



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences



Lebenszyklus der Maschine Lernen Modelle

Untertitel

► Violeta Vogel, TI BFH

Agenda

- ▶ Definitionen
 - ▶ Modelllebenszyklus, MLOps , DevOps
- ▶ Gestaltungsprinzipien
- ▶ Rollen
- ▶ Modell-Lebenszyklus-Architekturen: CRISP, AWS, Gen AI
- ▶ Modell-Lebenszyklus basierend auf CRISP-DM:
 - ▶ Identifizierung des Geschäftsziels und des ROI von ML
 - ▶ Datenverständnis
 - ▶ Datenaufbereitung
 - ▶ DataOps und Daten-Engineering
 - ▶ Modelltraining
 - ▶ Modellbewertung
 - ▶ Modell-Implementierung und Überwachung
 - ▶ Gut durchdachte ML-Designprinzipien
 - ▶ MLOps und DevOps
 - ▶ Modellumschulung
- ▶ Modell Governance

Wer wir sind ?

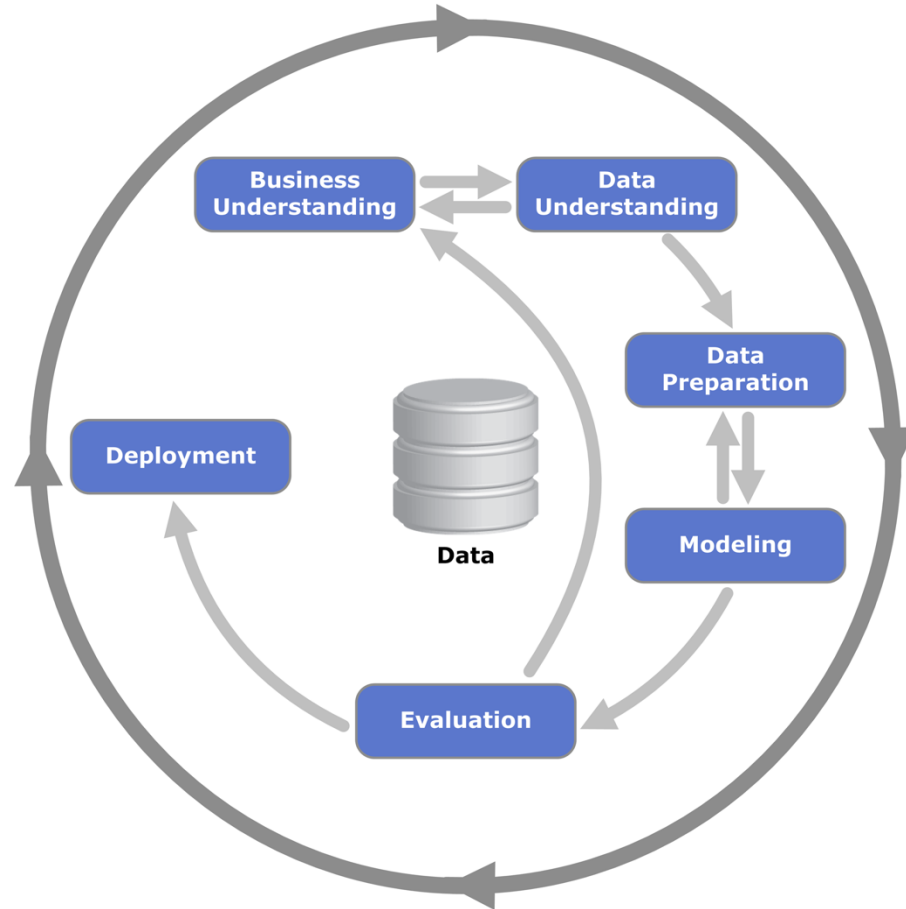
MLOps , ModelOps ,
Modelllebenszyklus, ML-
Engineering

DevOps, AI-Ops,
Softwareentwicklung

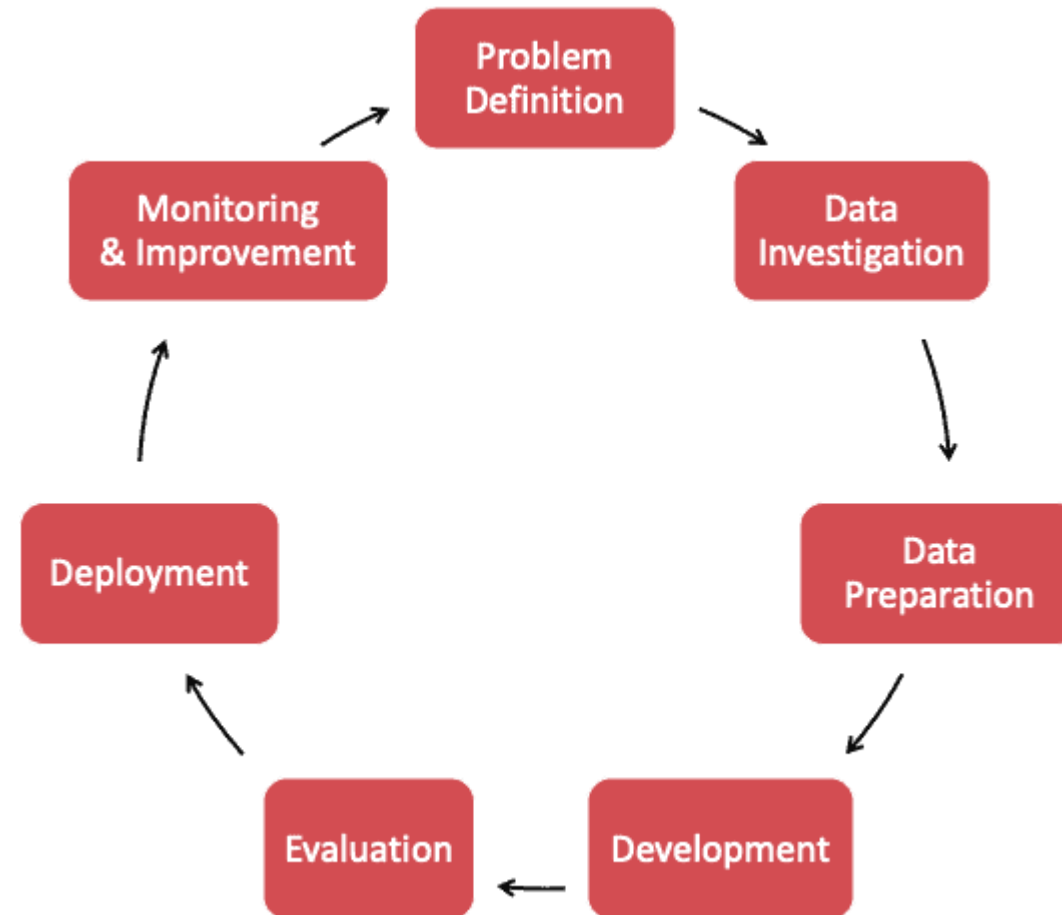
Datenoperationen,
Datenautomatisierung

- ▶ Finden Sie alle möglichen Definitionen zu diesem Thema.
- ▶ Beschreiben Sie sie
- ▶ Halten Sie eine kurze Präsentation

ML LifeCycle CRISP-DM

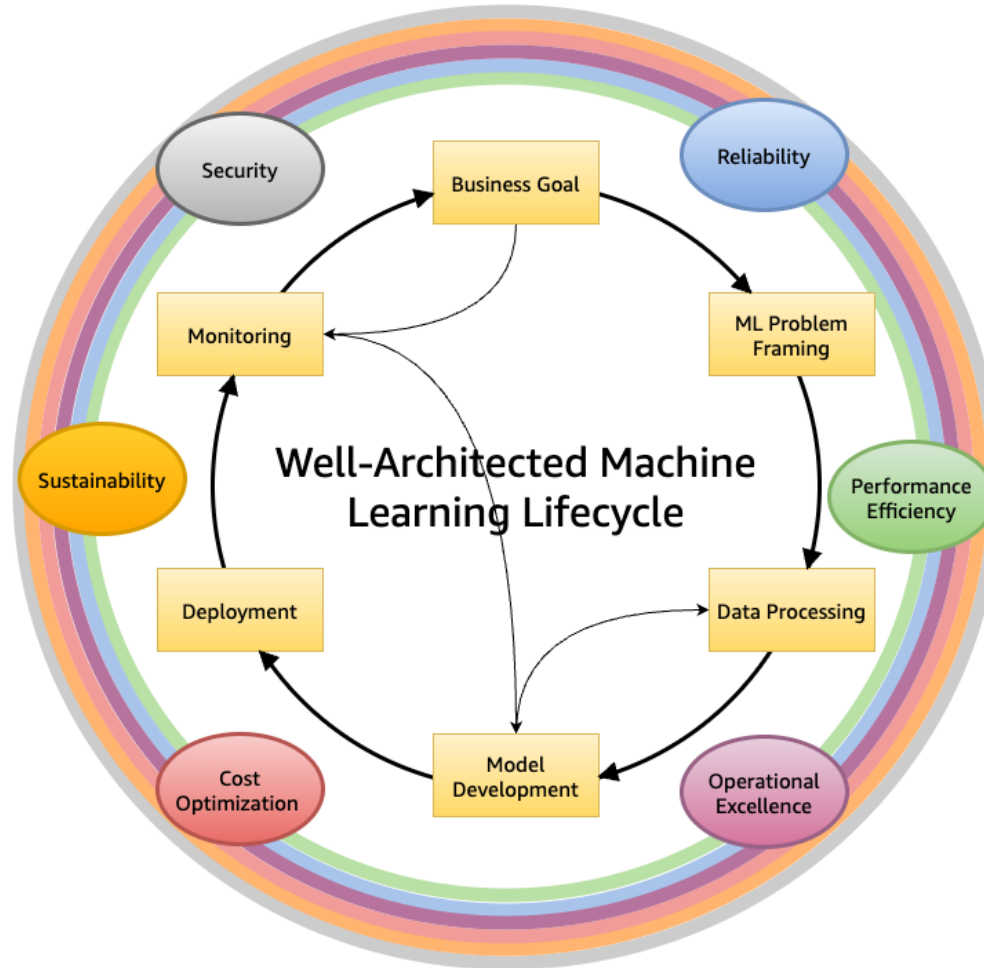


Gen AI Lebenszyklus



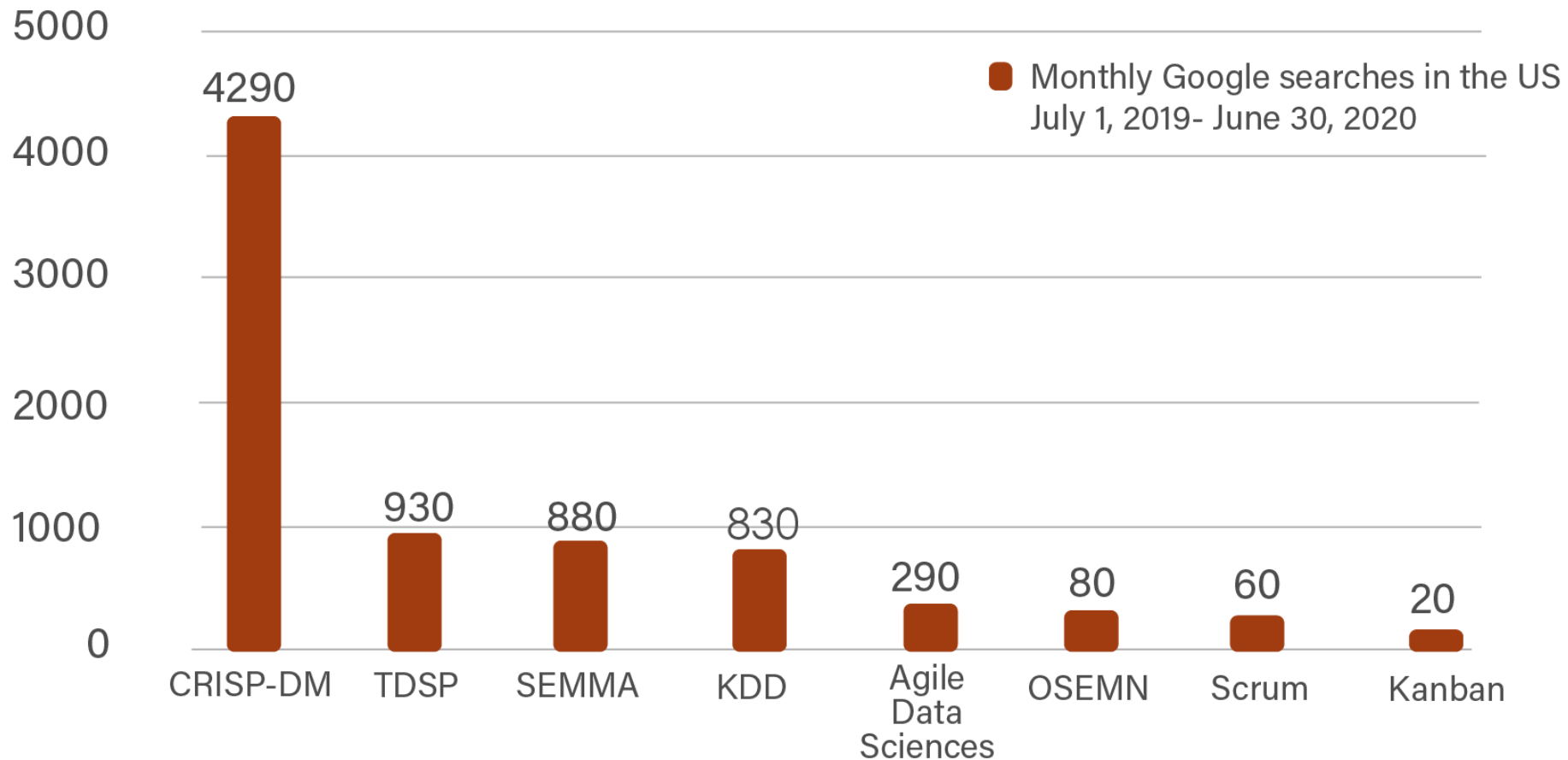
ML-Lebenszyklus AWS

Untertitel



<https://docs.aws.amazon.com/wellarchitected/latest/machine-learning-lens/well-architected-machine-learning-lifecycle.html>

Processes Search Volume



Wie eine Kreditkarte das großartige Modell zerstören kann...

Geschäftsverständnis

Was braucht das Unternehmen?

1. **Geschäftsziele festlegen:** Sie sollten zunächst „aus betriebswirtschaftlicher Sicht genau verstehen, was der Kunde wirklich erreichen will“ und anschließend die Kriterien für den Geschäftserfolg definieren.
2. **Situationsanalyse:** Ressourcenverfügbarkeit und Projektanforderungen ermitteln, Risiken und Eventualitäten einschätzen und eine Kosten-Nutzen-Analyse durchführen.
3. **Data-Mining-Ziele festlegen:** Zusätzlich zur Definition der Geschäftsziele sollten Sie auch definieren, wie Erfolg aus technischer Data-Mining-Perspektive aussieht.
4. **Projektplan erstellen:** Technologien und Werkzeuge auswählen und detaillierte Pläne für jede Projektphase definieren.

Datenverständnis

Welche Daten haben wir? Welche benötigen wir? Sind sie sauber?

1. **Sammeln Sie Ausgangsdaten:** Beschaffen Sie die notwendigen Daten und laden Sie diese gegebenenfalls in Ihr Analysetool.
2. **Daten beschreiben:** Untersuchen Sie die Daten und dokumentieren Sie deren Oberflächeneigenschaften wie Datenformat, Anzahl der Datensätze oder Feldbezeichnungen.
3. **Daten erkunden:** Gehen Sie den Daten auf den Grund. Fragen Sie sie ab, visualisieren Sie sie und identifizieren Sie Zusammenhänge zwischen den Daten.
4. **Überprüfen Sie die Datenqualität:** Wie sauber/fehlerhaft sind die Daten? Dokumentieren Sie alle Qualitätsprobleme.

Datenaufbereitung

Wie organisieren wir Daten für die Modellierung?

1. **Daten auswählen:** Bestimmen Sie, welche Datensätze verwendet werden, und dokumentieren Sie die Gründe für die Einbeziehung/den Ausschluss.
2. **Datenbereinigung:** Dies ist oft der zeitaufwändigste Schritt. Ohne sie besteht die Gefahr, dass fehlerhafte Daten zu minderwertigen Ergebnissen führen. Üblicherweise werden dabei fehlerhafte Werte korrigiert, ergänzt oder entfernt.
3. **Daten erstellen:** Neue Attribute ableiten, die hilfreich sind. Beispielsweise den Body-Mass-Index einer Person aus den Feldern für Größe und Gewicht berechnen.
4. **Daten integrieren:** Erstellen Sie neue Datensätze, indem Sie Daten aus mehreren Quellen kombinieren.
5. **Daten formatieren:** Formatieren Sie die Daten nach Bedarf neu. Beispielsweise können Sie Zeichenketten, die Zahlen speichern, in numerische Werte umwandeln, um mathematische Operationen durchführen zu können.

Modellentwicklung

Welche Modellierungstechniken sollten wir anwenden?

1. **Modellierungstechniken auswählen** : Bestimmen Sie, welche Algorithmen Sie ausprobieren möchten (z. B. Regression, neuronales Netz).
2. **Testdesign erstellen**: Je nach gewähltem Modellierungsansatz müssen Sie die Daten möglicherweise in Trainings-, Test- und Validierungsdatensätze aufteilen.
3. **Modell erstellen**: So glamourös das auch klingen mag, es könnte sich dabei lediglich um die Ausführung einiger weniger Codezeilen wie „reg = LinearRegression ().fit(X, y)“ handeln.
4. **Bewertung des Modells**: Im Allgemeinen konkurrieren mehrere Modelle miteinander, und der Datenwissenschaftler muss die Modellergebnisse auf der Grundlage von Domänenwissen, den vordefinierten Erfolgskriterien und dem Testdesign interpretieren.

Würden Sie ein Modell mit einer Genauigkeit von 4 % in die Produktion einführen?

Ja!

- ▶ Kundenzahl 3,5 Mio.
- ▶ 1 Brief kostet 1 CHF
- ▶ Gesamtkosten ohne Modell = 3,5 Mio. CHF
- ▶ **Gesamtkosten mit Modell 450.000 CHF**

Anzahl Kunden	1.000.000											
		10	20	30	40	50	60	70	80	90		100
Präzision												

Modellbewertung

Welches Modell erfüllt die Geschäftsziele am besten?

1. **Ergebnisse auswerten:** Erfüllen die Modelle die Kriterien für den Geschäftserfolg? Welches/Welche Modell(e) sollten wir für das Unternehmen freigeben?
2. **Überprüfungsprozess:** Überprüfen Sie die geleistete Arbeit. Wurde etwas übersehen? Wurden alle Schritte ordnungsgemäß ausgeführt? Fassen Sie die Ergebnisse zusammen und korrigieren Sie gegebenenfalls Fehler.
3. **Nächste Schritte festlegen:** Auf Grundlage der drei vorangegangenen Aufgaben entscheiden Sie, ob Sie mit der Bereitstellung fortfahren, weitere Iterationen durchführen oder neue Projekte initiieren.

Einsatz

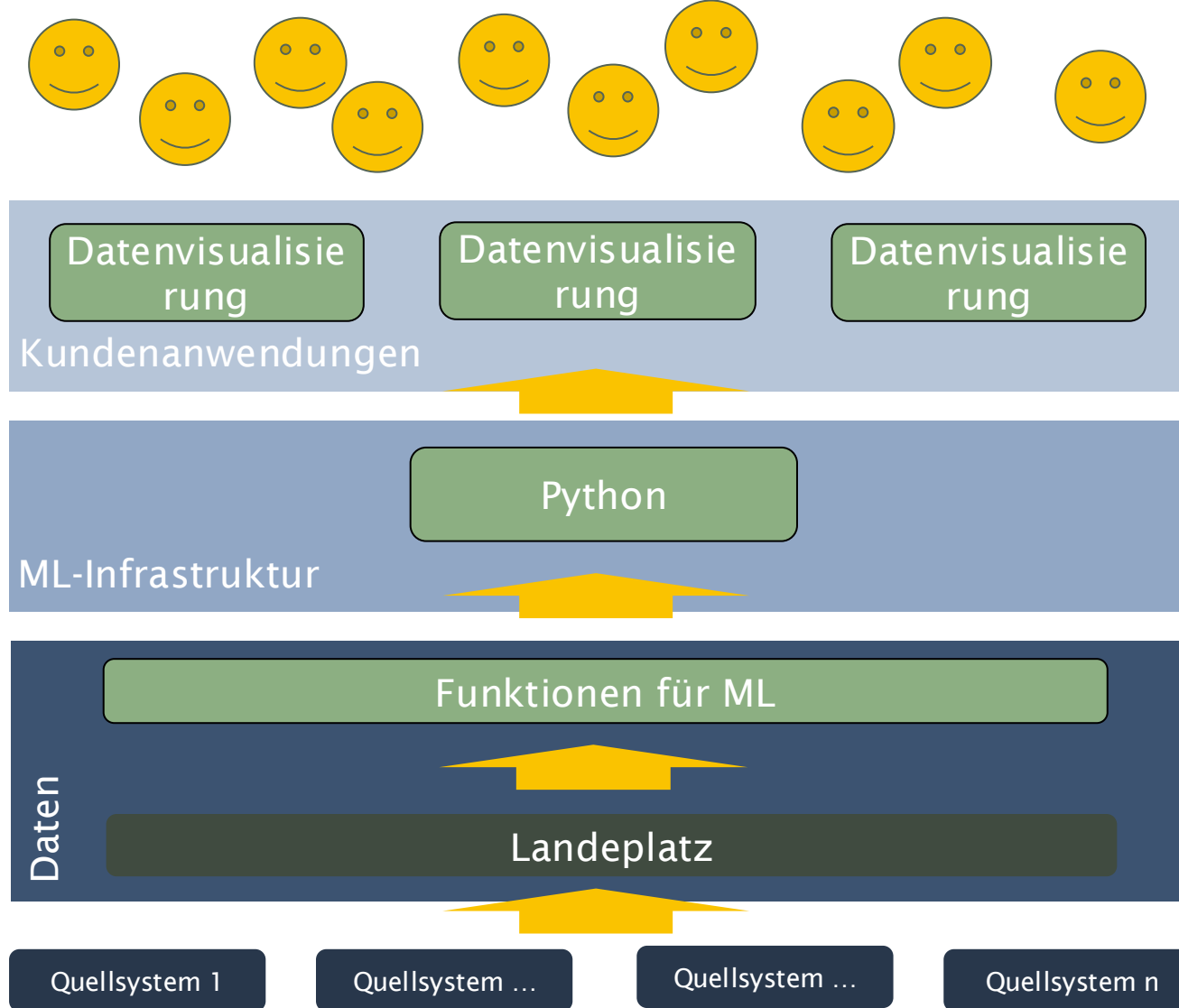
Wie erhalten die Interessengruppen Zugriff auf die Ergebnisse?

1. **Bereitstellungsplan:** Entwickeln und dokumentieren Sie einen Plan für die Bereitstellung des Modells.
2. **Überwachung und Wartung planen:** Entwickeln Sie einen gründlichen Überwachungs- und Wartungsplan, um Probleme während der Betriebsphase (oder der Nachprojektphase) eines Modells zu vermeiden.
3. **Abschlussbericht erstellen:** Das Projektteam erstellt eine Zusammenfassung des Projekts, die auch eine abschließende Präsentation der Ergebnisse des Data-Minings beinhalten kann.
4. **Projektrückblick:** Führen Sie eine Projektrückblicksanalyse durch, um zu besprechen, was gut lief, was hätte besser laufen können und wie man sich in Zukunft verbessern kann.

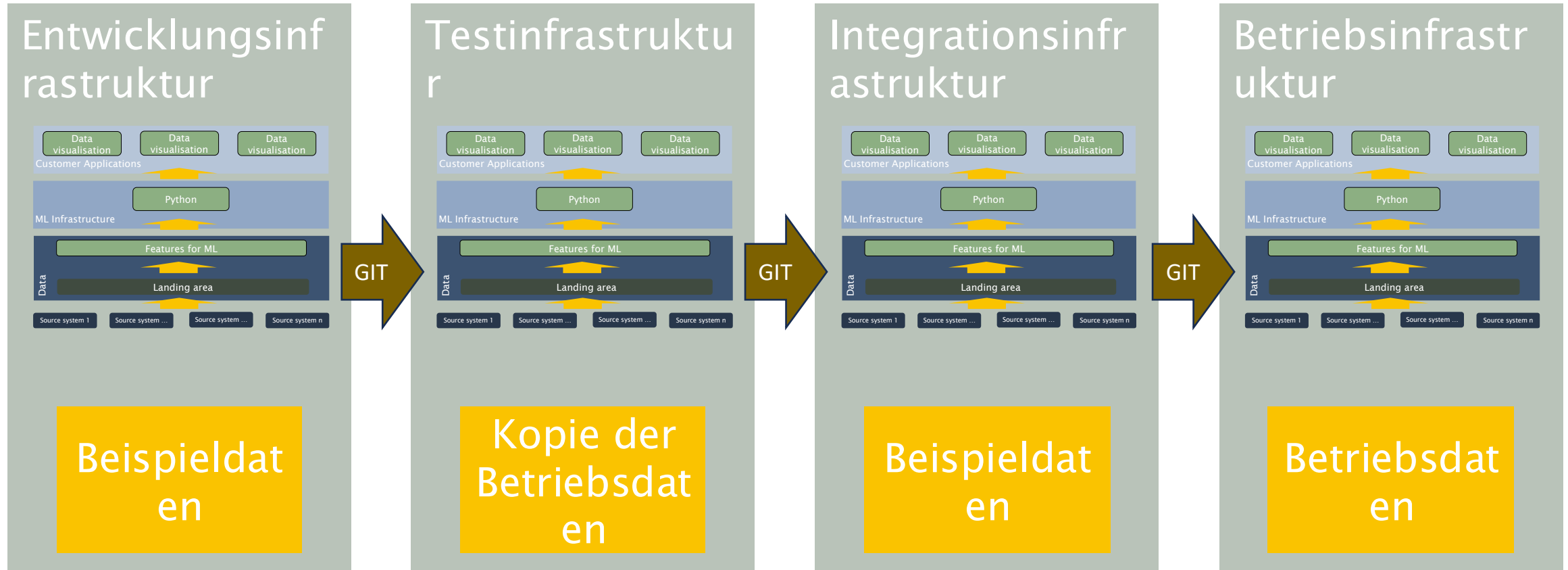
Wir betrachten den ML- Lebenszyklus in Unternehmen.

- ▶ „Nur ein Prozent der Beschäftigten arbeiten in Unternehmen, die jünger als zwei Jahre sind, während 60 Prozent in Unternehmen arbeiten, die älter als zehn Jahre sind.“ [1]
- ▶ „Es braucht 43 Start-ups, bis nach zehn Jahren nur noch ein einziges Unternehmen existiert, das außer dem Gründer noch jemanden beschäftigt.“ [1]
- ▶ Erfolgreiche Unternehmen, die ihren bisherigen Erfolg ausbauen möchten, sollten über die Lösungen von Start-ups hinausblicken. Kennzahlen wie Personalgewinnung, unternehmensweiter Support, Geschäftskontinuität und Preis sind entscheidende Leistungsindikatoren (KPIs).

Technologie-Stack für Unternehmen



Technologie-Stack für Unternehmen



Was ist MLOps ?

- ▶ Maschinelles Lernen (ML) + Operationen (Ops) = MLOps
- ▶ MLOps ist der Prozess des Entwerfens, Erstellens, Ermöglichens und Unterstützens des effizienten Einsatzes von ML-Modellen in der Produktion, um die Geschäftstätigkeit kontinuierlich zu verbessern.
- ▶ MLOps basiert auf Automatisierung, Agilität und Zusammenarbeit zur Verbesserung der Qualität.
- ▶ „ MLOps hat zum Ziel, die Entwicklung und das Management von ML-Modellen sowie die Operationalisierung der ML-Pipeline zu standardisieren. Es unterstützt die Freigabe, Aktivierung, Überwachung, Leistungsverfolgung, Verwaltung, Wiederverwendung, Wartung und Governance von ML-Artefakten“ (Gardner).

Was ist DevOps? (1/2)

- ▶ DevOps ist eine Reihe von technischen und Managementpraktiken, die darauf abzielen, die Geschwindigkeit einer Organisation bei der Veröffentlichung qualitativ hochwertiger Software zu erhöhen.
- ▶ Vorteile: Geschwindigkeit, Zuverlässigkeit, Skalierbarkeit und Sicherheit.
- ▶ Bewährte Verfahren:
 - ▶ **Continuous Integration (CI)** ist der Prozess des kontinuierlichen Testens von Softwareprojekten und der Verbesserung der Qualität auf der Grundlage der Ergebnisse dieser Tests.
 - ▶ **Kontinuierliche Auslieferung (CD)** Die Methode liefert Code ohne menschliches Eingreifen in eine neue Umgebung.

Was ist DevOps? (1/2)

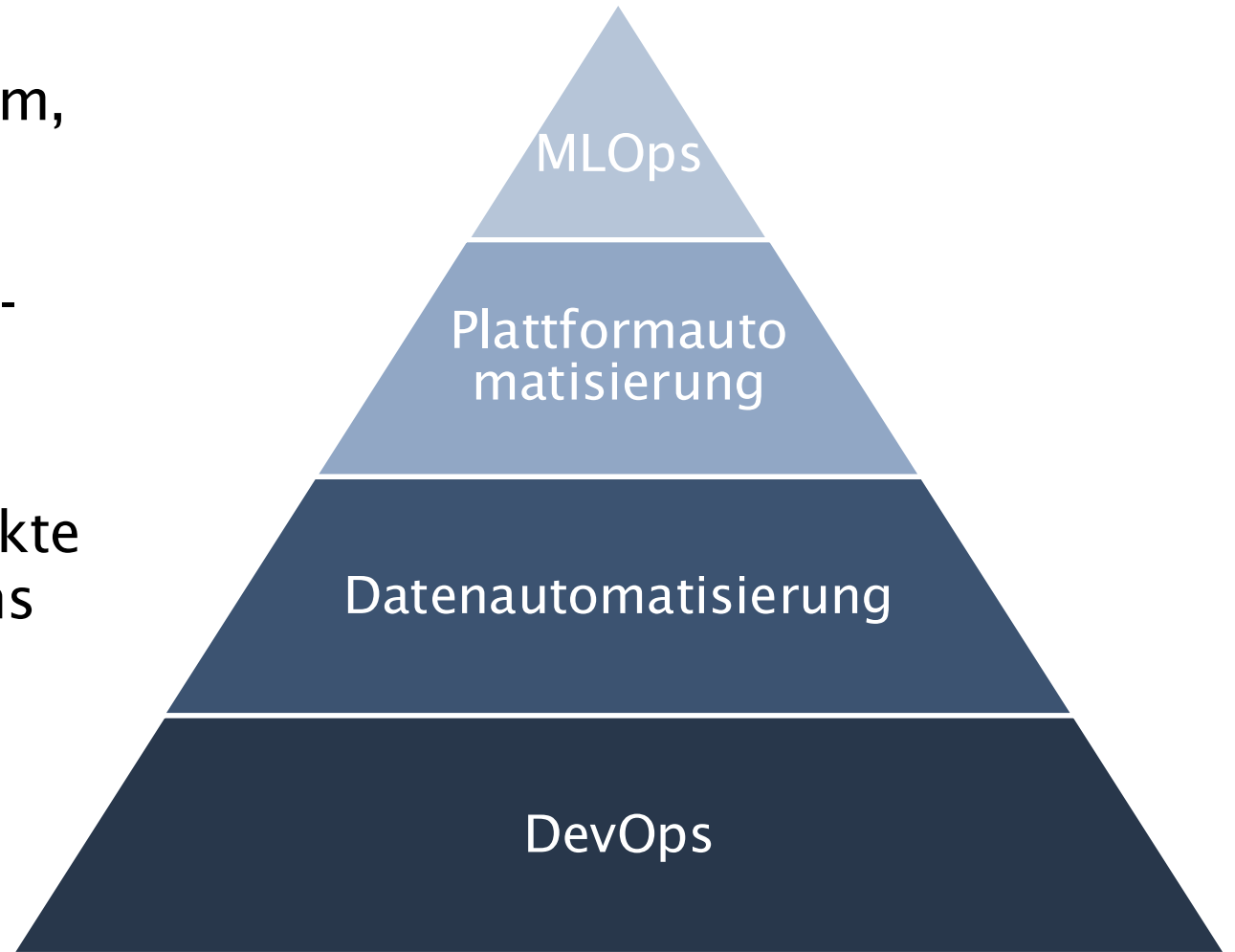
- ▶ **Microservices** sind Softwaredienste mit klar definierten Funktionen, die nur wenige oder gar keine Abhängigkeiten aufweisen. (Flask -> Python-basiertes Microservice-Framework).
- ▶ **Infrastructure as a Code (IaC)** ist der Prozess, bei dem die Infrastruktur in ein Quellcode-Repository eingchecked und anschließend „bereitgestellt“ wird, um Änderungen in dieses Repository zu übertragen.
- ▶ **Monitoring und Instrumentierung** sind die Prozesse und Techniken, die es einer Organisation ermöglichen, Entscheidungen über die Leistungsfähigkeit und Zuverlässigkeit von Softwaresystemen zu treffen.
- ▶ **Effektive technische Kommunikation:** Die Fähigkeit, effektive, wiederholbare und effiziente Kommunikationsmethoden zu entwickeln.

Was ist DevOps? (1/2)

- ▶ **Effektives technisches Projektmanagement** nutzt effizient menschliche und technologische Lösungen wie Ticketsysteme und Tabellenkalkulationen zur Projektsteuerung. Es erfordert die Aufteilung von Problemen in kleine, überschaubare Arbeitspakete, um schrittweise Fortschritte zu erzielen.
- ▶ **Anti-Pattern im Bereich des maschinellen Lernens** ist die Arbeit eines Teams an einem einzigen Produktionsmaschinenmodell, das ein Problem „perfekt“ löst. Stattdessen ist ein skalierbarer und umsichtigerer Ansatz für die Modellentwicklung, der auf täglichen oder wöchentlichen kleineren Erfolgen basiert.

MLOps versus DevOps

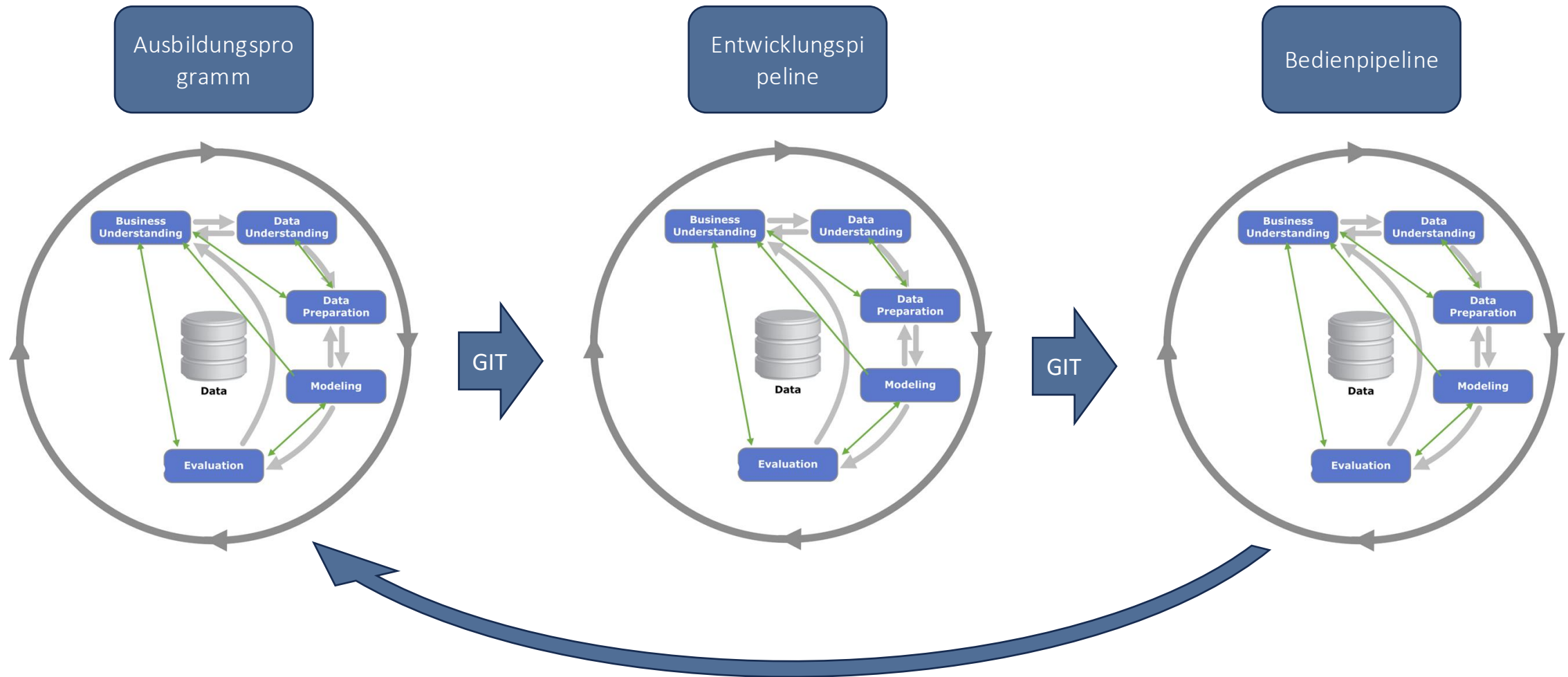
- ▶ Ein ML-System ist ein Softwaresystem, und Softwaresysteme funktionieren effizient und zuverlässig, wenn DevOps- und Data-Engineering-Best-Practices angewendet werden.
- ▶ Eines der Hauptprobleme, die Projekte im Bereich des maschinellen Lernens behindern, ist die fehlende Notwendigkeit einer soliden Grundlage aus DevOps, Datenautomatisierung, Plattformautomatisierung und schließlich echter ML-Automatisierung.



MLOps versus DevOps

Aspekt	MLOps	DevOps
Fokus	ML-Operationen und -Modelle	Softwareentwicklung und IT-Betrieb
Zweck	Optimieren Sie ML-Workflows, Bereitstellung und Betrieb	Optimierung von Softwareentwicklung, -bereitstellung und -betrieb
Hauptkomponenten	Datenpipelines, Modellregister, Überwachung	Code-Repositories, CI/CD-Pipelines, Infrastruktur
Datenverarbeitung	Behandelt ML-spezifische Daten und Modelle	Verwaltet Code und anwendungsbezogene Daten
Hauptherausforderung	Modelldrift, Datenverzerrung, Modellerklärbarkeit	Kontinuierliche Integration, Infrastrukturmanagement
Kernziel	Verbesserung der Bereitstellung und Verwaltung von ML-Modellen	Beschleunigen Sie die Softwarebereitstellung und -zuverlässigkeit
Kernaktivitäten	Modelltraining, Validierung, Überwachung	Codeintegration, Testen, Bereitstellung
Zusammenarbeit	Beteiligt sind Datenwissenschaftler, Analysten und IT-Betriebsmitarbeiter.	Erfordert die Zusammenarbeit zwischen Entwicklung und Betrieb.
Hauptvorteil	Verbesserung der Effizienz und Zuverlässigkeit von ML-Modellen	Steigerung der Geschwindigkeit und Qualität der Softwareentwicklung

ML LifeCycle CRISP-DM



Gestaltungsprinzipien 1/3

- **Verantwortung übertragen** – Setzen Sie die richtigen Fähigkeiten und die richtige Anzahl an Ressourcen in Verbindung mit Verantwortlichkeit und Befähigung ein, um die Produktivität zu steigern.
- **Schutz gewährleisten** – Sicherheitskontrollen auf Systeme und Dienste anwenden, die Modelldaten, Algorithmen, Berechnungen und Endpunkte hosten. Dies gewährleistet einen sicheren und unterbrechungsfreien Betrieb.
- **Ermöglichen Sie Ausfallsicherheit** – Gewährleisten Sie Fehlertoleranz und Wiederherstellbarkeit von ML-Modellen durch Versionskontrolle, Rückverfolgbarkeit und Erklärbarkeit .
- **Ermöglichen Sie die Wiederverwendbarkeit** – Verwenden Sie unabhängige, modulare Komponenten, die gemeinsam genutzt und wiederverwendet werden können. Dies trägt zur Zuverlässigkeit bei, steigert die Produktivität und optimiert die Kosten.

Gestaltungsprinzipien 2/3

- **Reproduzierbarkeit gewährleisten** – Verwenden Sie Versionskontrolle für alle Komponenten wie Infrastruktur, Daten, Modelle und Code. Verfolgen Sie Änderungen bis zu einem bestimmten Veröffentlichungszeitpunkt zurück. Dieser Ansatz ermöglicht die Steuerung von Modellen und die Einhaltung von Prüfstandards.
- **Ressourcen optimieren** – Führen Sie eine Abwägungsanalyse der verfügbaren Ressourcen und Konfigurationen durch, um ein optimales Ergebnis zu erzielen.
- **Kosten senken** – Identifizieren Sie die Potenziale zur Kostensenkung durch Automatisierung oder Optimierung, indem Sie Prozesse, Ressourcen und Abläufe analysieren .

Gestaltungsprinzipien 3/3

- **Automatisierung ermöglichen** – Nutzen Sie Technologien wie Pipelining, Scripting und Continuous Integration (CI), Continuous Delivery (CD) und Continuous Training (CT), um die Agilität zu steigern, die Leistung zu verbessern, die Ausfallsicherheit zu gewährleisten und die Kosten zu senken.
- **Ermöglichen Sie kontinuierliche Verbesserung** – Entwickeln und verbessern Sie die Arbeitsbelastung durch kontinuierliches Monitoring, Analyse und Lernen.
- **Minimieren Sie die Umweltbelastung** – Legen Sie Nachhaltigkeitsziele fest und verstehen Sie die Auswirkungen von ML-Modellen. Nutzen Sie Managed Services und setzen Sie effiziente Hard- und Software ein, um deren Nutzung zu maximieren.

Rollen: Fachexperten

Rolle im ML-LiveCycle

- ▶ Geben Sie geschäftliche Fragestellungen, Ziele oder KPIs an, die mit ML-Modellen in Verbindung stehen und wie diese formuliert werden sollten.
- ▶ Die Leistung des Modells muss kontinuierlich überprüft und sichergestellt werden, dass sie dem ursprünglichen Bedarf entspricht oder diesen erfüllt.

MLOps- Anforderungen

- ▶ Eine einfache Möglichkeit, die Leistung des eingesetzten Modells in geschäftlichen Begriffen zu verstehen.
- ▶ Mechanismus oder Feedbackschleife zur Kennzeichnung von Modellergebnissen, die nicht den Geschäftserwartungen entsprechen.

Rollen: Datenwissenschaftler

Rolle im ML-LiveCycle

- ▶ Entwickeln Sie Modelle, die auf die von Fachexperten eingebrachten geschäftlichen Fragestellungen oder Bedürfnisse eingehen.
- ▶ Bereitstellung funktionsfähiger Modelle, damit diese in der Produktionsumgebung und mit Produktionsdaten ordnungsgemäß eingesetzt werden können.
- ▶ Beurteilen Sie die Modellqualität (sowohl des Originalmodells als auch des Testmodells) gemeinsam mit Fachexperten, um sicherzustellen, dass sie die ersten geschäftlichen Fragen oder Bedürfnisse beantworten.

MLOps- Anforderungen

- ▶ Automatisierte Modellverpackung und -lieferung für eine schnelle und einfache Implementierung in der Produktion.
- ▶ Fähigkeit zur Entwicklung von Tests zur Bestimmung der Qualität eingesetzter Modelle und zur kontinuierlichen Verbesserung.
- ▶ Einblick in die Leistung aller eingesetzten Modelle von einem zentralen Standort aus.
- ▶ Die Fähigkeit, die Datenpipelines jedes Modells zu untersuchen, um schnell Einschätzungen und Anpassungen vorzunehmen, unabhängig davon, wer das Modell ursprünglich erstellt hat.

Rollen: Dateningenieure

Rolle im ML-LiveCycle

- ▶ Optimierung des Abrufs und der Nutzung von Daten zur Unterstützung von ML-Modellen.

MLOps- Anforderungen

- ▶ Einblick in die Leistung aller eingesetzten Modelle.
- ▶ Möglichkeit, die vollständigen Details einzelner Datenpipelines einzusehen

Rollen: Software-Ingenieure

Rolle im ML-LiveCycle

- ▶ ML-Modelle in die Anwendungen und Systeme des Unternehmens integrieren
- ▶ Stellen Sie sicher, dass ML-Modelle nahtlos mit anderen, nicht auf maschinellem Lernen basierenden Anwendungen zusammenarbeiten.

MLOps- Anforderungen

- ▶ Versionierung und automatische Tests.
- ▶ Die Fähigkeit, parallel an derselben Anwendung zu arbeiten.

Rollen: DevOps

Rolle im ML-LiveCycle

- ▶ Operative Systeme entwickeln und aufbauen sowie auf Sicherheit, Leistung und Verfügbarkeit testen.
- ▶ Management der Continuous Integration/Continuous Delivery (CI/CD)-Pipeline.

MLOps- Anforderungen

- ▶ Nahtlose Integration von MLOps in die übergeordnete DevOps-Strategie des Unternehmens.
- ▶ Nahtlose Bereitstellungs-pipeline.

Rollen: Modellrisikomanager / Auditoren

Rolle im ML-LiveCycle

- ▶ Minimierung des Gesamtrisikos für das Unternehmen durch den Einsatz von ML-Modellen in der Produktion.
- ▶ Stellen Sie sicher, dass alle internen und externen Anforderungen erfüllt sind, bevor Sie ML-Modelle in die Produktion überführen.

MLOps- Anforderungen

- ▶ Robuste, wahrscheinlich automatisierte Reporting-Tools für alle Modelle (derzeit oder jemals in Produktion), einschließlich Datenherkunft.

Rollen: Architekten für maschinelles Lernen

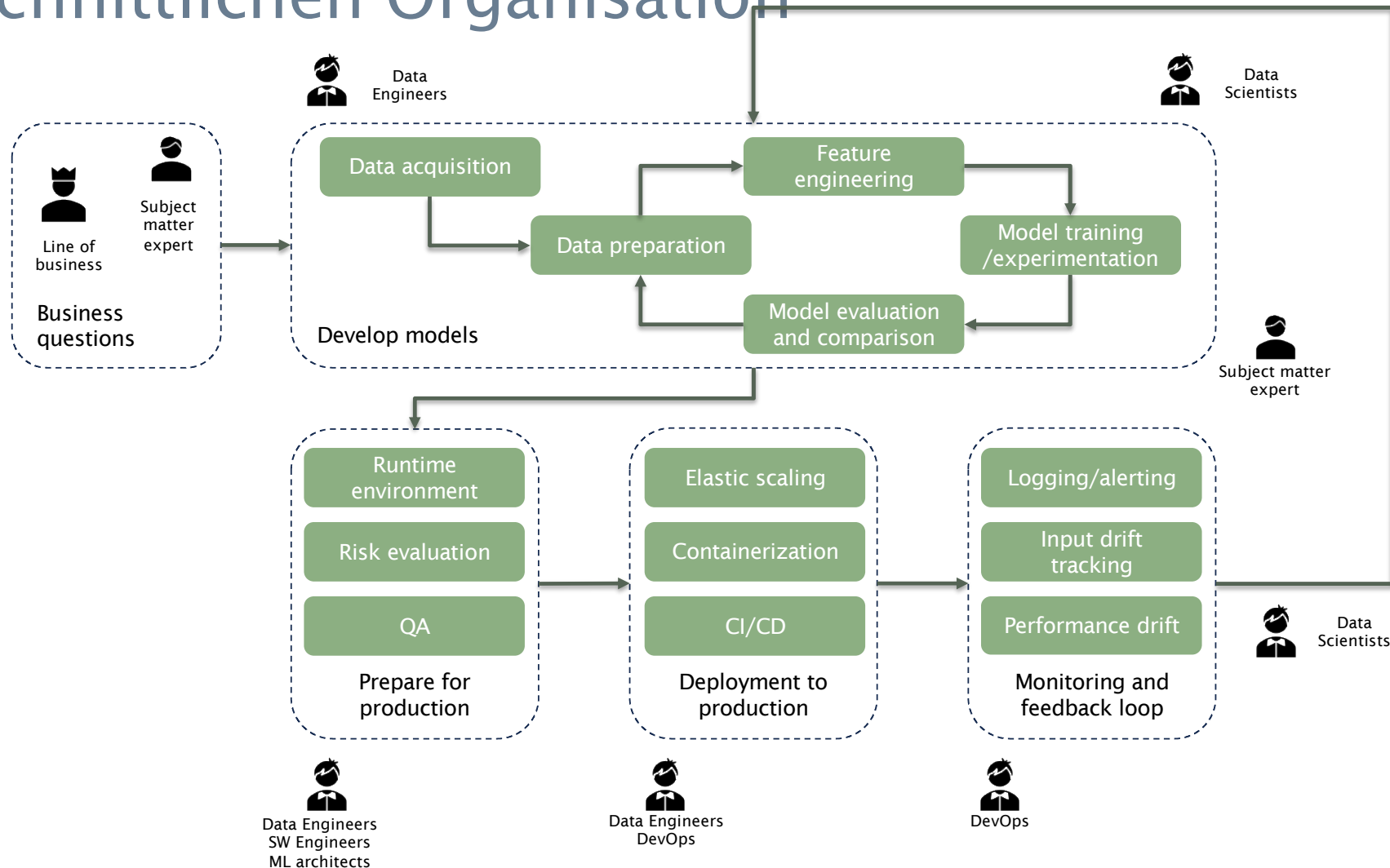
Rolle im ML-LiveCycle

- ▶ Gewährleisten Sie eine skalierbare und flexible Umgebung für ML-Modellpipelines, vom Design über die Entwicklung bis hin zur Überwachung.
- ▶ Führen Sie gegebenenfalls neue Technologien ein, die die Leistung von ML-Modellen in der Produktion verbessern.

MLOps- Anforderungen

- ▶ Überblick über die Modelle und ihren Ressourcenverbrauch.
- ▶ Die Fähigkeit, Datenpipelines bis ins Detail zu analysieren, um den Infrastrukturbedarf zu ermitteln und anzupassen.

Das realistische Bild eines ML-Lebenszyklus innerhalb einer durchschnittlichen Organisation



Literatur

1. <https://yalebooks.yale.edu/book/9780300158564/the-illusions-of-entrepreneurship/>