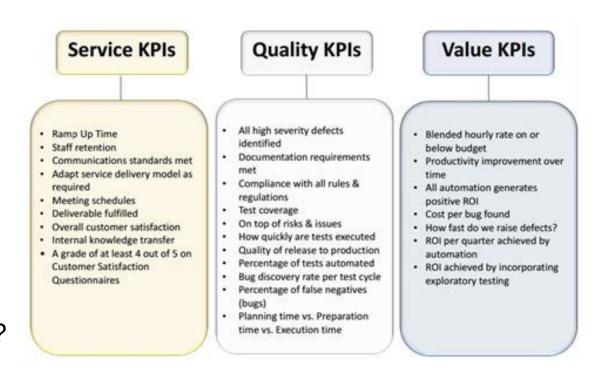




Understanding the Business

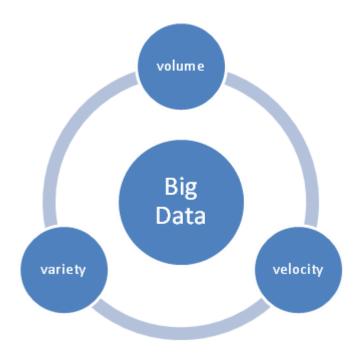
- What does the business need?
 - What are the problems that need to be solved?
 - Is there enough information to state the problem?
 - What are the specific outcomes that are needed?
- Service Level Agreements
 - What are the quality levels needed?
 - How do we measure outcomes?
 - What is the necessary business outcome?
 - How will it be measured?
- Key Performance Indicators
 - What needs to be measured and why?
 - How do the KPIs relate to SLAs?



Data Sources and Exploratory Data Analysis

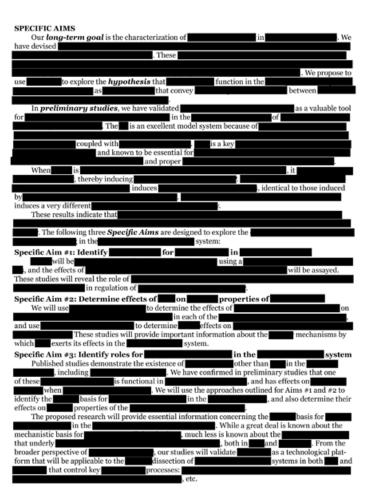
Key questions to be answered:

- What relevant datasets are available?
- Is this data sufficiently accurate and reliable?
- How can stakeholders get access to this data?
- What data properties (known as features) can be made available by combining multiple sources of data?
- Will this data be available in real time?
- Is there a need to label some of the data with the "ground truth" that is to be predicted, or does unsupervised learning make sense? If so, how much will this cost in terms of time and resources?
- What platform should be used?
- How will data be updated once the model is deployed?
- Will the use of the model itself reduce the representativeness of the data?
- How will the KPIs, which were established along with the business objectives, be measured?



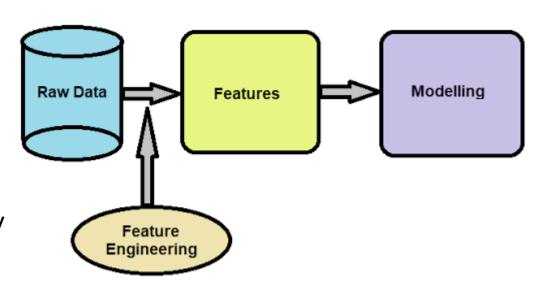
Data Constraints

- Key questions to be answered:
 - Can the selected datasets be used for this purpose?
 - What are the terms of use?
 - Is there personally identifiable information (PII) that must be redacted or anonymized?
 - Are there features, such as gender, that legally cannot be used in this business context?
 - Are minority populations sufficiently well represented that the model has equivalent performances on each group?



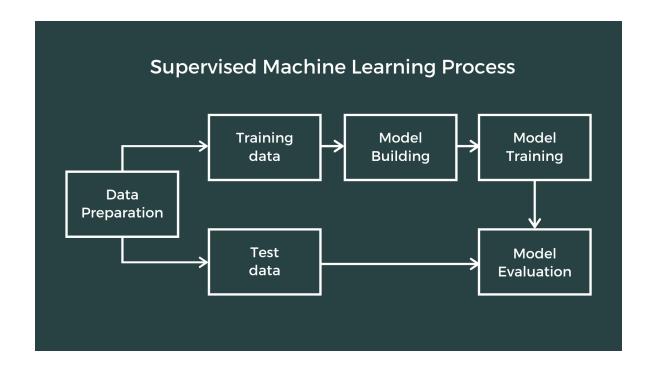
Feature Engineering and Selection

- Critical part of model development
- Poor feature selection impacts MLOps in a variety of ways
 - The model can become more and more expensive to compute.
 - More features require more inputs and more maintenance down the line.
 - More features mean a loss of some stability.
 - The sheer number of features can raise privacy concerns.



Training and Evaluation

- Standard methodology in ML
- For MLOps
 - Is the training data realistic?
- We train a model on fixed data
 - Tune results by algorithm choice
 - Tune results by feature selection
 - Tune results with hyperparameters
- Overfitting is real concern
- Setting evaluation criteria is important
 - Moderate success on wide ranges of training data versus high success on narrow sets of training data



Reproducibility

- Supported by good CI practices
- What was created in dev can be reproduced in prod
- Ability to roll back to previous versions
- Requires version control of ALL assets used in developing the model



Responsible Al

- Results need to be explainable
- Mitigate uncertainty and help prevent unintended consequences
- Uses:
 - Partial dependence plots, which look at the marginal impact of features on the predicted outcome
 - Subpopulation analyses, which look at how the model treats specific subpopulations and that are the basis of many fairness analyses
 - Individual model predictions, such as Shapley values, which explain how the value of each feature contributes to a specific prediction
 - What-if analysis, which helps the ML model user to understand the sensitivity of the prediction to its inputs



Maturity Levels

- Various attempts to quantify the organization's level of expertise in using MLOps
 - https://www.eqengineered.co m/insights/mlops-maturitylevels
 - https://docs.microsoft.com/en us/azure/architecture/exampl e-scenario/mlops/mlopsmaturity-model

Level 1: ML Pipeline Automation

- Rapid experimentation · Automatic data and model
- validation Close integration of ML
- and operations
- · Continuous delivery of models and pipeline · Management of features
- and metadata · Manual triggering and
- retraining
- · Limited traceability and reproducibility

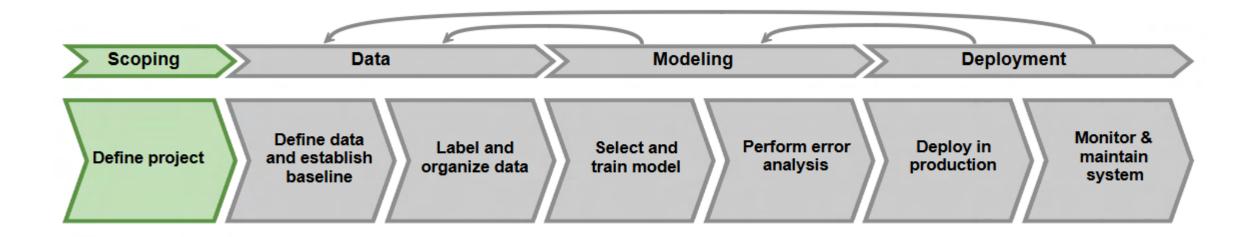
Level 2: Deployment **Pipeline** Automation

- Integration and versioning of code, model registry, feature store, & metadata
- Continuous integration and Continuous delivery of pipeline and model
- Integrated A/B testing of model performance
- · Automatic triggering & retraining
- · Model performance monitoring
- Full traceability and reproducibility

Level 0: Manual

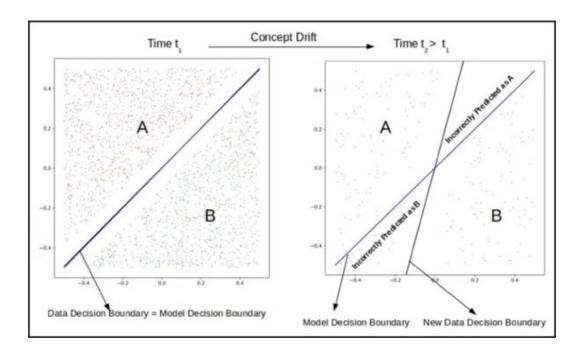
- Manual or script-driven process
- Deployment related only to the prediction service
- Disconnection between ML and operations
- · Infrequent release iterations
- Manual triggering and retraining
- · No versioning or management of modeling
- · No monitoring of model behavior

Model Lifecycle



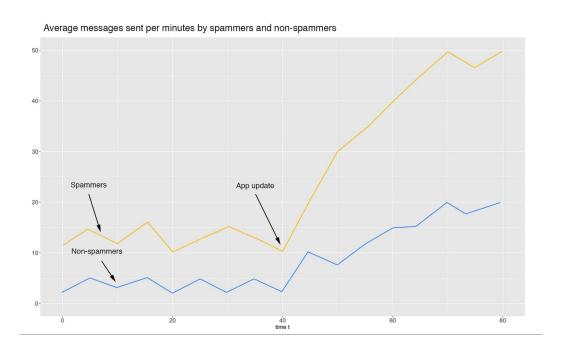
Concept Drift

- ML models are trained assuming a certain conceptual relationship between inputs and predictions
 - When that relationship changes in the real world, we have concept drift
 - The model no longer describes the actual relationships
 - For example, floor area is no longer a factor in home prices.
 - Indicates a change in the decision boundary
- Concept drift can be managed only by retraining the model



Data Drift

- Key ML assumption
 - Future is predictable from the past
- Data drift is when
 - The distribution of the input data has changed
- Temporal shifts
 - The population changes over time changing demographics for example
 - Features in the model no longer correspond to features in the data
- Spatial shifts
 - The model is deployed in a different population than it was trained for
 - US models deployed in China



Scaffolding Walkthrough ERIT 5(n-4) . s(n-j 5(n) = Wn. s(n-1) + Wz.



