeit, komplexe Situationen aus verschiedenen Blickwinkeln zu analysieren, um Muster in digitalen Bedrohungen zu erkennen und innovative Lösungen unter Verwendung künstlicher Intelligenz zu entwickeln, die technologische Herausforderungen präzise und anpassungsfähig angehen
- **Datengestützte Entscheidungsfindung:** Fähigkeit, große Datenmengen auszuwerten und Prognosemodelle anzuwenden, die Echtzeit-Strategien zur Sicherstellung von Maßnahmen zur effizienten Risikominderung liefern
- **Technologische Anpassungsfähigkeit:** Fähigkeit, neue KI-Tools, -Technologien und -Methoden rasch in die berufliche Praxis zu integrieren, indem sie schnell auf Veränderungen in der digitalen Landschaft und neue Formen von Cyberangriffen reagieren
- **Ethisches und verantwortungsvolles Management:** Eingehendes Verständnis der rechtlichen und ethischen Aspekte im Zusammenhang mit dem Datenschutz und dem Einsatz von künstlicher Intelligenz, wobei ethisch und im Einklang mit internationalen Vorschriften gehandelt wird, um einen verantwortungsvollen Einsatz von Technologien im Bereich der Cybersicherheit zu gewährleisten

Nach Abschluss des Studiengangs werden Sie in der Lage sein, Ihre Kenntnisse und Fähigkeiten in den folgenden Positionen anzuwenden:

1. **Analyst für Cybersicherheit mit künstlicher Intelligenz:** Verantwortlich für die Identifizierung, Vorbeugung und Entschärfung digitaler Bedrohungen unter Verwendung fortschrittlicher Modelle der künstlichen Intelligenz zum Schutz kritischer Systeme.
2. **Digitaler forensischer Analyst mit künstlicher Intelligenz:** Verantwortlich für die Identifizierung, Extraktion und Analyse digitaler Beweise unter Verwendung fortschrittlicher Technologien der künstlichen Intelligenz.
3. **Berater für proaktive digitale Verteidigung:** Berater, der sich auf die Entwicklung von auf künstlicher Intelligenz basierenden Sicherheitsstrategien spezialisiert hat, um aufkommende Bedrohungen in Unternehmensumgebungen zu antizipieren.
4. **Experte für digitale Forensik mit künstlicher Intelligenz:** Verantwortlich für die Untersuchung und Rekonstruktion von Cybersicherheitsvorfällen unter Verwendung von Tools der künstlichen Intelligenz zur Extraktion und Analyse digitaler Beweise.
5. **Designer für prädiktive Modelle der Cybersicherheit:** Konzentriert sich auf die Entwicklung und Implementierung von Systemen, die auf maschinellem Lernen und neuronalen Netzen basieren, um Schwachstellen vorherzusehen. Verantwortlichkeiten:
6. **Koordinator für die Sicherheit kritischer Infrastrukturen:** Verantwortlich für die Beaufsichtigung der Implementierung von KI-basierten Cybersicherheitslösungen in strategischen Sektoren wie Energie, Transport oder Finanzen.
7. **Manager von Cyberrisiken mit künstlicher Intelligenz:** Verantwortlich für die Planung und Durchführung von Strategien zur Identifizierung und Minimierung von Cyberrisiken mithilfe von künstlicher Intelligenz.
8. **Leiter der Post-Quanten-Kryptographie:** Experte für die Entwicklung robuster Verschlüsselungssysteme auf der Grundlage quantenresistenter Algorithmen, die einen langfristigen Datenschutz gewährleisten.
9. **Verwalter von Systemen zur Erkennung von Angriffen mit generativer künstlicher Intelligenz:** Verantwortlich für die Konfiguration und Optimierung automatisierter Sicherheitstools, die generative künstliche Intelligenz zur Erkennung von und Reaktion auf Bedrohungen nutzen.
10. **Auditor für digitale Sicherheit mit Hilfe von künstlicher Intelligenz:** Verantwortlich für die Bewertung und Zertifizierung von digitalen Sicherheitssystemen unter Verwendung fortschrittlicher KI-gestützter Analysetools.

Führen Sie Cybersicherheitslösungen auf der Grundlage intelligenter Systeme ein, um Systeme und Netzwerke vor möglichen Angriffen zu schützen“

06

Studienmethodik

TECH ist die erste Universität der Welt, die die Methodik der ***case studies*** mit ***Relearning*** kombiniert, einem 100%igen Online-Lernsystem, das auf geführten Wiederholungen basiert.

Diese disruptive pädagogische Strategie wurde entwickelt, um Fachleuten die Möglichkeit zu bieten, ihr Wissen zu aktualisieren und ihre Fähigkeiten auf intensive und gründliche Weise zu entwickeln. Ein Lernmodell, das den Studenten in den Mittelpunkt des akademischen Prozesses stellt und ihm die Hauptrolle zuweist, indem es sich an seine Bedürfnisse anpasst und die herkömmlichen Methoden beiseite lässt.

TECH bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein“

Der Student: die Priorität aller Programme von TECH

Bei der Studienmethodik von TECH steht der Student im Mittelpunkt.
Die pädagogischen Instrumente jedes Programms wurden unter Berücksichtigung der Anforderungen an Zeit, Verfügbarkeit und akademische Genauigkeit ausgewählt, die heutzutage nicht nur von den Studenten, sondern auch von den am stärksten umkämpften Stellen auf dem Markt verlangt werden.

Beim asynchronen Bildungsmodell von TECH entscheidet der Student selbst, wie viel Zeit er mit dem Lernen verbringt und wie er seinen Tagesablauf gestaltet, und das alles bequem von einem elektronischen Gerät seiner Wahl aus. Der Student muss nicht an Präsenzveranstaltungen teilnehmen, die er oft nicht wahrnehmen kann.
Die Lernaktivitäten werden nach eigenem Ermessen durchgeführt. Er kann jederzeit entscheiden, wann und von wo aus er lernen möchte.

> *Bei TECH gibt es KEINE Präsenzveranstaltungen (an denen man nie teilnehmen kann)“*

Die international umfassendsten Lehrpläne

TECH zeichnet sich dadurch aus, dass sie die umfassendsten Studiengänge im universitären Umfeld anbietet. Dieser Umfang wird durch die Erstellung von Lehrplänen erreicht, die nicht nur die wesentlichen Kenntnisse, sondern auch die neuesten Innovationen in jedem Bereich abdecken.

Durch ihre ständige Aktualisierung ermöglichen diese Programme den Studenten, mit den Veränderungen des Marktes Schritt zu halten und die von den Arbeitgebern am meisten geschätzten Fähigkeiten zu erwerben. Auf diese Weise erhalten die Studenten, die ihr Studium bei TECH absolvieren, eine umfassende Vorbereitung, die ihnen einen bedeutenden Wettbewerbsvorteil verschafft, um in ihrer beruflichen Laufbahn voranzukommen.

Und das von jedem Gerät aus, ob PC, Tablet oder Smartphone.

> *Das Modell der TECH ist asynchron, d. h. Sie können an Ihrem PC, Tablet oder Smartphone studieren, wo immer Sie wollen, wann immer Sie wollen und so lange Sie wollen“*

Case studies oder Fallmethode

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Wirtschaftshochschulen der Welt. Sie wurde 1912 entwickelt, damit Studenten der Rechtswissenschaften das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernten, sondern auch mit realen komplexen Situationen konfrontiert wurden. Auf diese Weise konnten sie fundierte Entscheidungen treffen und Werturteile darüber fällen, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

Bei diesem Lehrmodell ist es der Student selbst, der durch Strategien wie *Learning by doing* oder *Design Thinking*, die von anderen renommierten Einrichtungen wie Yale oder Stanford angewandt werden, seine berufliche Kompetenz aufbaut.

Diese handlungsorientierte Methode wird während des gesamten Studiengangs angewandt, den der Student bei TECH absolviert. Auf diese Weise wird er mit zahlreichen realen Situationen konfrontiert und muss Wissen integrieren, recherchieren, argumentieren und seine Ideen und Entscheidungen verteidigen. All dies unter der Prämisse, eine Antwort auf die Frage zu finden, wie er sich verhalten würde, wenn er in seiner täglichen Arbeit mit spezifischen, komplexen Ereignissen konfrontiert würde.

Relearning-Methode

Bei TECH werden die *case studies* mit der besten 100%igen Online-Lernmethode ergänzt: *Relearning*.

Diese Methode bricht mit traditionellen Lehrmethoden, um den Studenten in den Mittelpunkt zu stellen und ihm die besten Inhalte in verschiedenen Formaten zu vermitteln. Auf diese Weise kann er die wichtigsten Konzepte der einzelnen Fächer wiederholen und lernen, sie in einem realen Umfeld anzuwenden.

In diesem Sinne und gemäß zahlreicher wissenschaftlicher Untersuchungen ist die Wiederholung der beste Weg, um zu lernen. Aus diesem Grund bietet TECH zwischen 8 und 16 Wiederholungen jedes zentralen Konzepts innerhalb ein und derselben Lektion, die auf unterschiedliche Weise präsentiert werden, um sicherzustellen, dass das Wissen während des Lernprozesses vollständig gefestigt wird.

Das Relearning ermöglicht es Ihnen, mit weniger Aufwand und mehr Leistung zu lernen, sich mehr auf Ihre Spezialisierung einzulassen, einen kritischen Geist zu entwickeln, Argumente zu verteidigen und Meinungen zu kontrastieren: eine direkte Gleichung zum Erfolg.

Ein 100%iger virtueller Online-Campus mit den besten didaktischen Ressourcen

Um ihre Methodik wirksam anzuwenden, konzentriert sich TECH darauf, den Studenten Lehrmaterial in verschiedenen Formaten zur Verfügung zu stellen: Texte, interaktive Videos, Illustrationen und Wissenskarten, um nur einige zu nennen. Sie alle werden von qualifizierten Lehrkräften entwickelt, die ihre Arbeit darauf ausrichten, reale Fälle mit der Lösung komplexer Situationen durch Simulationen, dem Studium von Zusammenhängen, die für jede berufliche Laufbahn gelten, und dem Lernen durch Wiederholung mittels Audios, Präsentationen, Animationen, Bildern usw. zu verbinden.

Die neuesten wissenschaftlichen Erkenntnisse auf dem Gebiet der Neurowissenschaften weisen darauf hin, dass es wichtig ist, den Ort und den Kontext, in dem der Inhalt abgerufen wird, zu berücksichtigen, bevor ein neuer Lernprozess beginnt. Die Möglichkeit, diese Variablen individuell anzupassen, hilft den Menschen, sich zu erinnern und Wissen im Hippocampus zu speichern, um es langfristig zu behalten. Dies ist ein Modell, das als *Neurocognitive context-dependent e-learning* bezeichnet wird und in diesem Hochschulstudium bewusst angewendet wird.

Zum anderen, auch um den Kontakt zwischen Mentor und Student so weit wie möglich zu begünstigen, wird eine breite Palette von Kommunikationsmöglichkeiten angeboten, sowohl in Echtzeit als auch zeitversetzt (internes Messaging, Diskussionsforen, Telefondienst, E-Mail-Kontakt mit dem technischen Sekretariat, Chat und Videokonferenzen).

Darüber hinaus wird dieser sehr vollständige virtuelle Campus den Studenten der TECH die Möglichkeit geben, ihre Studienzeiten entsprechend ihrer persönlichen Verfügbarkeit oder ihren beruflichen Verpflichtungen zu organisieren. Auf diese Weise haben sie eine globale Kontrolle über die akademischen Inhalte und ihre didaktischen Hilfsmittel, in Übereinstimmung mit ihrer beschleunigten beruflichen Weiterbildung.

> *Der Online-Studienmodus dieses Programms wird es Ihnen ermöglichen, Ihre Zeit und Ihr Lerntempo zu organisieren und an Ihren Zeitplan anzupassen“*

Die Wirksamkeit der Methode wird durch vier Schlüsselergebnisse belegt:

1. Studenten, die diese Methode anwenden, nehmen nicht nur Konzepte auf, sondern entwickeln auch ihre geistigen Fähigkeiten durch Übungen zur Bewertung realer Situationen und zur Anwendung ihres Wissens.
2. Das Lernen basiert auf praktischen Fähigkeiten, die es den Studenten ermöglichen, sich besser in die reale Welt zu integrieren.
3. Eine einfachere und effizientere Aufnahme von Ideen und Konzepten wird durch die Verwendung von Situationen erreicht, die aus der Realität entstanden sind.
4. Das Gefühl der Effizienz der investierten Anstrengung wird zu einem sehr wichtigen Anreiz für die Studenten, was sich in einem größeren Interesse am Lernen und einer Steigerung der Zeit, die für die Arbeit am Kurs aufgewendet wird, niederschlägt.

Die von ihren Studenten am besten bewertete Hochschulmethodik

Die Ergebnisse dieses innovativen akademischen Modells lassen sich an der Gesamtzufriedenheit der Absolventen der TECH ablesen.

Die Studenten bewerten die pädagogische Qualität, die Qualität der Materialien, die Struktur und die Ziele der Kurse als ausgezeichnet. Es überrascht nicht, dass die Einrichtung im global score Index mit 4,9 von 5 Punkten die von ihren Studenten am besten bewertete Universität ist.

Sie können von jedem Gerät mit Internetanschluss (Computer, Tablet, Smartphone) auf die Studieninhalte zugreifen, da TECH in Sachen Technologie und Pädagogik führend ist.

Sie werden die Vorteile des Zugangs zu simulierten Lernumgebungen und des Lernens durch Beobachtung, d. h. Learning from an expert, nutzen können.

In diesem Programm stehen Ihnen die besten Lehrmaterialien zur Verfügung, die sorgfältig vorbereitet wurden:

Studienmaterial

Alle didaktischen Inhalte werden von den Fachkräfte, die den Kurs unterrichten werden, speziell für den Kurs erstellt, so dass die didaktische Entwicklung wirklich spezifisch und konkret ist.

Diese Inhalte werden dann auf ein audiovisuelles Format übertragen, das unsere Online-Arbeitsweise mit den neuesten Techniken ermöglicht, die es uns erlauben, Ihnen eine hohe Qualität in jedem der Stücke zu bieten, die wir Ihnen zur Verfügung stellen werden.

Übungen für Fertigkeiten und Kompetenzen

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein Spezialist im Rahmen der Globalisierung, in der wir leben, entwickeln muss.

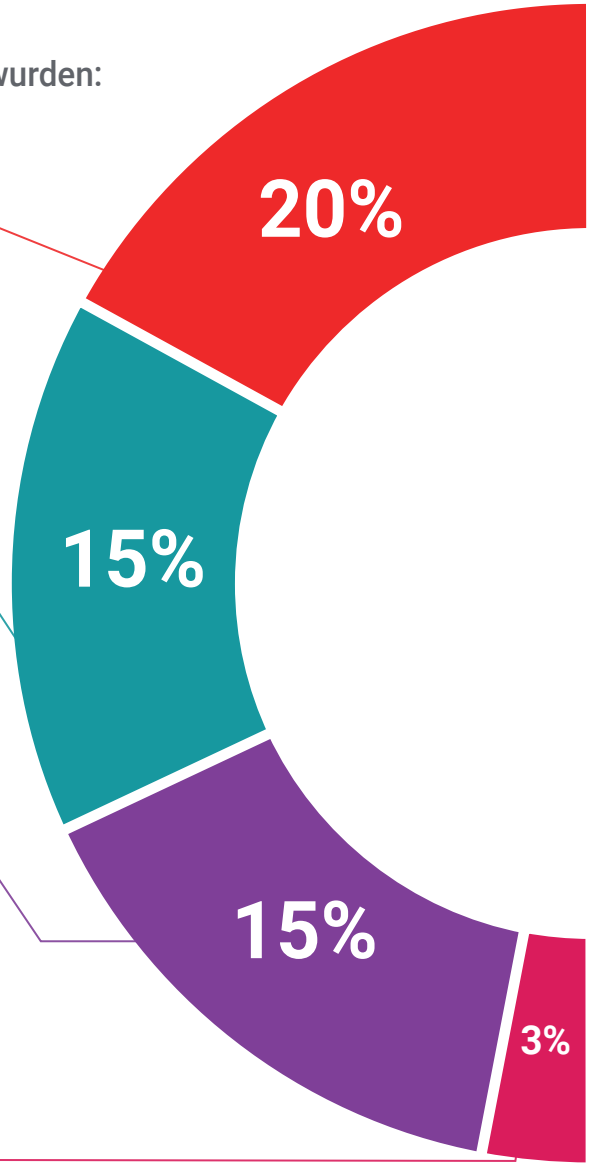
Interaktive Zusammenfassungen

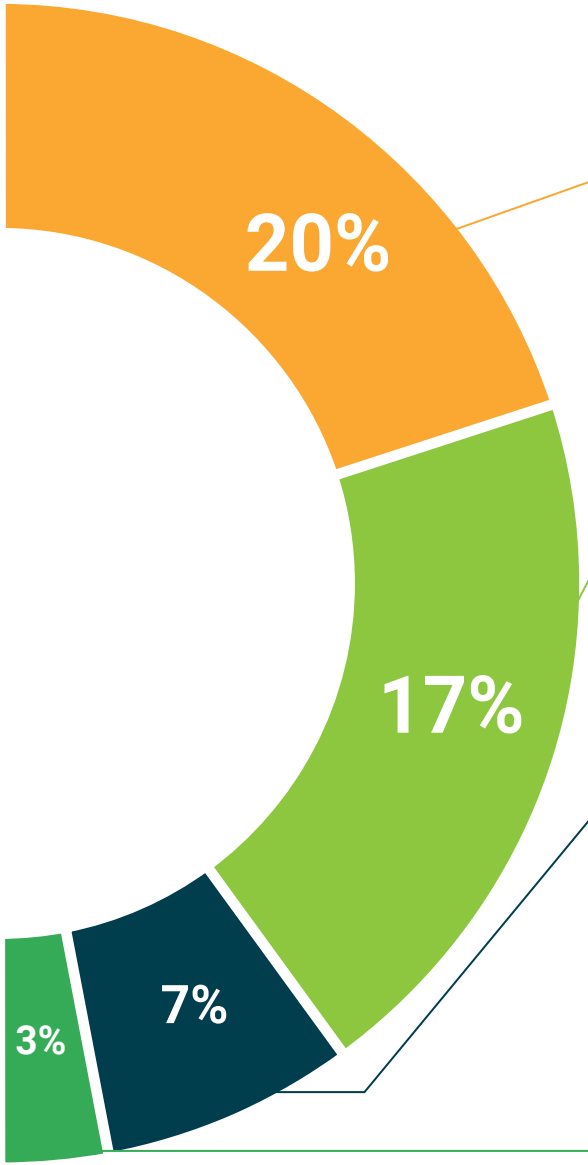
Wir präsentieren die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu festigen.

Dieses einzigartige System für die Präsentation multimedialer Inhalte wurde von Microsoft als „Europäische Erfolgsgeschichte" ausgezeichnet.

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente, internationale Leitfäden... In unserer virtuellen Bibliothek haben Sie Zugang zu allem, was Sie für Ihre Ausbildung benötigen.





Case Studies

Sie werden eine Auswahl der besten *case studies* zu diesem Thema bearbeiten. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.

Testing & Retesting

Während des gesamten Programms werden Ihre Kenntnisse in regelmäßigen Abständen getestet und wiederholt. Wir tun dies auf 3 der 4 Ebenen der Millerschen Pyramide.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

Das sogenannte *Learning from an Expert* stärkt das Wissen und das Gedächtnis und schafft Vertrauen in unsere zukünftigen schwierigen Entscheidungen.

Kurzanleitungen zum Vorgehen

TECH bietet die wichtigsten Inhalte des Kurses in Form von Arbeitsblättern oder Kurzanleitungen an. Ein synthetischer, praktischer und effektiver Weg, um dem Studenten zu helfen, in seinem Lernen voranzukommen.

07

Lehrkörper

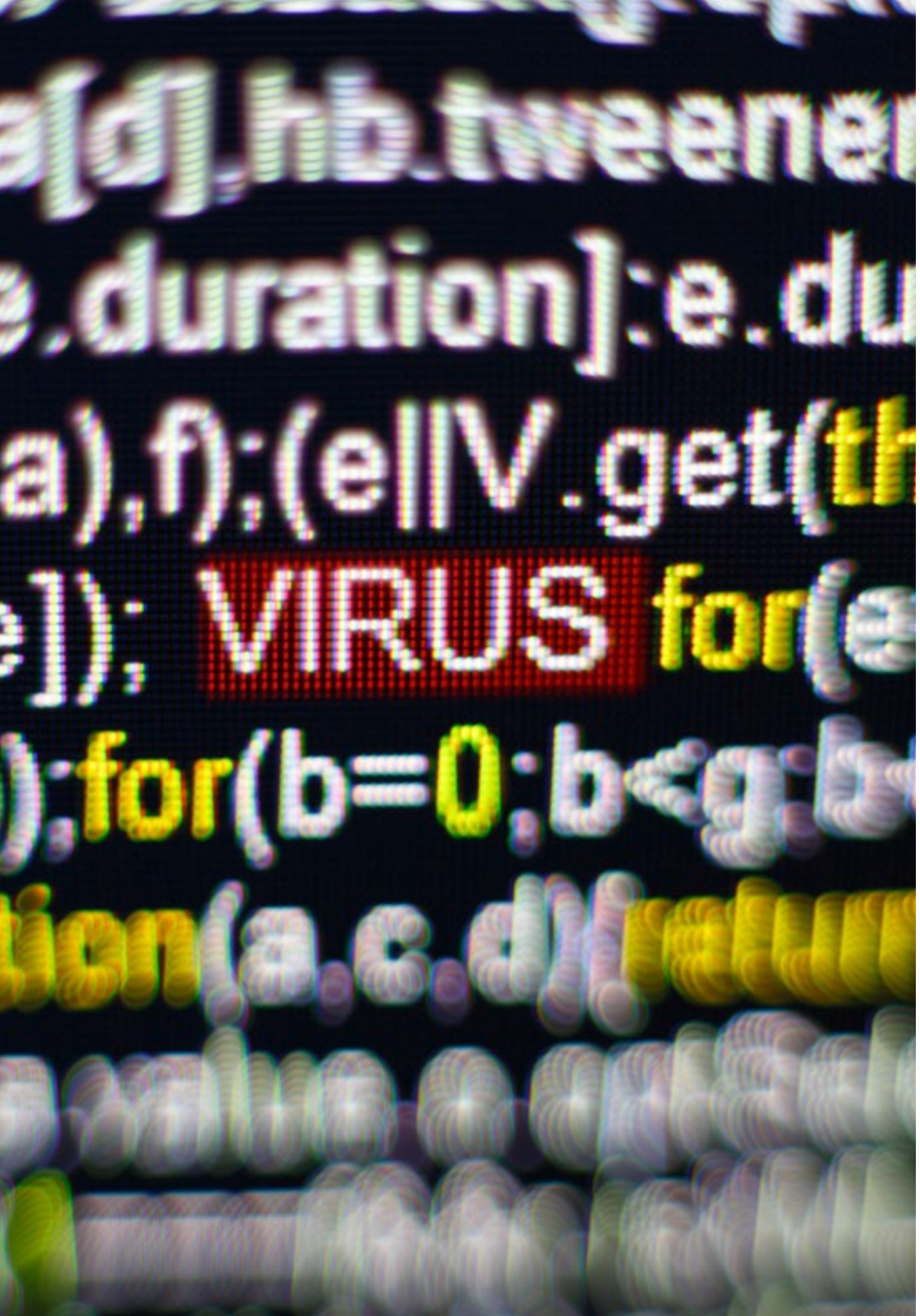
Die Philosophie von TECH basiert darauf, jedem die vollständigsten und aktuellsten Universitätsprogramme der akademischen Landschaft zur Verfügung zu stellen. Aus diesem Grund führt TECH einen sorgfältigen Prozess zur Zusammenstellung ihrer Lehrkörper durch. Daher nehmen an diesem weiterbildenden Masterstudiengang echte Experten für die Anwendung von künstlicher Intelligenz im Bereich der Cybersicherheit teil. Auf diese Weise haben sie zahlreiche Lehrinhalte entwickelt, die sich durch ihre hohe Qualität auszeichnen und den Anforderungen des Arbeitsmarktes entsprechen. Die Studenten kommen so in den Genuss einer tiefgreifenden Erfahrung, die ihre Berufsaussichten verbessern wird.

Das Dozententeam dieses Universitätsprogramms setzt sich aus führenden Experten für die Implementierung von künstlicher Intelligenz in der Cybersicherheit zusammen“

Leitung

Dr. Peralta Martín-Palomino, Arturo

- CEO und CTO bei Prometeus Global Solutions
- CTO bei Korporate Technologies
- CTO bei AI Shepherds GmbH
- Berater und strategischer Unternehmensberater bei Alliance Medical
- Direktor für Design und Entwicklung bei DocPath
- Promotion in Computertechnik an der Universität von Castilla La Mancha
- Promotion in Wirtschaftswissenschaften, Unternehmen und Finanzen an der Universität Camilo José Cela
- Promotion in Psychologie an der Universität von Castilla La Mancha
- Masterstudiengang Executive MBA von der Universität Isabel I
- Masterstudiengang in Business und Marketing Management von der Universität Isabel I
- Masterstudiengang in Big Data bei Formación Hadoop
- Masterstudiengang in Fortgeschrittene Informationstechnologie an der Universität von Castilla La Mancha
- Mitglied von: Forschungsgruppe SMILE



Professoren

Hr. Del Rey Sánchez, Alejandro

- Verantwortlich für die Umsetzung von Programmen zur Verbesserung der taktischen Versorgung in Notfällen
- Hochschulabschluss in Ingenieurwesen für industrielle Organisation
- Zertifizierung in *Big Data und Business Analytics*
- Zertifizierung in Microsoft Excel Advanced, VBA, KPI und DAX
- Zertifizierung in CIS Telekommunikation und Informationssysteme

Eine einzigartige, wichtige und entscheidende Fortbildungserfahrung, die Ihre berufliche Entwicklung fördert"

08

Qualifizierung

Der Weiterbildender Masterstudiengang in Künstliche Intelligenz in der Cybersicherheit garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Global University ausgestellten Diplom.

Schließen Sie dieses Programm erfolgreich ab und erhalten Sie Ihren Universitätsabschluss ohne lästige Reisen oder Formalitäten”

Mit diesem Programm erwerben Sie den von **TECH Global University**, der größten digitalen Universität der Welt, bestätigten eigenen Titel **Weiterbildender Masterstudiengang in Künstliche Intelligenz in der Cybersicherheit**.

TECH Global University ist eine offizielle europäische Universität, die von der Regierung von Andorra ***(Amtsblatt)*** öffentlich anerkannt ist. Andorra ist seit 2003 Teil des Europäischen Hochschulraums (EHR). Der EHR ist eine von der Europäischen Union geförderte Initiative, die darauf abzielt, den internationalen Ausbildungsrahmen zu organisieren und die Hochschulsysteme der Mitgliedsländer dieses Raums zu vereinheitlichen. Das Projekt fördert gemeinsame Werte, die Einführung gemeinsamer Instrumente und die Stärkung der Mechanismen zur Qualitätssicherung, um die Zusammenarbeit und Mobilität von Studenten, Forschern und Akademikern zu verbessern.

Dieser eigene Abschluss der **TECH Global University** ist ein europäisches Programm zur kontinuierlichen Weiterbildung und beruflichen Fortbildung, das den Erwerb von Kompetenzen in seinem Wissensgebiet garantiert und dem Lebenslauf des Studenten, der das Programm absolviert, einen hohen Mehrwert verleiht.

Titel: **Weiterbildender Masterstudiengang in Künstliche Intelligenz in der Cybersicherheit**

Modalität: **online**

Dauer: **12 Monate**

Akkreditierung: **90 ECTS**


tech global university

Hr./Fr. _____, mit der Ausweis-Nr. _____ hat erfolgreich bestanden und den folgenden Abschluss erworben:

Weiterbildender Masterstudiengang in Künstliche Intelligenz in der Cybersicherheit

Es handelt sich um einen eigenen Abschluss mit einer Dauer von 2.700 Stunden, was 90 ECTS entspricht, mit Anfangsdatum am dd/mm/aaaa und Enddatum am dd/mm/aaaa.

TECH Global University ist eine von der Regierung Andorras am 31. Januar 2024 offiziell anerkannte Universität, die dem Europäischen Hochschulraum (EHR) angehört.

Andorra la Vella, den 28. Februar 2024

Dr. Pedro Navarro Illana
Rektor

einzigartiger Code TECH: AFWOR23S techtitute.com/titel


Weiterbildender Masterstudiengang in Künstliche Intelligenz in der Cybersicherheit

Allgemeiner Aufbau des Lehrplans

Fachkategorie	Stunden
Obligatorisch (OB)	90
Wahlfach(OP)	0
Externes Praktikum (PR)	0
Masterarbeit (TFM)	0
	Summe 90

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	ECTS	Kategorie
1°	Grundlagen der künstlichen Intelligenz	4	OB
1°	Datentypen und Datenlebenszyklus	4	OB
1°	Daten in der künstlichen Intelligenz	4	OB
1°	Data Mining. Auswahl, Vorverarbeitung und Transformation	4	OB
1°	Algorithmik und Komplexität in der künstlichen Intelligenz	4	OB
1°	Intelligente Systeme	4	OB
1°	Maschinelles Lernen und Data Mining	4	OB
1°	Neuronale Netze, die Grundlage von Deep Learning	4	OB
1°	Training Tiefer Neuronaler Netze	4	OB
1°	Anpassung von Modellen und Training mit TensorFlow	4	OB
1°	Deep Computer Vision mit Convolutional Neural Networks	4	OB
1°	Natürliche Sprachverarbeitung (NLP) mit rekurrenten neuronalen Netzen (RNN) und Aufmerksamkeit	4	OB
1°	Autoencoder, GANs und Diffusionsmodelle	4	OB
1°	Bio-inspiriertes Computing	4	OB
1°	Künstliche Intelligenz: Strategien und Anwendungen	4	OB
1°	Cybersicherheit und Analyse moderner Bedrohungen mit ChatGPT	4	OB
1°	Erkennung und Vorbeugung von Angriffen mit Modellen der generativen künstlichen Intelligenz	4	OB
1°	Moderne Kryptographie mit ChatGPT-Unterstützung beim Datenschutz	4	OB
1°	Digitale Forensik und KI-gestützte Reaktion auf Vorfälle	9	OB
1°	Prädiktive Modelle für die proaktive Verteidigung in der Cybersicherheit mit ChatGPT	9	OB

Dr. Pedro Navarro Illana
Rektor

tech global university

*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH Global University die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech global university

Weiterbildender Masterstudiengang

Künstliche Intelligenz in der Cybersicherheit

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Global University**
- Akkreditierung: **90 ECTS**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Weiterbildender Masterstudiengang

Künstliche Intelligenz in der Cybersicherheit

tech global university