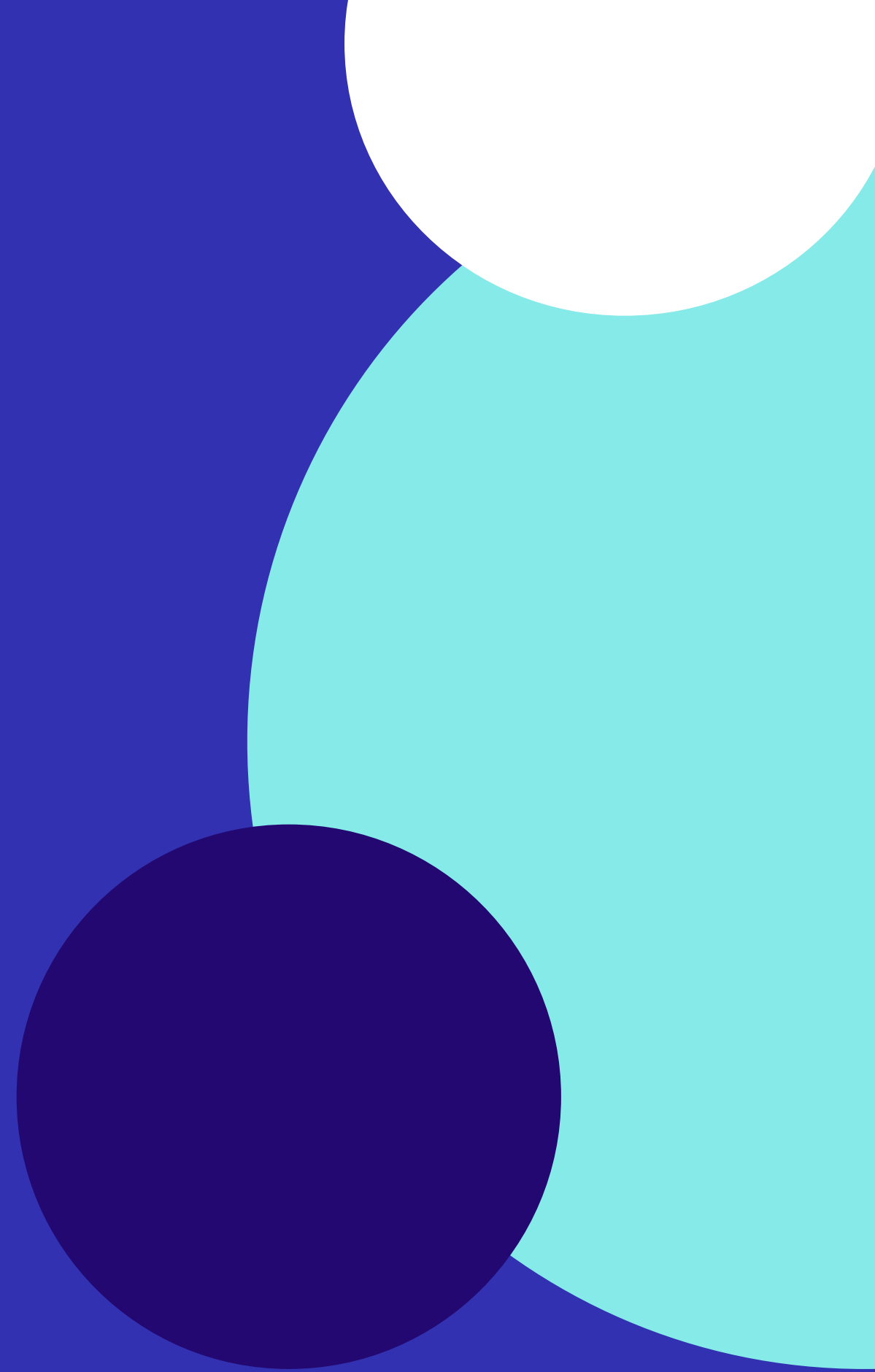


Introduction to MLOps

Bridging the Gap Between Machine Learning and
Operations

Lecturer: Vangelis Oden - Technology Lead (Kera)

Assistant: Natalija Mitic - AI/ML Engineer (Kera)



Course Agenda

- Lectures - Mornings/Afternoons
- Labs - Afternoons
- Breaks - 2 during lectures/labs
- Projects - 2, Last week of the Month, Teams
- Quizzes - 2, Last day each week
- Practice - Anywhere
- Questions - Anywhere, anytime (channels, physical)
- Campuswire - Essential

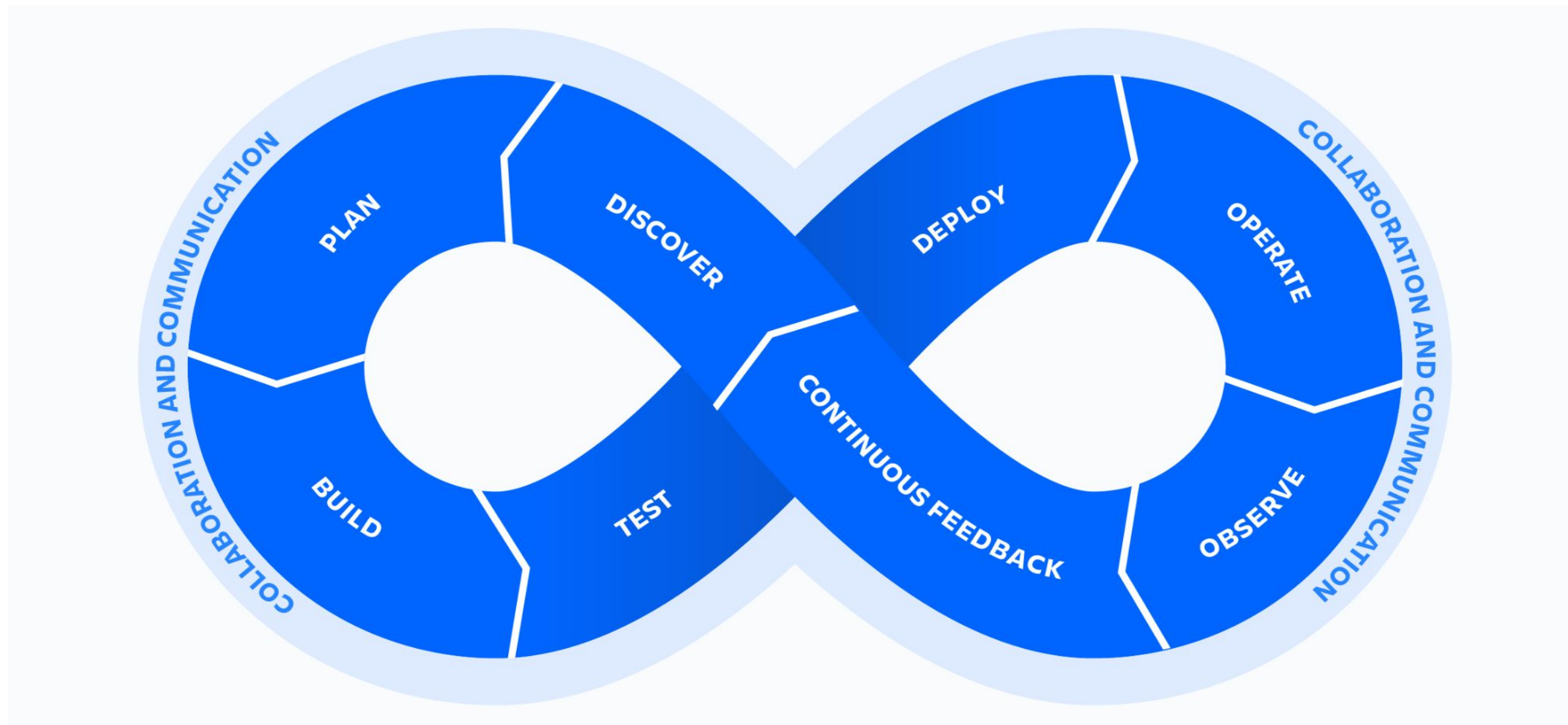
FAQs

- Who is this course for?
- Prerequisites?
- Why is this course important now?
- Others...

Agenda

- What is MLOps?
- Why MLOps Matters
- Key Concepts in MLOps
- MLOps Workflow
- Tools and Technologies
- Challenges and Best Practices
- Case Studies
- Q&A

What is MLOps - What is DevOps?



What is MLOps - What is DevOps?

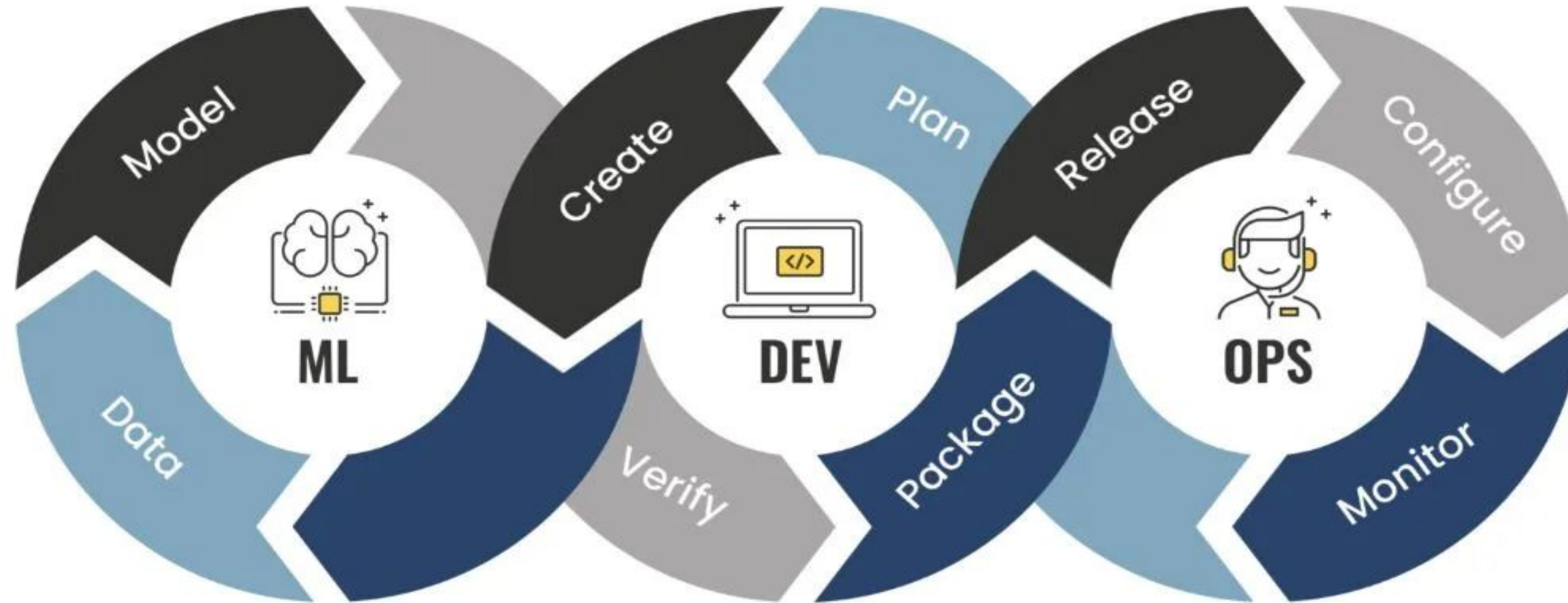
Definition:

The DevOps lifecycle is a continuous software development process that employs DevOps best practices to plan, build, integrate, deploy, monitor, operate, and offer continuous feedback throughout the software lifecycle.

DevOps - Benefits?

- Collaboration and Trust
- Release Faster and Work Smarter
- Accelerate time-to-resolution
- Better manage unplanned work

What is MLOps?



What is MLOps?

Definition:

- MLOps stands for “Machine Learning Operations.”
- It’s a set of practices that combine Machine Learning, DevOps, and Data Engineering to deploy and maintain ML systems in production reliably and efficiently.

Analogy:

- Think of MLOps as DevOps but for machine learning.

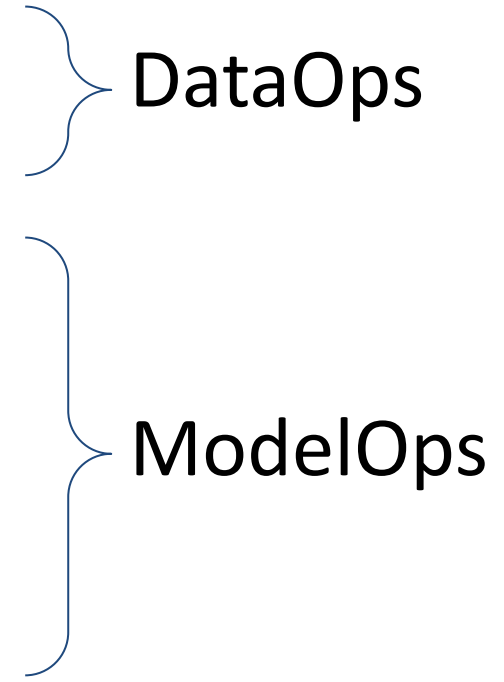
Why it matters?

- **Scalability:** Allows scaling ML models to production efficiently.
- **Reproducibility:** Ensures that models are reproducible and maintainable.
- **Automation:** Automates repetitive tasks in the ML lifecycle.
- **Collaboration:** Facilitates collaboration between data scientists, engineers, and operations teams.

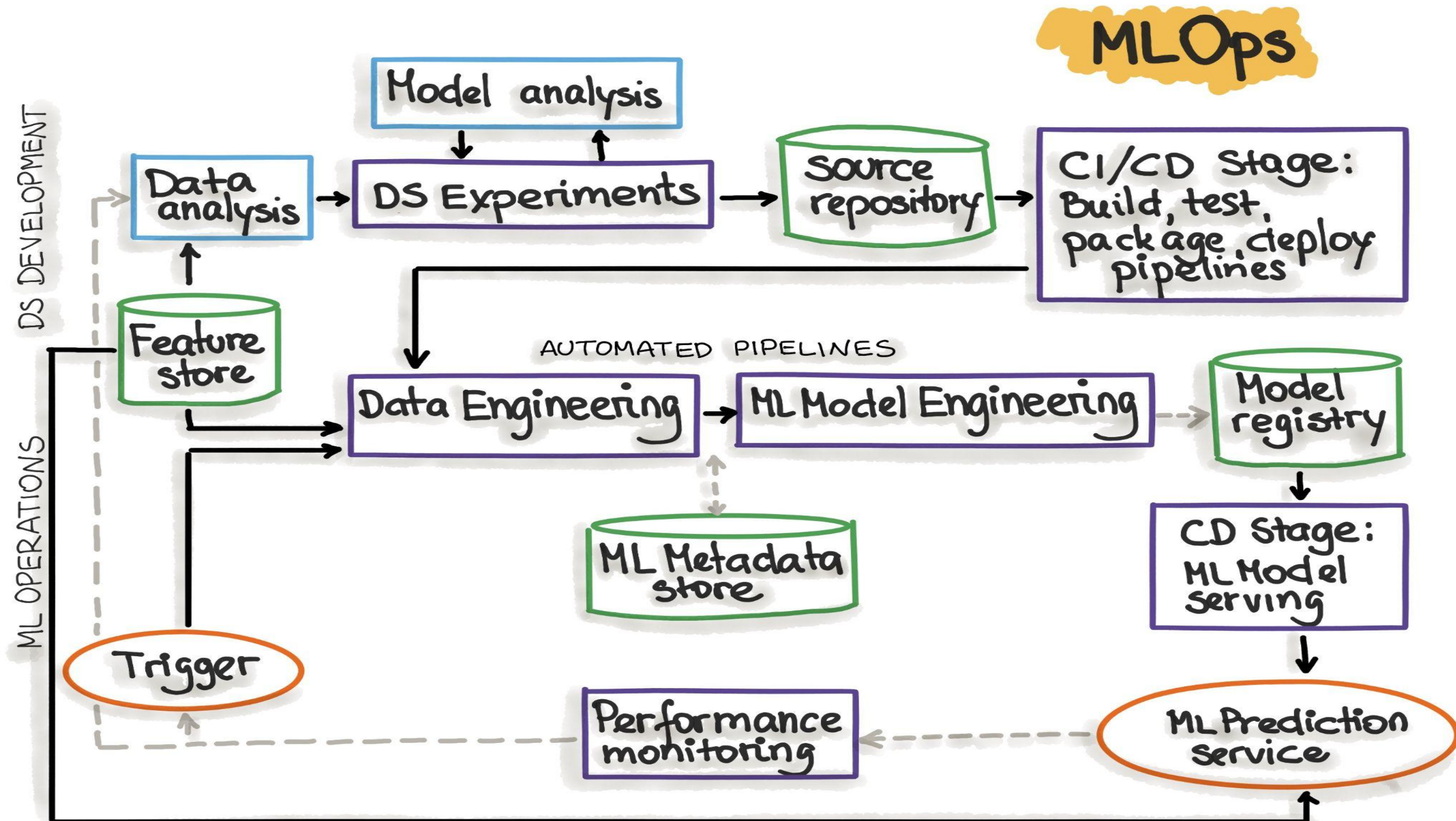
Key Concepts in MLOps

- Version Control for Models and Data
- Continuous Integration/Continuous Deployment (CI/CT/CD)
- Model Monitoring and Management
- Automated Testing and Validation
- Infrastructure as Code (IaC)

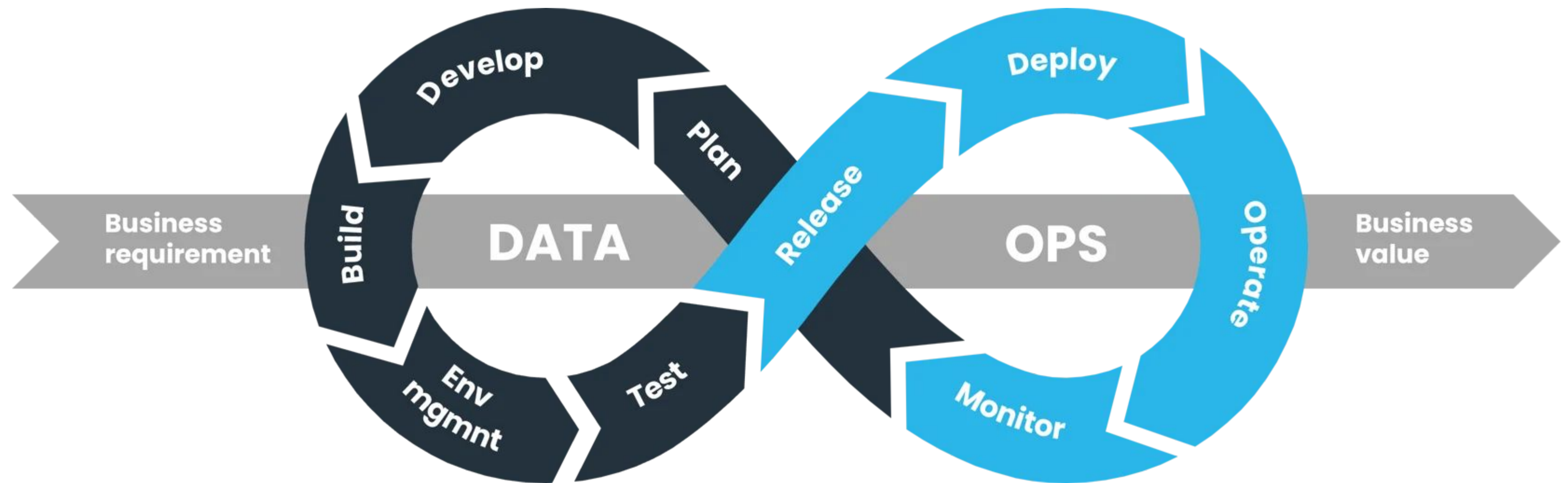
MLOps Workflow

- **Step 1:** Data Collection and Preprocessing
 - **Step 2:** Data Versioning
 - **Step 3:** Model Development
 - **Step 4:** Model Training and Validation
 - **Step 5:** Model Versioning
 - **Step 6:** Model Deployment
 - **Step 7:** Continuous Monitoring and Maintenance
 - **Step 8:** Feedback Loop and Model Improvement
- 
- The diagram illustrates the MLOps workflow steps grouped into two categories:
- DataOps:** Includes Step 1 (Data Collection and Preprocessing) and Step 2 (Data Versioning).
 - ModelOps:** Includes Step 3 (Model Development), Step 4 (Model Training and Validation), Step 5 (Model Versioning), and Step 6 (Model Deployment).
- Steps 7 and 8 (Continuous Monitoring and Maintenance, and Feedback Loop and Model Improvement) are not grouped into either category.

MLOps Workflow



DataOps

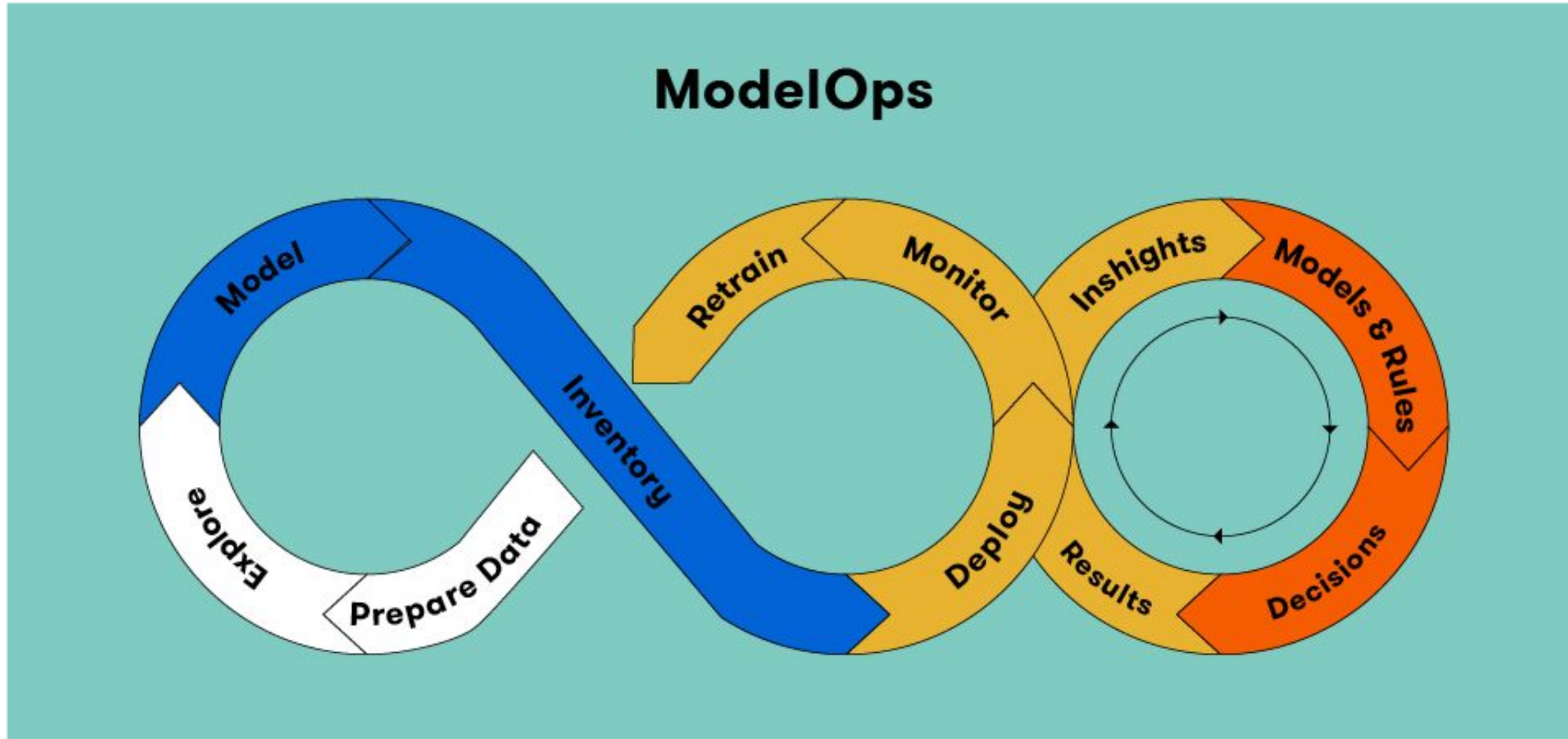


DataOps

Definition:

- DataOps (short for data operations) is a data management practice that makes building, testing, deploying, and managing ***data products*** and ***data apps*** the same as it is for software products.
- It combines technologies and processes to improve trust in data and reduce your company's data products' time to value.

ModelOps



ModelOps

Definition:

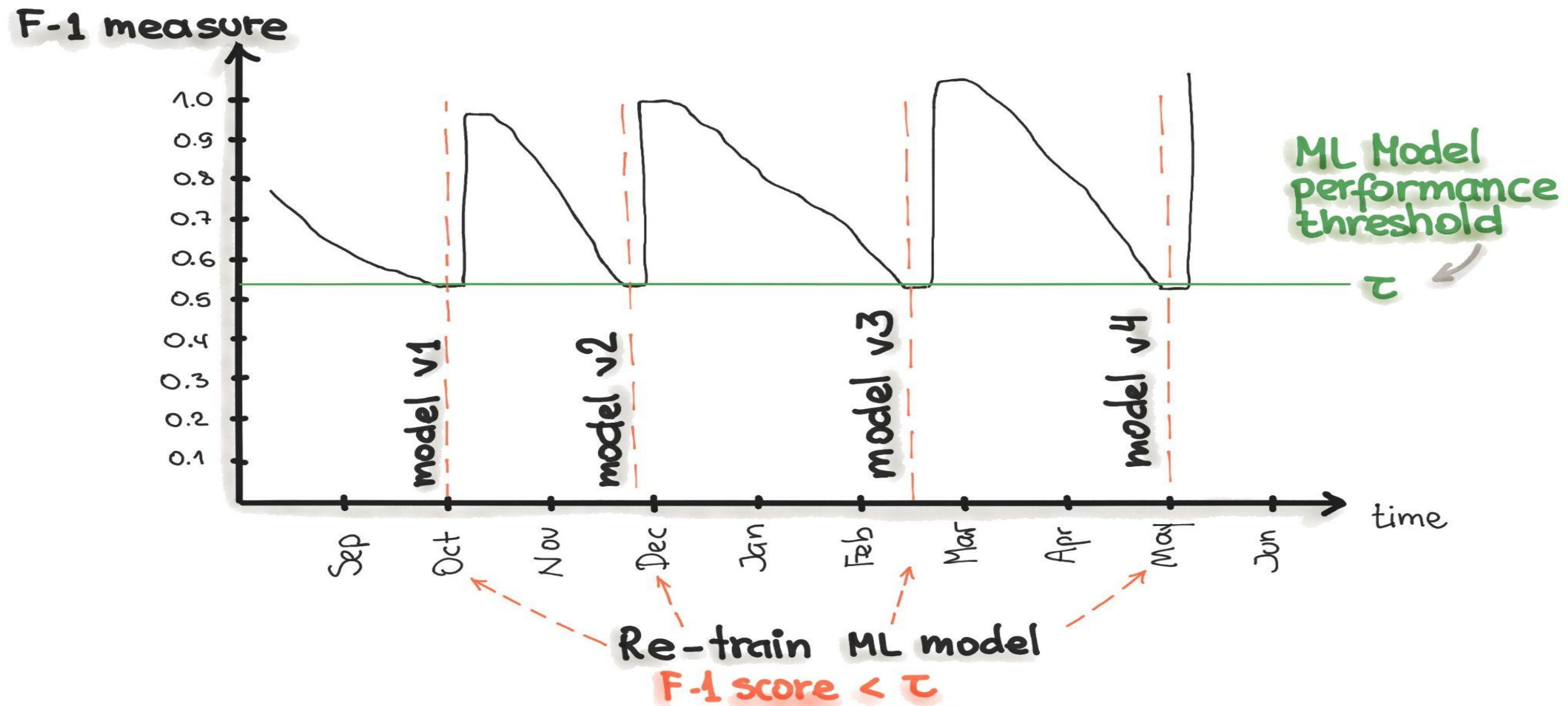
- ModelOps (or **AI model operationalization**) is focused primarily on the governance and life cycle management of a wide range of operationalized artificial intelligence (AI) and decision models.
- Decision models including machine learning, knowledge graphs, rules, optimization, linguistic and agent-based models.

Tools and Technologies

- **Version Control:** Git, DVC
- **CI/CD Pipelines:** Jenkins, GitLab CI, CircleCI, GH Actions, Cloud Build, etc.
- **ETL Pipelines:** AirFlow
- **Model Serving:** TensorFlow Serving, TorchServe, FastAPI, Kubernetes
- **Monitoring:** Prometheus, Grafana, Seldon, Custom Monitoring - ELK Stack
- **Experiment Tracking:** MLflow, Weights & Biases, KubeFlow
- **Infrastructure:** Docker, Kubernetes, Terraform
- **Cloud Platforms:** Azure, GCP, AWS
- **Scaling:** GPUs, TPUs
- **Security and Compliance:** API Keys, Encryption, GDPR and HIPAA

Challenges in MLOps

ML MODEL DECAY MONITORING



Challenges in MLOps

- **Data Drift:** Models becoming less accurate as data changes over time.
- **Complexity:** Managing and orchestrating complex pipelines.
- **Scalability:** Handling large-scale data, model training and model delivery.
- **Collaboration:** Bridging gaps between data science and engineering teams.

Best Practices

- **Automate Everything:** From data pipelines to deployment.
- **Keep Everything Versioned:** Data, code, and models.
- **Monitor Continuously:** Use monitoring tools to track performance and detect issues early.
- **Test Thoroughly:** Implement testing for data quality, model accuracy, and deployment pipelines.
- **Collaborate Across Teams:** Encourage communication between data scientists, engineers, and operations.

Case Studies

Company	Industry	Results
AgroScout	Agriculture	<ul style="list-style-type: none">-Increased data volume 100x without growing the data team-Increased experiment volume 50x-Decreased the time to production by 50%
Booking.com	e-Commerce	<ul style="list-style-type: none">-Ability to scale AI with 150 customer facing ML models
Payoneer	Fin-Services	<ul style="list-style-type: none">-Built a scalable and reliable fraud prediction and prevention model that analyzes fresh data in real-time and adapts to new threats
Oyak Cement	Manufacturing	<ul style="list-style-type: none">-Increased alternative fuel usage by 7 times-Cut 2% of total CO2 emissions-Reduced costs by \$39 million

Conclusion

- Summary: MLOps is essential for scaling and maintaining ML models in production as well as ensuring trust in the models built.
- Next Steps: Explore the tools and techniques introduced today.

Q&A



Thank You!

Additional Resources:

- Documentation - Cloud Setup