Software Development AI and DevOps

Hasan Yasar

Technical Director, Adjunct Faculty Member

Software Engineering Institute | Carnegie Mellon University

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0697

Outline

- Modern SW Development: DevOps
- AI for DevOps
- DevOps for AI

Modern SW Development: DevOps

DevOps is a set of principles and practices emphasizing collaboration and communication between software development teams and IT operations staff along with acquirers, suppliers, and other stakeholders in the lifecycle of a software system

DevSecOps is a model on integrating the software development and operational process considering security activities: requirements, design, coding, testing , delivery , deployment and incident response.

Mature DevOps practices are constantly testing, deploying and validating that software meets every requirement and allows for fast recovery in the event of a problem. As a result we can easily say,

“DevSecOps is DevOps done right”

Who are Dev?

- Follow Agile methodologies
  - Using Scrum, Kanban and modern development approaches
  - Self directing, self managed, self organized
- Using any new technology
  - Each Dev has own development strategy
  - OpenSource,
- Allowed to have
  - Close relationships with the business
  - Software driven economy

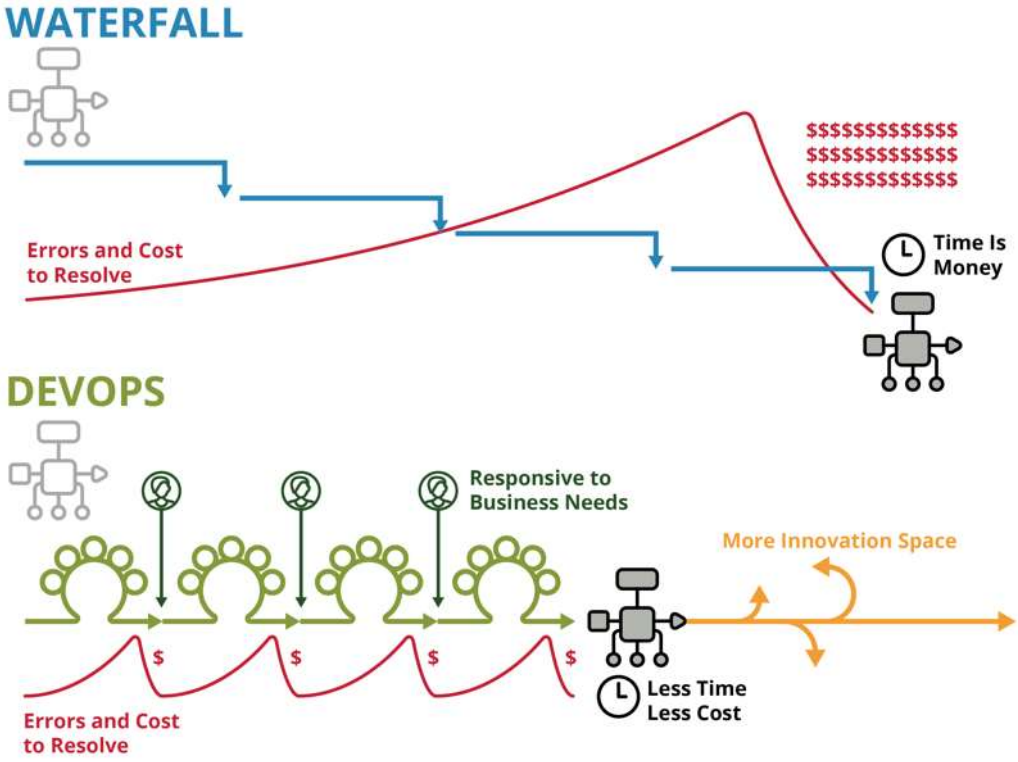
Want to deliver software faster with new requirements…

Who are Ops?

- Operations
  - Runs the application
  - Manages the infrastructure
  - Support the applications
- Operations provides
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operations
  - Secure systems

Want to maintain stability, reliability and security…

Key Benefits of DevOps



- Reduced errors during deployment
- Reduced time to deploy and resolve discovered errors
- **Repeatable** steps
- **Continuous availability** of pipeline and application
- Increased innovation time
- **Responsiveness** to business needs
- **Traceability** throughout the application lifecycle
- Increased stability and quality
- **Continuous feedback**

DevOps aims to Increase…

…the pace of **innovation**

…**responsiveness** to business needs

…**collaboration**

…software **stability and quality**

… continuous feedback

DevOps has four Fundamental Principles

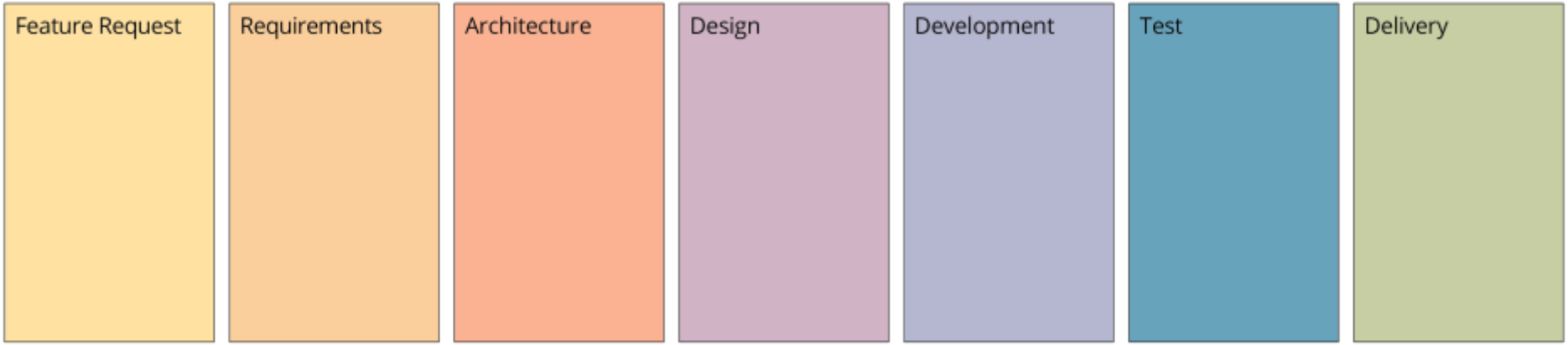
- **Collaboration:** between project team roles

- **Infrastructure as Code:** all assets are versioned, scripted, and shared where possible

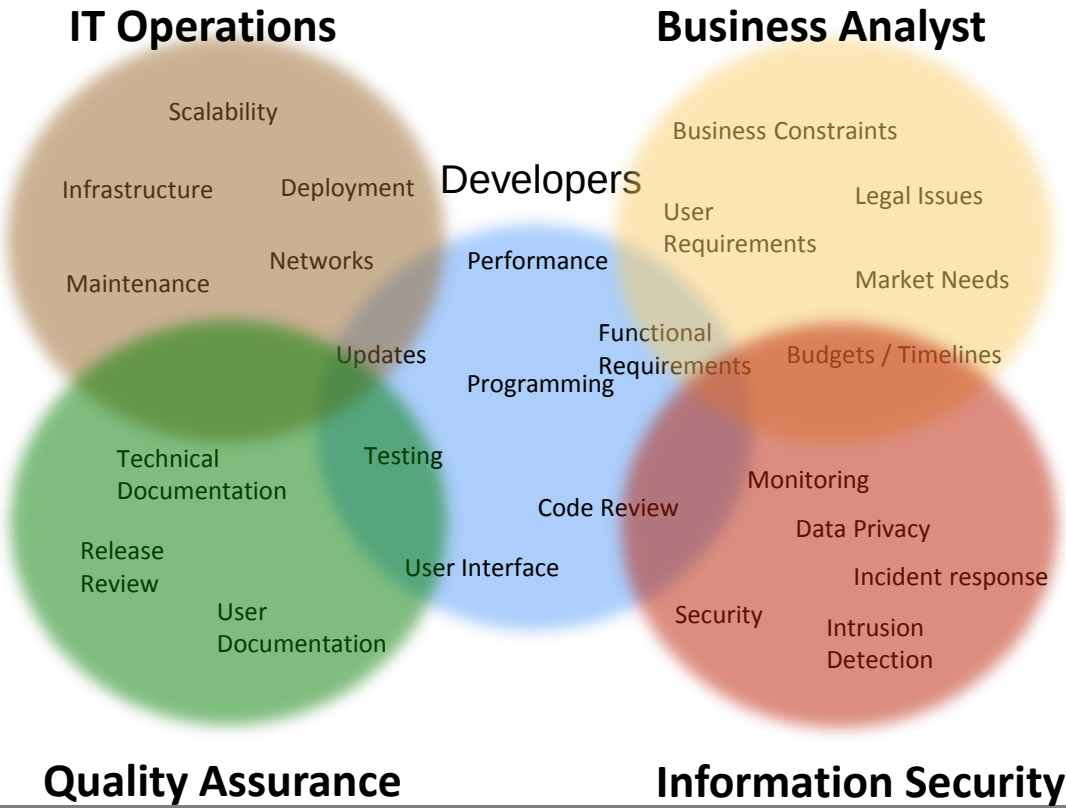
- **Automation:** deployment, testing, provisioning, any manual or human-error-prone process

- **Monitoring:** any metric in the development or operational spaces that can inform priorities, direction, and policy

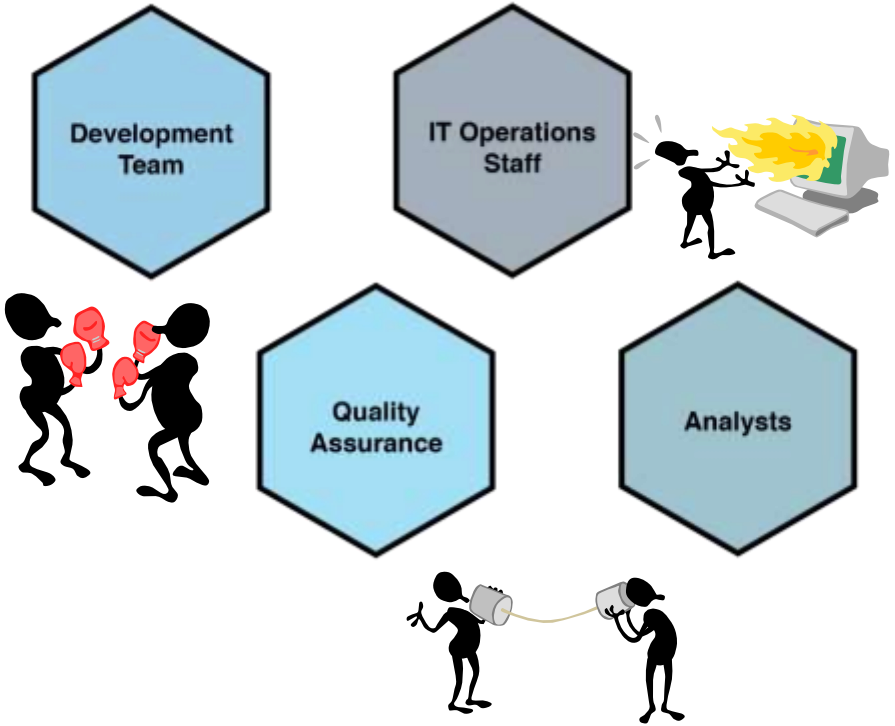
SW Development Phases



Collaboration: *Many stakeholders*

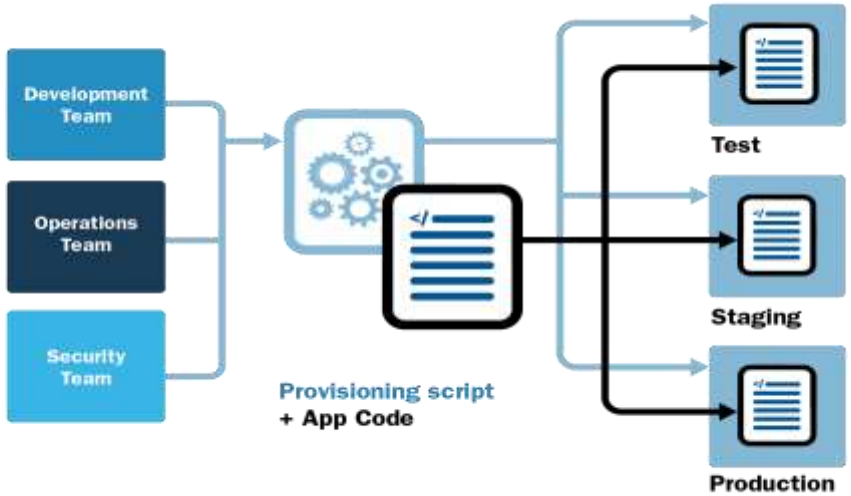


Collaboration: *Silos Inhibit Collaboration and poor communication*



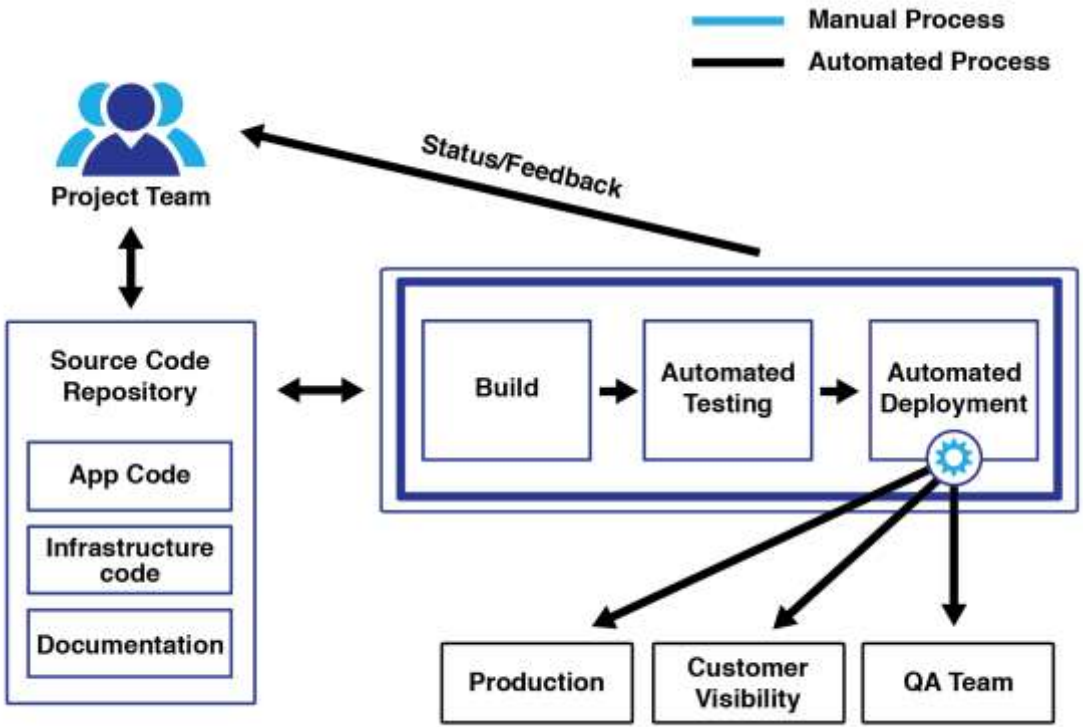
Infrastructure as Code (IaC)

A program that creates infrastructure,



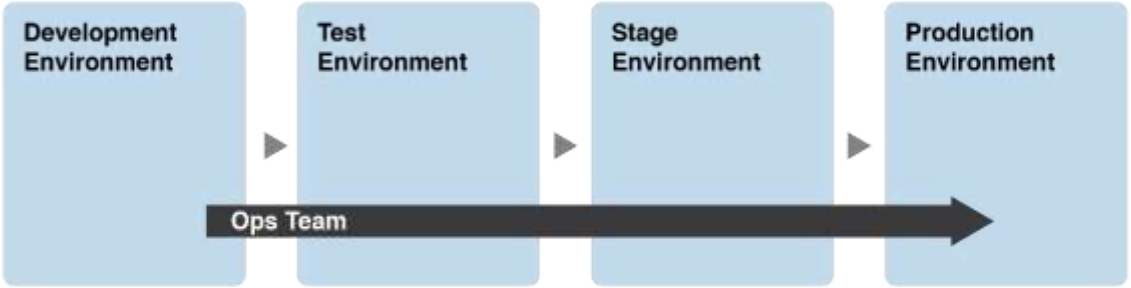
A concretely defined description of the environment is good material for conversation between team members.

Automation : *Continuous Integration (CI)*



Continuous integration is a process that continually merges a system's artifacts, including source code updates and configuration items from all stakeholders on a team, into a shared mainline to build and test the developed system.

Automation : *Continuous Delivery / Deployment (CD)*

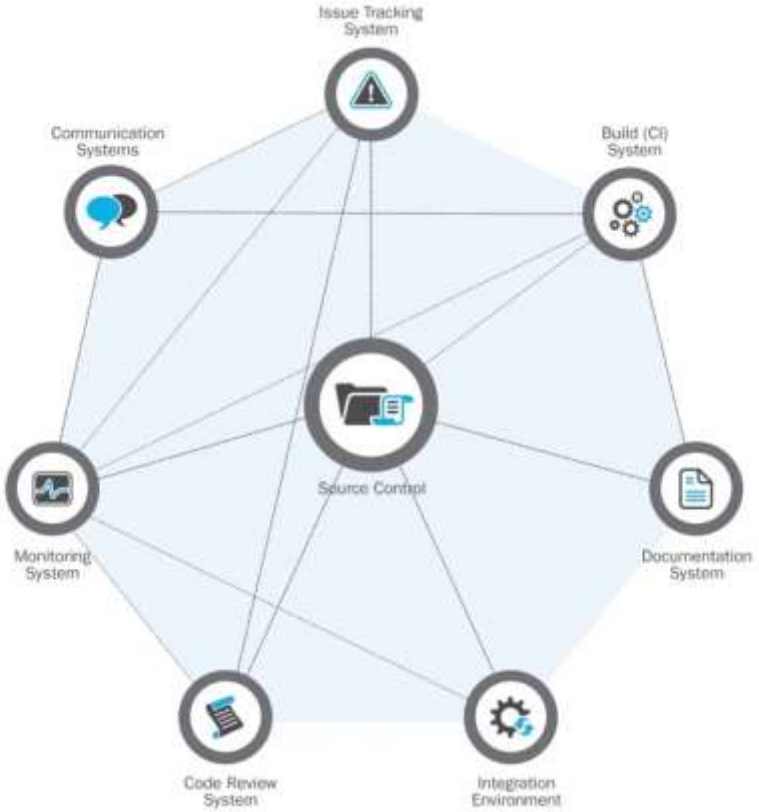


Shift Left Operational Concerns Enforced by Continuous Delivery with parity across various environment

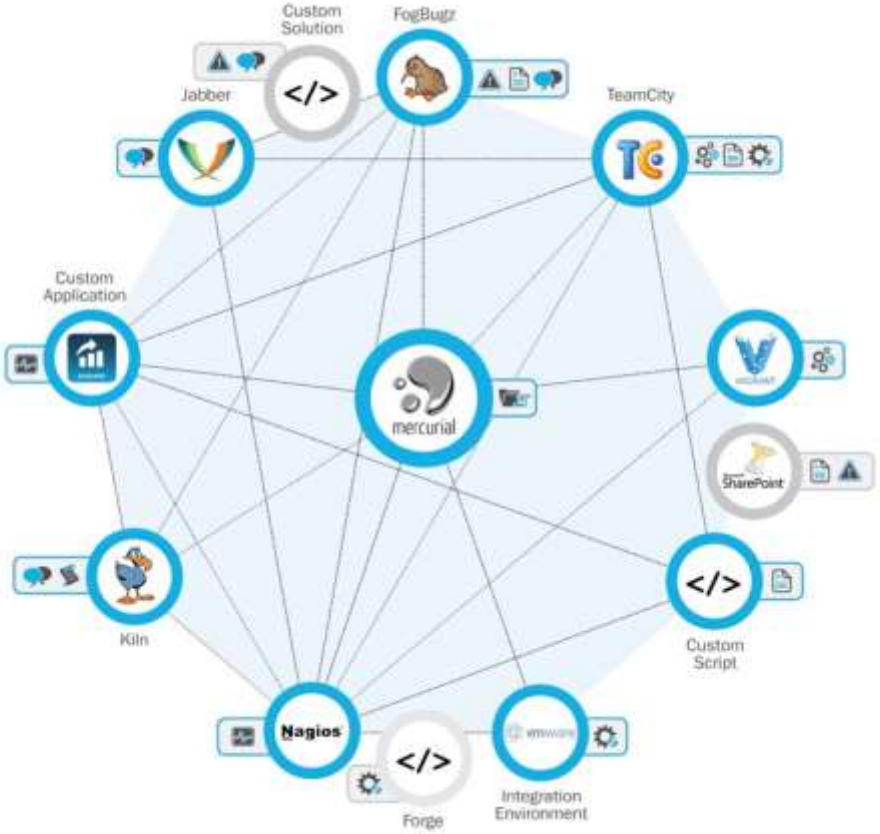
Continuous delivery is a software engineering practice that allows for frequent releases of new software to staging or various test environments through the use of automated testing.

Continuous deployment is the automated process of deploying changes to production by verifying intended features and validations to minimize risk.

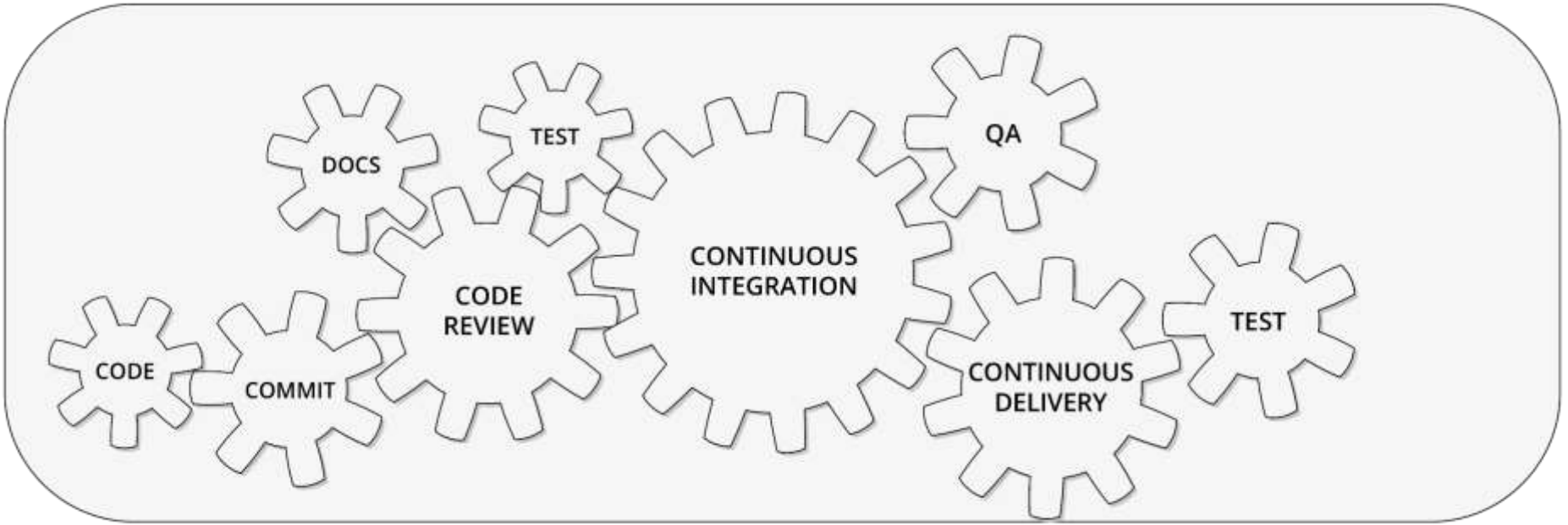
Integrated Development Pipeline - General



Integrated Development Pipeline – With Tooling

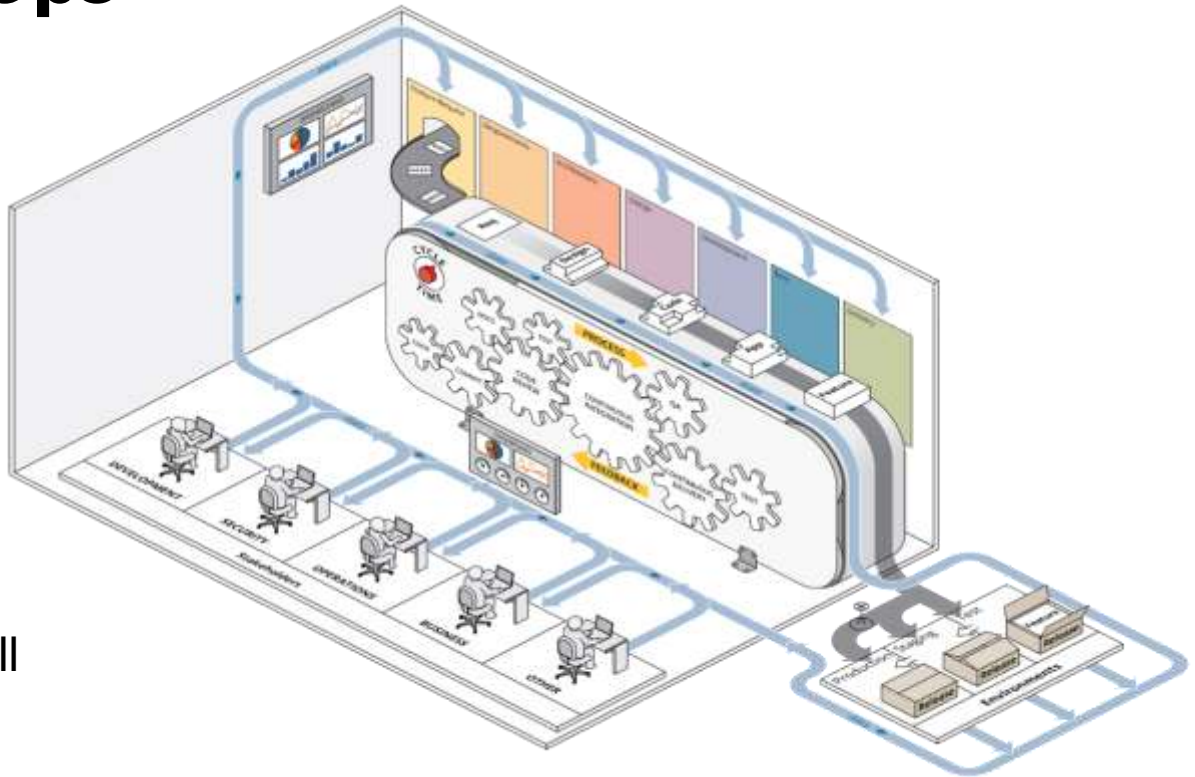


Automation with IaC, CI, CD

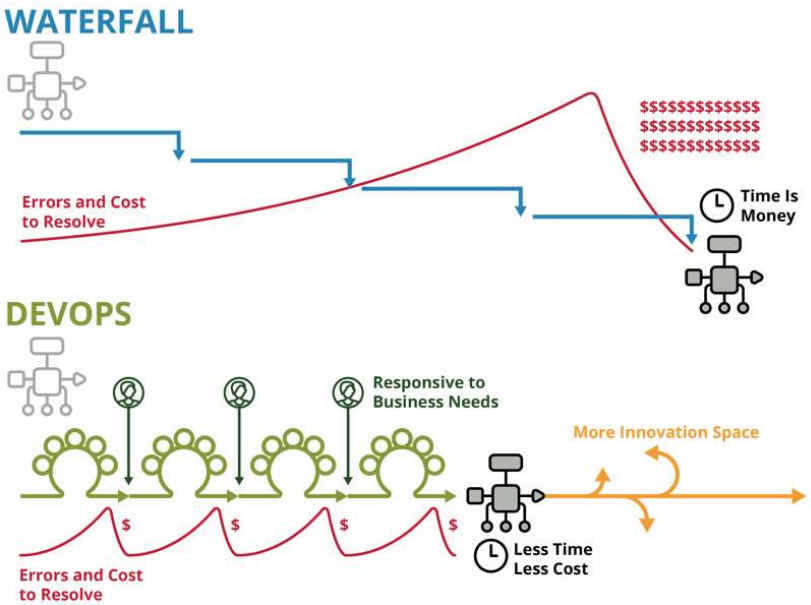


Principles of DevOps

- Feature to deployment
- Iterative and incremental development
- Automation in every phase of the SDLC
- Continuous feedback
- Metrics and measurement
- Complete engagement with all stakeholders
- Transparency and traceability across the lifecycle

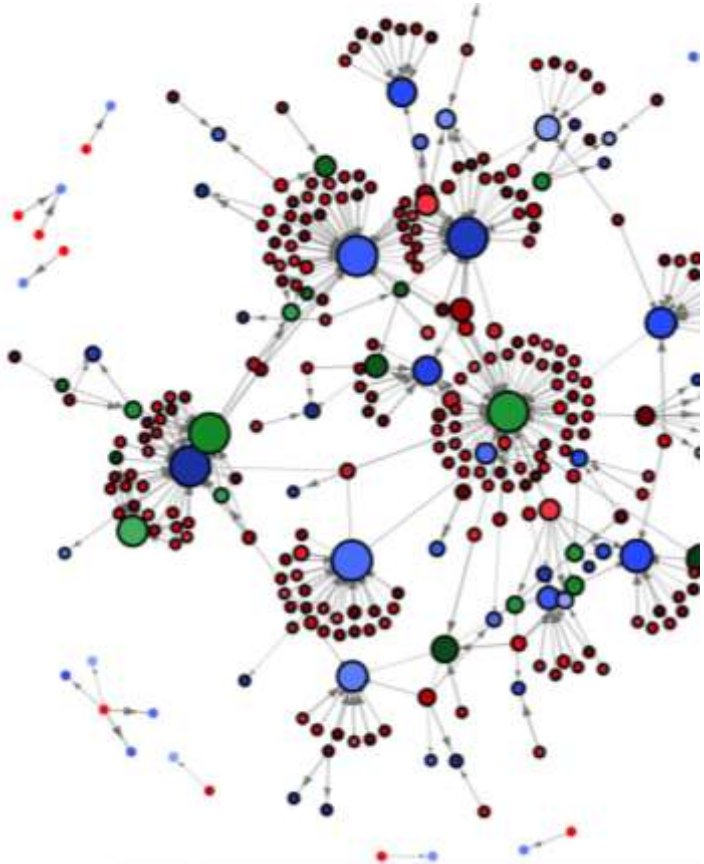


Key benefits of DevOps

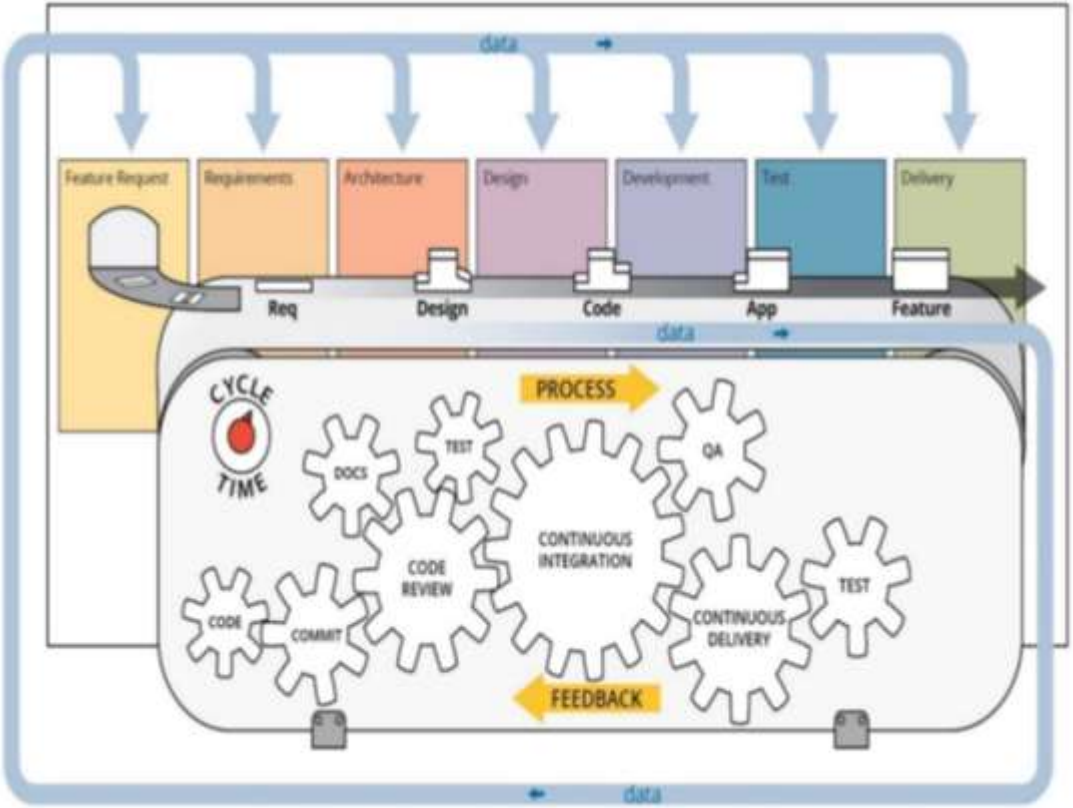


- Reduced errors during deployment
- Reduced time to deploy and resolve discovered errors
- **Repeatable** steps
- **Continuous availability** of pipeline and application
- Increased innovation time
- **Responsiveness** to business needs
- **Traceability** throughout the application lifecycle
- Increased stability and quality
- **Continuous feedback**

AI for DevOps



AI For DevOps

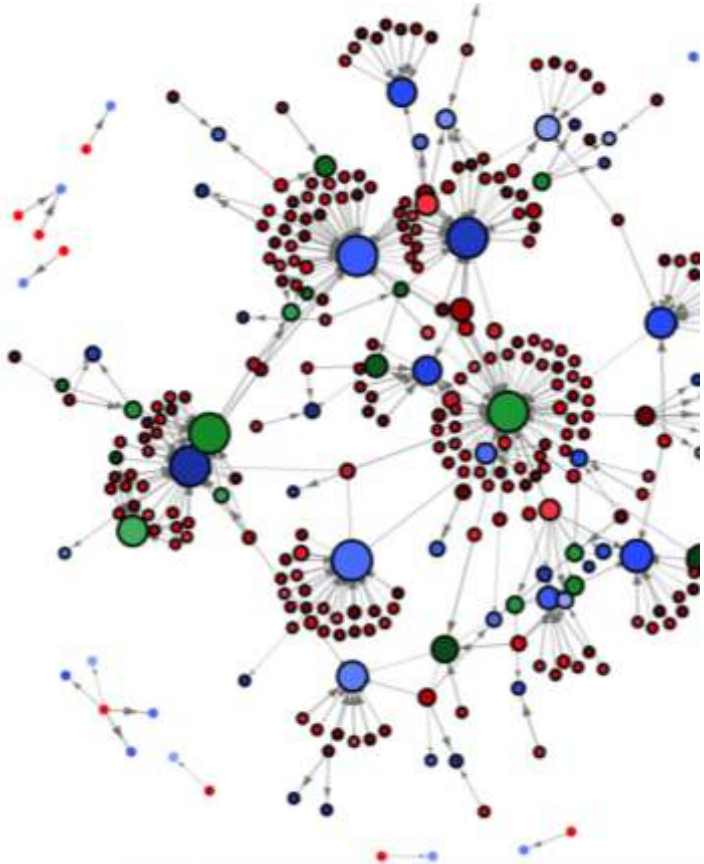


Using ML and AI to ‘inform’ a DevOps factory or pipeline of notable events, usually to help improve the process over time, or help make decisions based on real-time event.

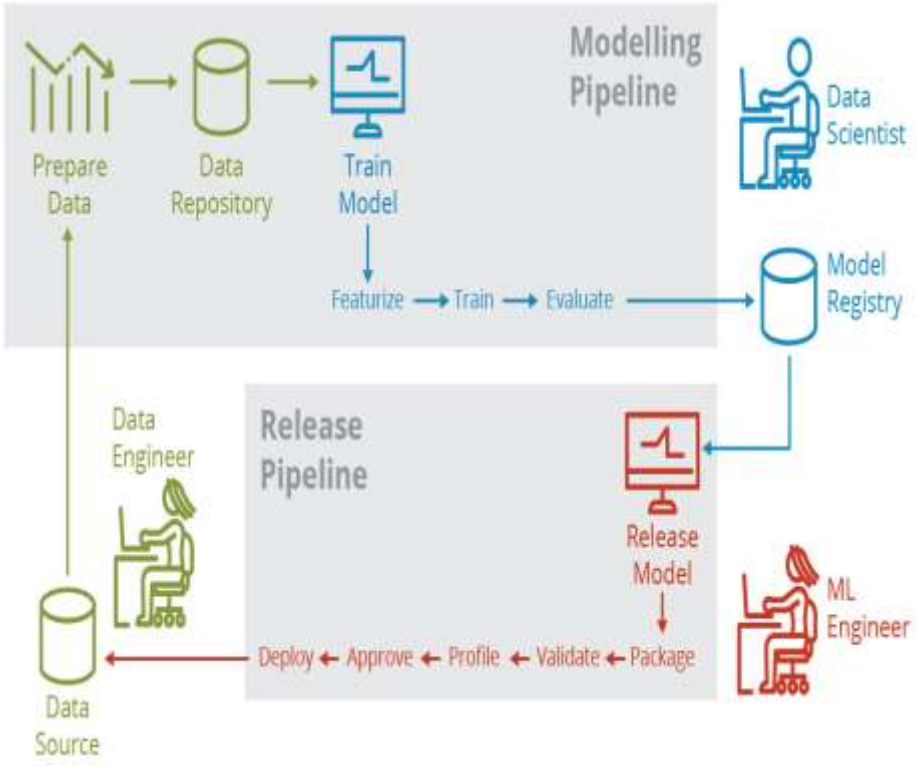
Requirements:

- Monitoring each step
- Must develop models that allow for ‘actionable’ events.

DevOps for AI



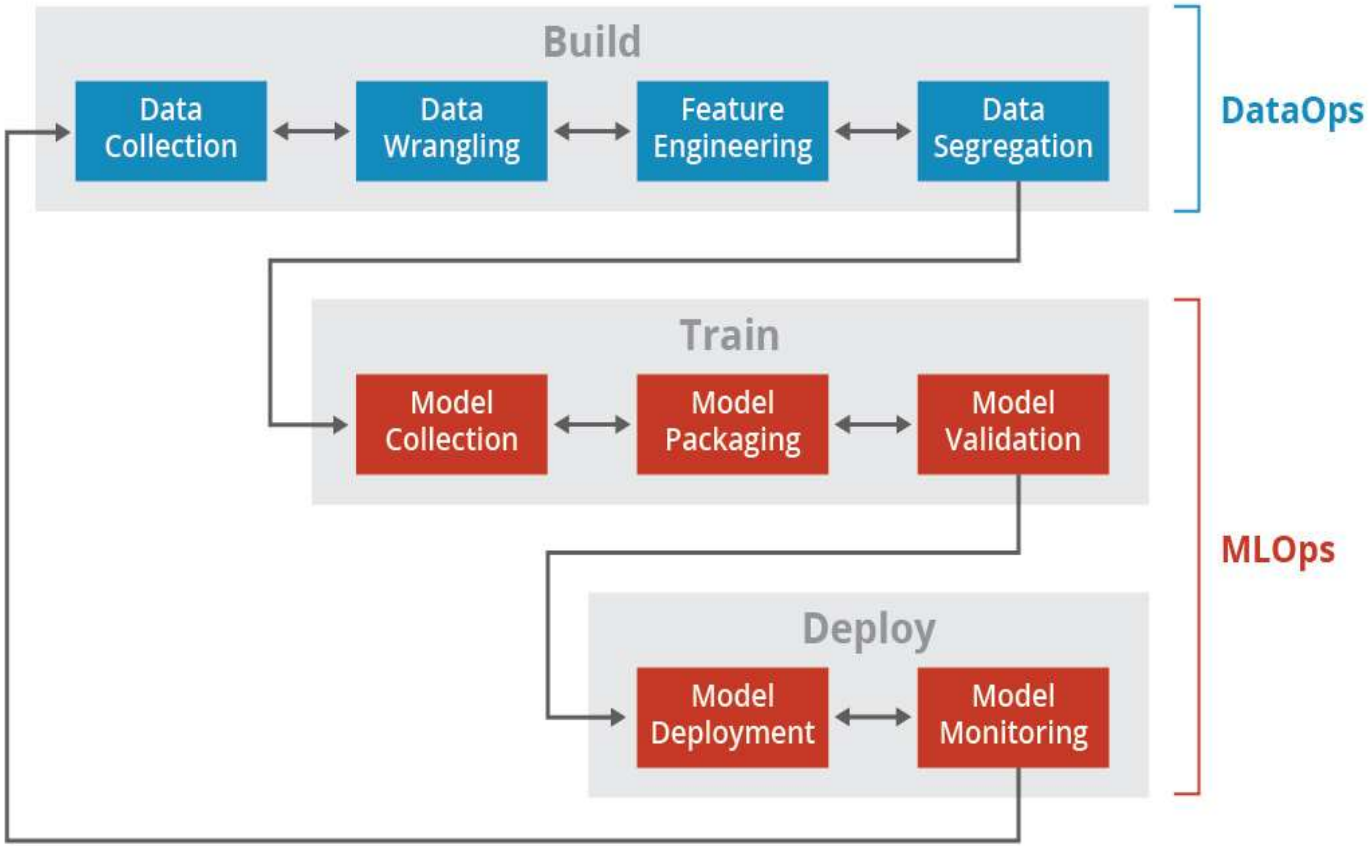
DevOps for AI



Using DevOps concepts and methodologies in every aspect of ML and AI enabled software systems.

- Data curation
- Training data
- Model creation, storage
- Deployment
- Monitoring
- Re-training

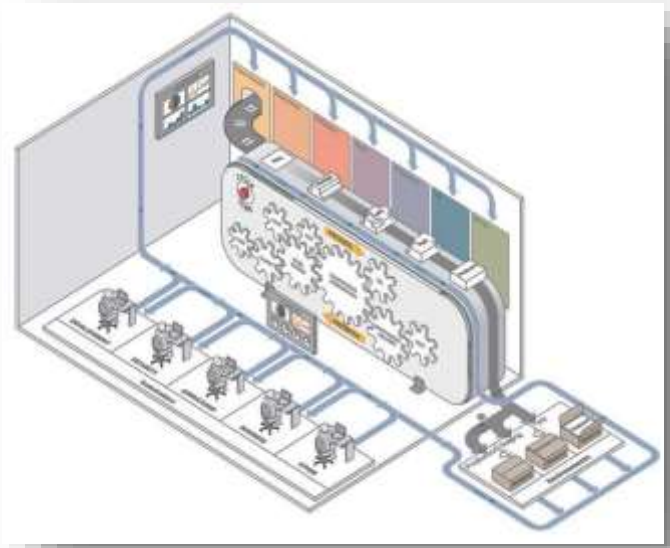
DataOps and MLOps exist



Important considerations

- Data must be prepared before model training
- Model release requires operationalization
- Post-deployment monitoring should record all real-world data serving as input to the deployed model
- Team members include
  - Data engineers, Data scientists
  - ML engineers, DevOps
  - Developers
- Model performance
- Deployment strategies
- Model storage and sharing

Necessary DevOps Factory additions



1. Embrace an MLOps culture to facilitate an ML-driven factory
2. Establish a cultural focus on data-driven development to facilitate ML model creation
3. Include data scientists and data engineers in software development teams

Images and quotes reside in the minor column.

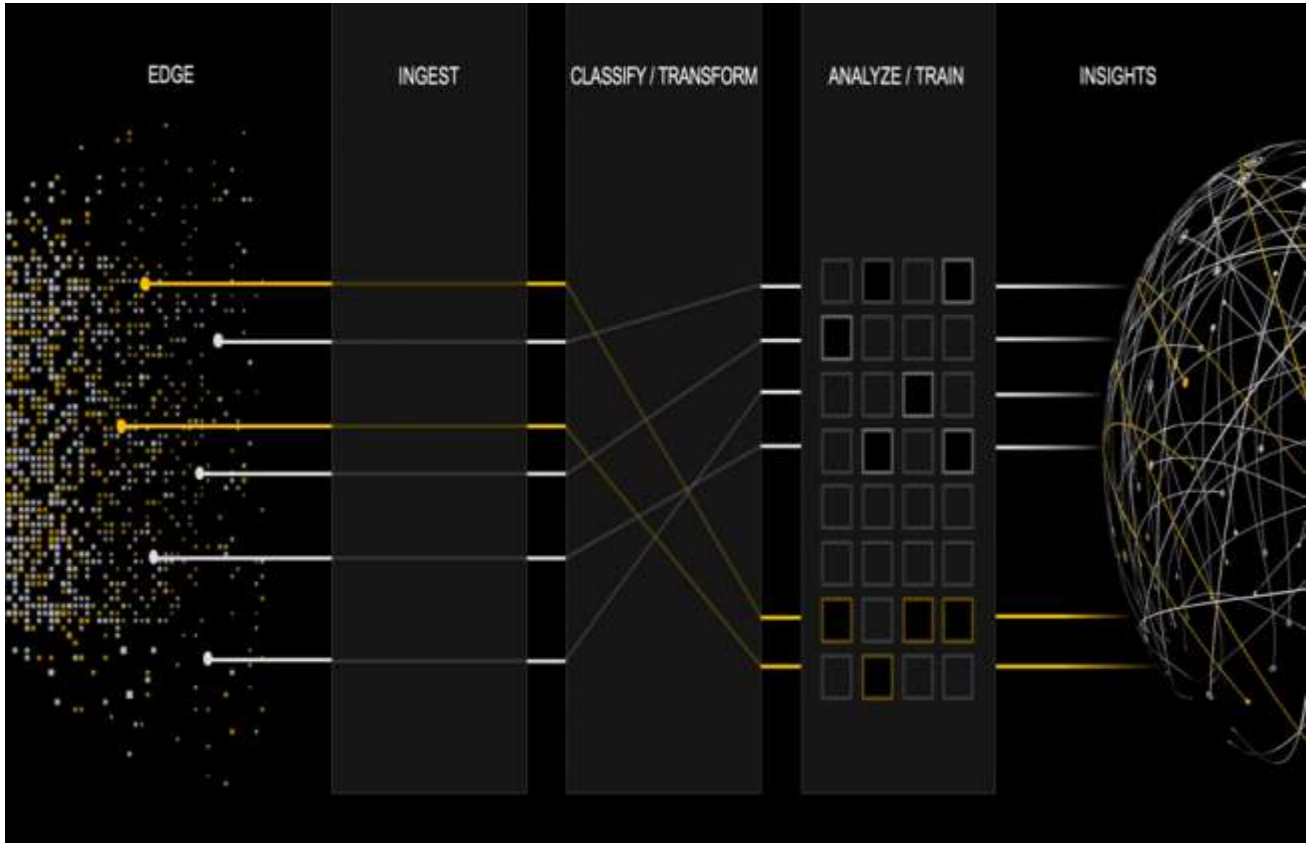
The major column accomodates more text.

DevOps for data curation

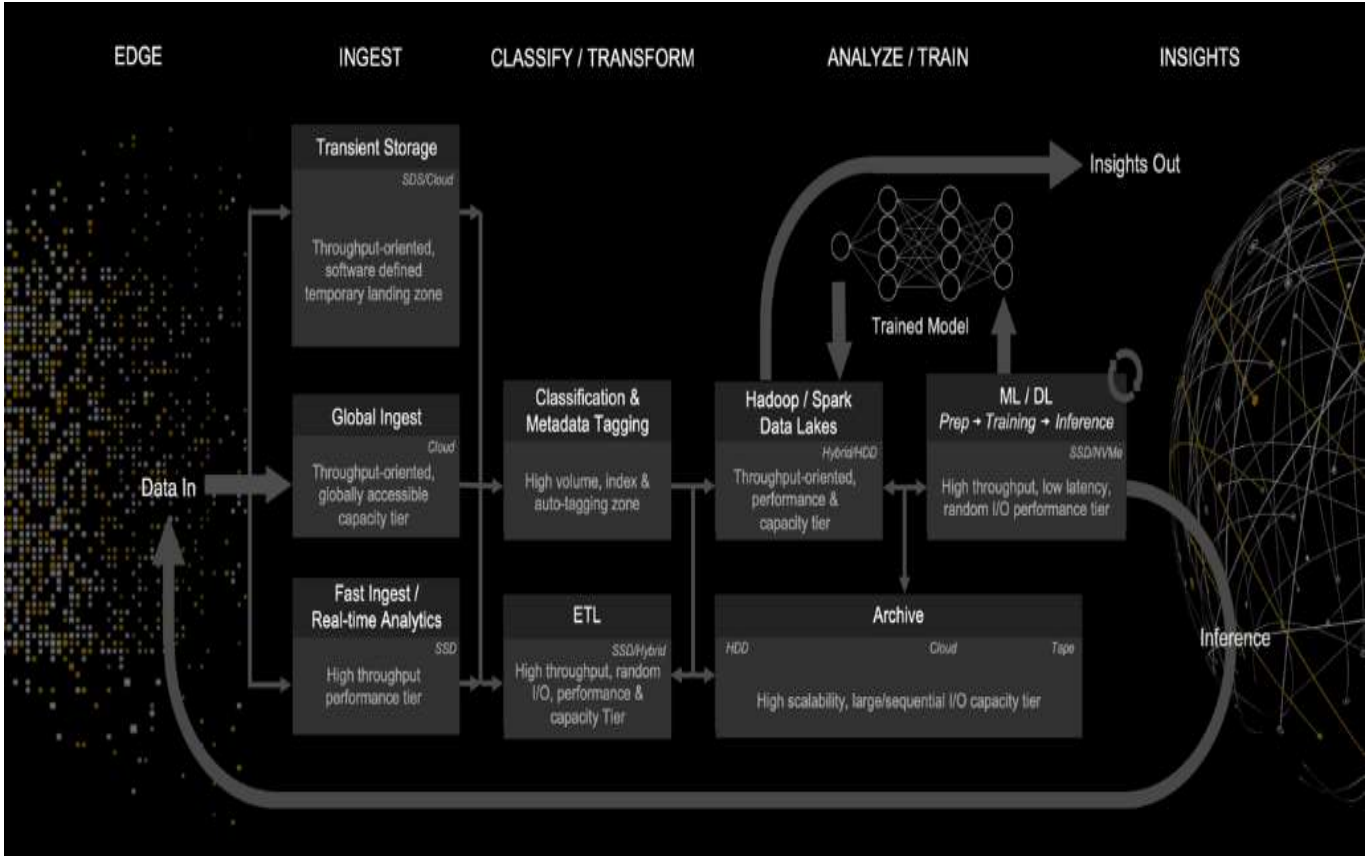
Data is a common critical element of an AI system

- The general process for data processing:
  - Ingest
  - Classify/transform/analyze
  - Insights

Data curation



Data curation - workflow

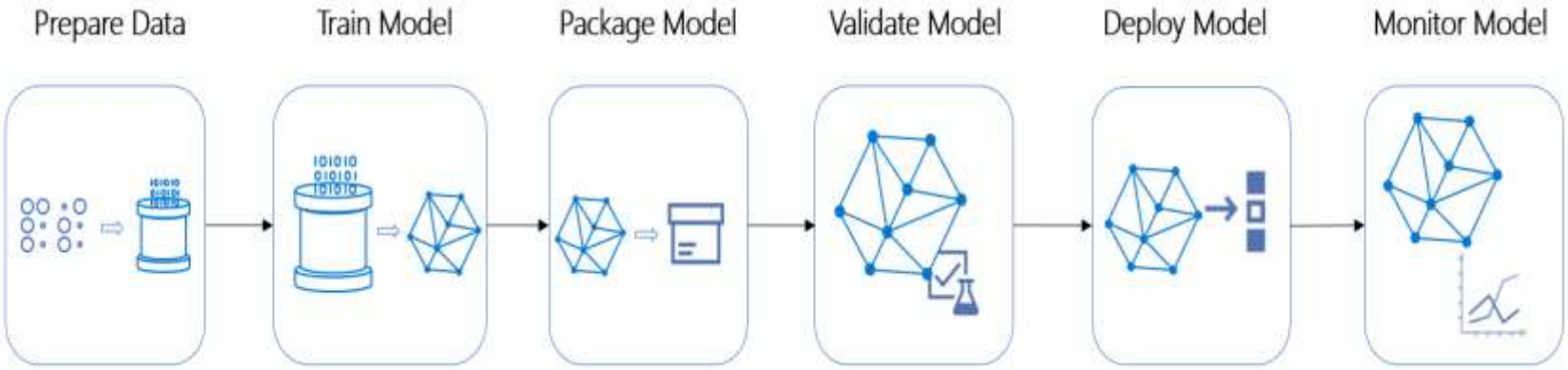


Monitoring deployed AI systems

- Include a return loop of data to the starting point of the pipeline
- Archive all ingress data to the model for future training
- Record and analyze the model's output for functionality and integrity
- Determine if a model requires modification or re-training

Additional guidance for an AI/ML Pipeline

- Capable of ingesting multiple data types
- Data maintained and versioned
  - Data Version Control (dvc.org)
- Real-time monitoring
- Responsive to changing conditions discovered during monitoring
- Traceability
- Language standardization



- Use DevOps to build, deploy, and monitor systems so that a pathway exists to take action on a ML/AI enabled system.
- These ‘actions’ could improve model performance, system security, and many other possibilities

For more information...

DevOps: https://www.sei.cmu.edu/go/devops

DevOps Blog: https://insights.sei.cmu.edu/devops

Webinar : https://www.sei.cmu.edu/publications/webinars/index.cfm

Podcast : https://www.sei.cmu.edu/publications/podcasts/index.cfm

Thank You

Hasan Yasar
Technical Director, Adjunct Faculty Member
Continuous Deployment of Capability
hyasar@sei.cmu.edu
@securelifecycle