Model Operationalization

With Governance and Model Risk Management

Open Data Science Conference (East) 2020

Sourav Mazumder
The Open Group Distinguished Data Scientist
ML Operationalization Leader
IBM Data and AI Expert Lab and Learning
smazumder@us.ibm.com
https://www.linkedin.com/in/souravmazumder/

Shikhar Kwatra
IBM Master Inventor
ML Operationalization Architect
IBM Data and AI Expert Lab and Learning
skwatra@us.ibm.com
https://www.linkedin.com/in/shikharkwatra/

Join us in https://github.com/ibm-cloud-architecture/refarch-ml-ops

Agenda

- Introduction to ML Operationalization
- ML Operationalization - Process, Persona, Environments and Frameworks/Platforms
- ML Operationalization in Action with Governance and Model Risk Management - Demonstration
- Hands On (Self Paced)

What is ML Operationalization

ML Operationalization

- Continuous Training
- Automated Validation and Deployment
- Insight Infusion at Scale
- Ensuring Transparency
- Removing Bias
- Business KPI Mapping
- Model Risk Management

"Creating an ML model is just a starting point. To bring the technology into production service, you need to solve various real-world issues such as building a **data pipeline for continuous training**, **automated validation** of the model, **version control** of the model, creating a **scalable serving infrastructure**, and ongoing operation of the ML infrastructure with **monitoring and alerting.**"

Forrester

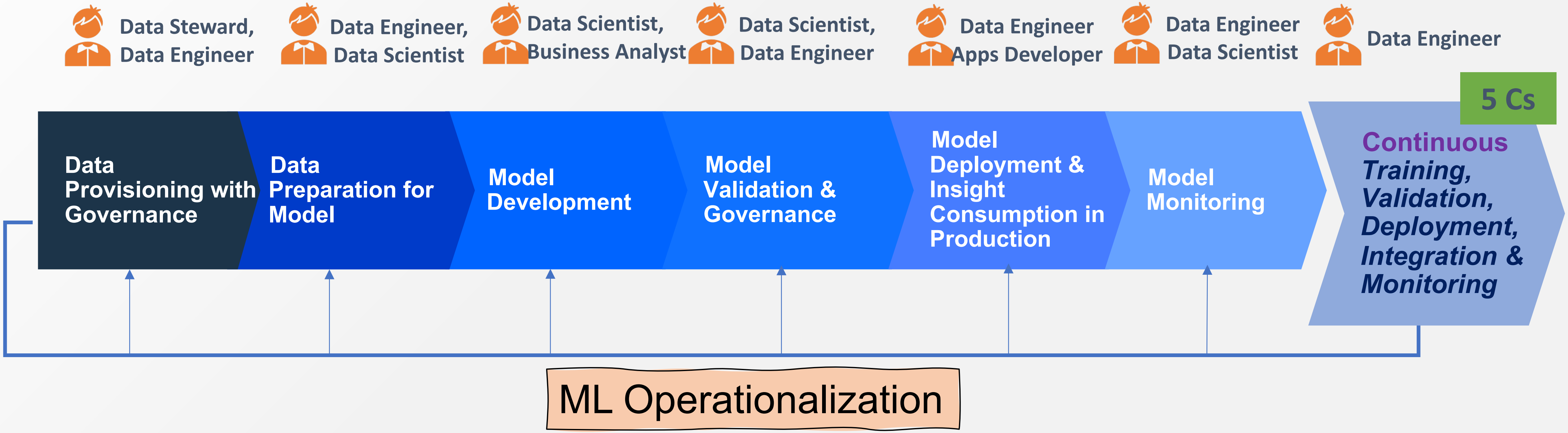
ML Ops can be daunting with different challenges faced by different organizations

- ‘From Model conception to use in Production it takes any time between 48 to 60 weeks
- ‘Need to onboard large number of contractors, track the datasets used for developing Models, how the Models are providing Business Value’
- ‘How to use the platform to scale the Model to serve 10 M requests in a day and Monitor those requests’
- ‘Need to institutionalize collaborative approach involving multiple teams to deliver Models without Bias and ability to trace back Models’ Lineage’
- ‘How to setup a process to make auditors believe on the approach to arrive at Prediction’
- ‘Need a Framework to ramp up my Business Analysts in Data Science to churn Models fast for use by Actuaries’
- ‘Need to get Explanation for every *case predicted as ‘Risk’* by I Risk Prediction Model

ML Operationalization – High Level Steps and Personas

ML Operationalization refers to operationalization of Machine Learning Models for production use to realize business value out of those Models.

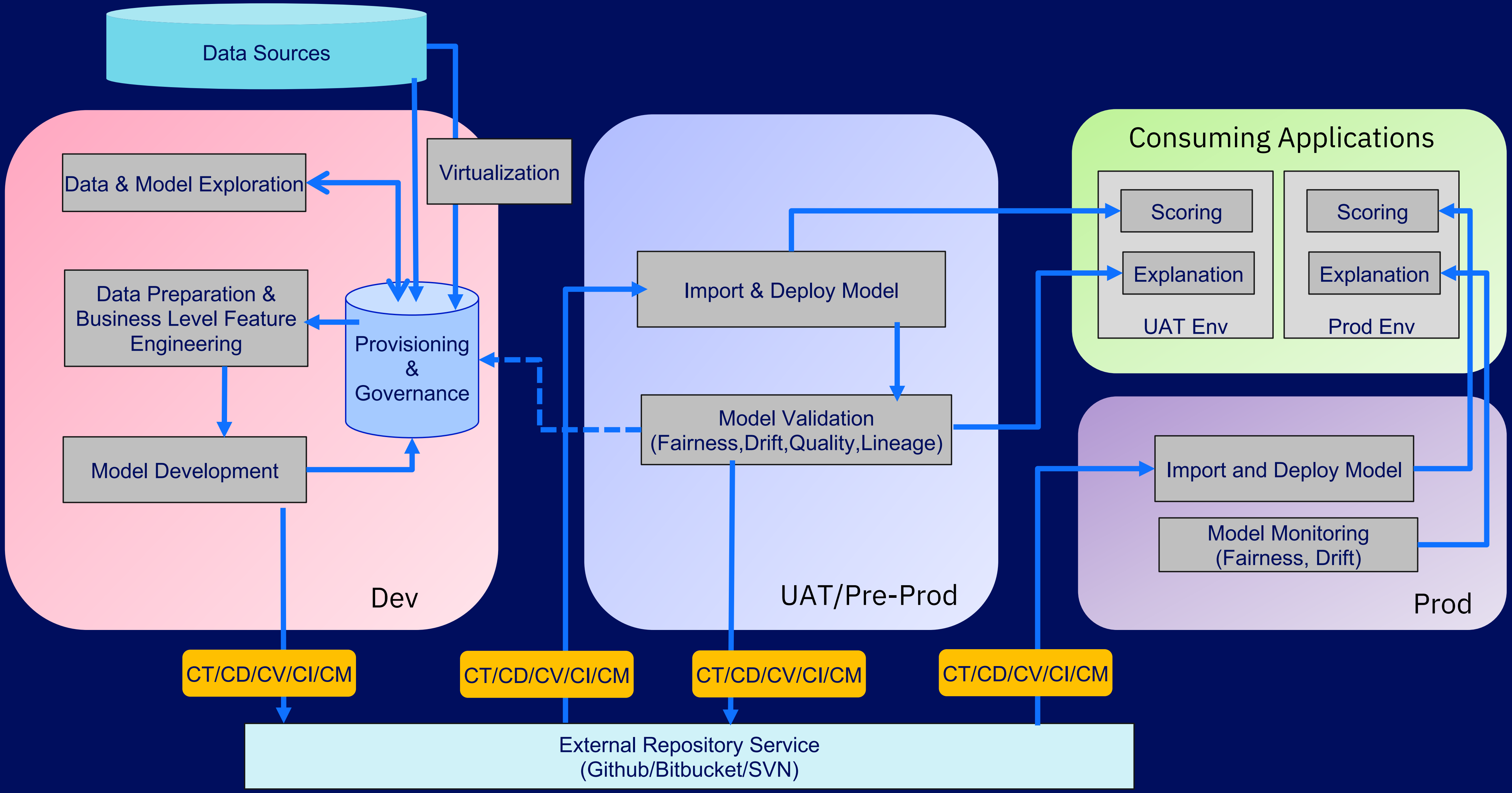
ML Operationalization overlays paradigm of DevOps on Model Lifecycle management process (CRISP-DM)



Data Steward, Data Engineer
Data Engineer, Data Scientist
Data Scientist, Business Analyst
Data Scientist, Data Engineer
Data Engineer Apps Developer
Data Engineer Data Scientist
Data Engineer
5 Cs
Data Provisioning with Governance
Data Preparation for Model
Model Development
Model Validation & Governance
Model Deployment & Insight Consumption in Production
Model Monitoring
Continuous Training, Validation, Deployment, Integration & Monitoring
ML Operationalization

For Conceptual View of ML Ops please check - https://ibm.co/AI-Ops

ML Operationalization spread across Dev, UAT & Prod Environments

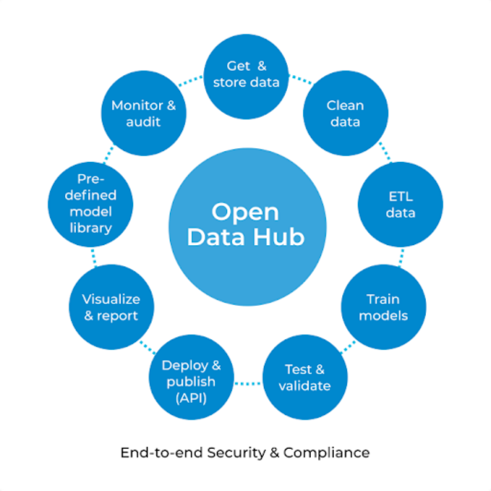


What to look for in ML Frameworks ?

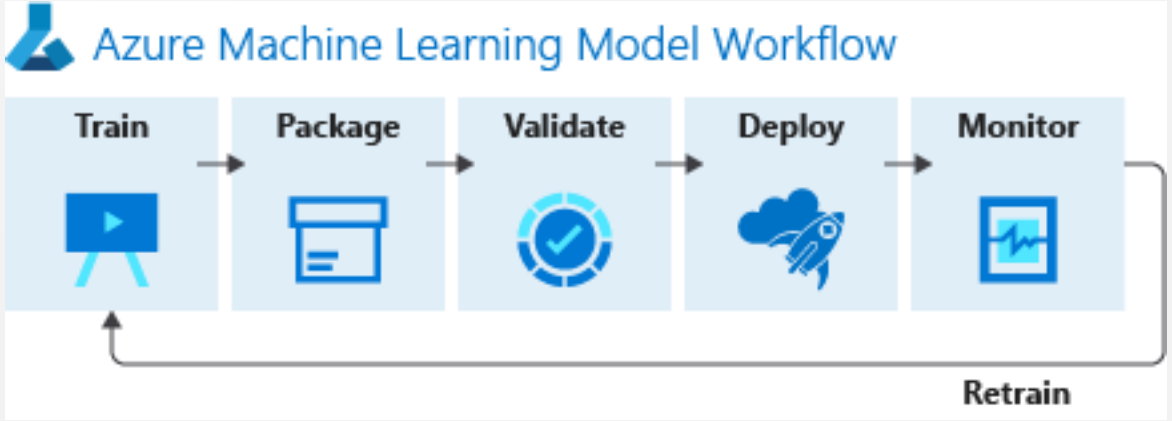
Features	Description
Flexibility/Customizability	How flexible is the platform in integrating and/or customizing new frameworks for AI model development.
Ease of Use	How easy is it to leverage these tools and proposed techniques from setup to application.
Integrations	How well does the platform integrate with Git or other model versioning and source control tools, catalogs (for governance and discoverability) or various data sources.
Governance	How well does the solution support governance and discoverability of assets (data assets, models, notebooks, ...)
Platform	Support for various platforms (public cloud, on-prem, hybrid cloud), and compute types (CPU/GPU) for training and scoring (or inference) AI models
Monitoring	How well does the solution support monitoring AI models for performance / explainability / fairness
Scalability	How scalable is the platform in supporting various Data & AI users in different roles to explore, develop, and deploy AI models.
Openness	How well does the platform support open-source technologies which has become a key differentiator for platform providers.
Security	How well does the platform support enterprise-grade security access to the platform in terms of authorization and authentication
Support for 5 Cs	Support for Continuous Training, Validation, Deployment, Integration and Monitoring

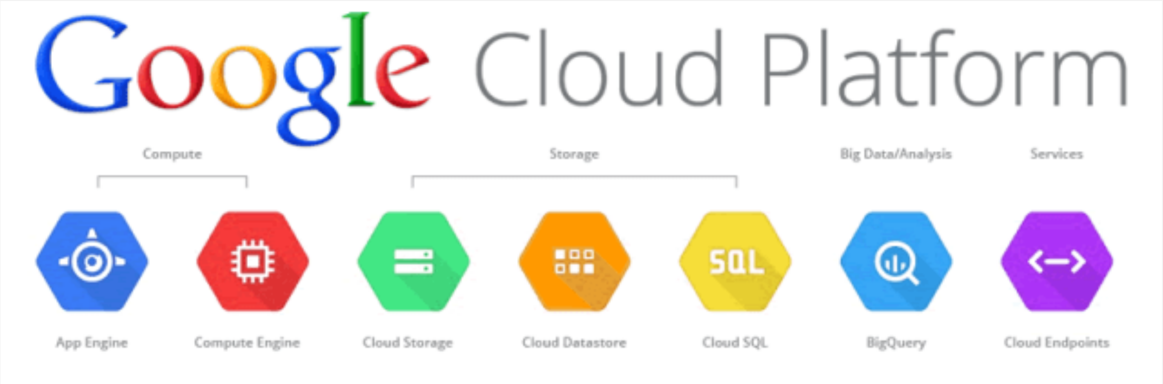
Popular ML Ops Tools and Frameworks

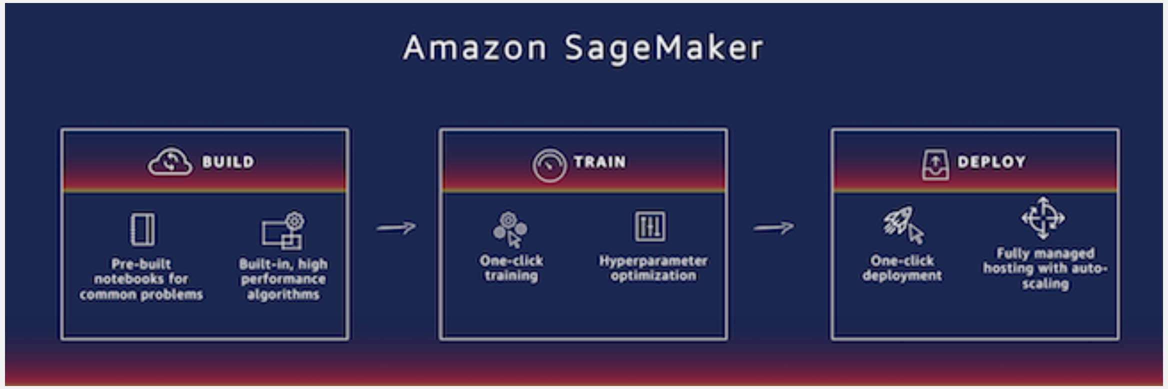
Open Source Frameworks



From Software Vendors

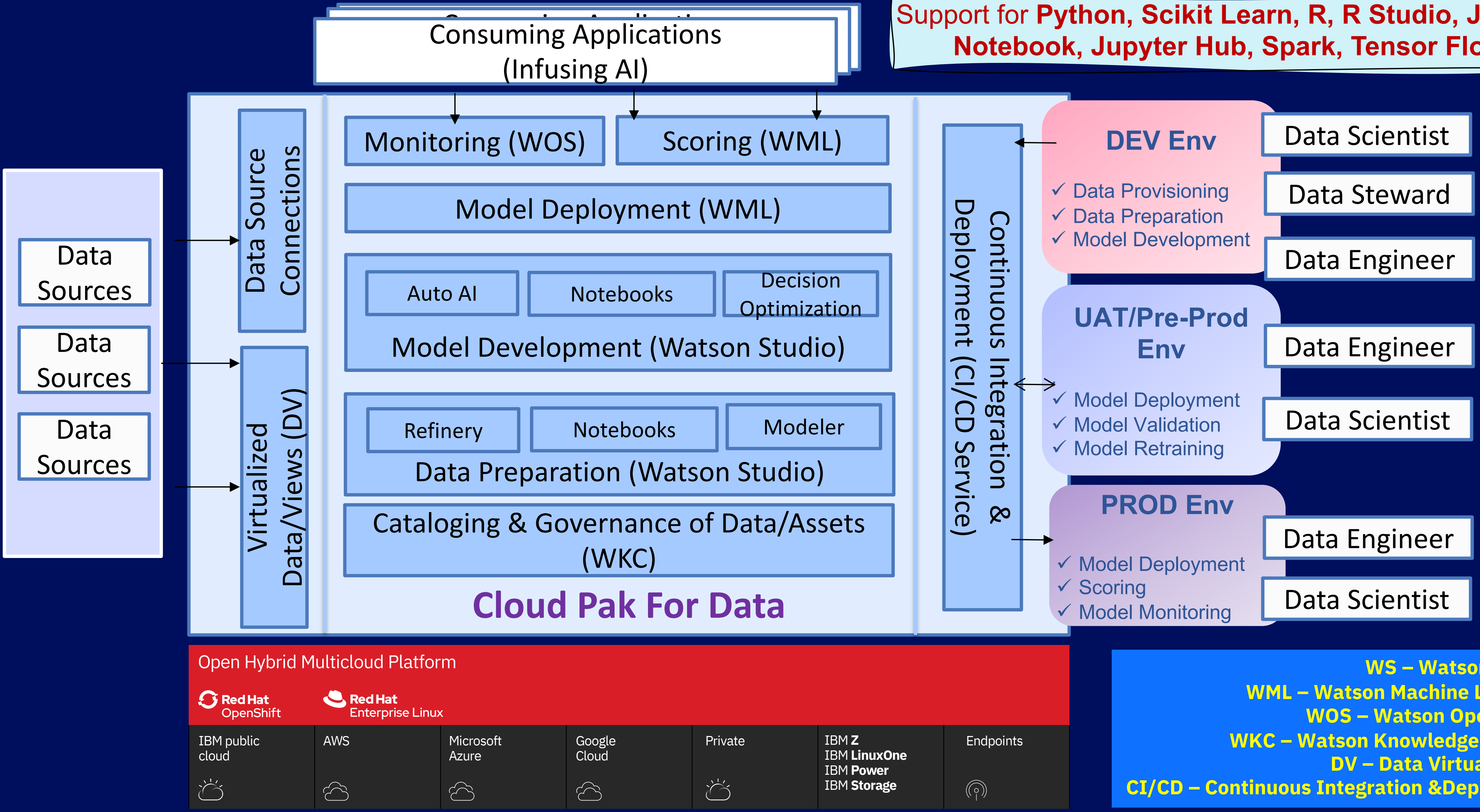





Amazon SageMaker
BUILD
Pre-built notebooks for common problems
Built-in, high performance algorithms
TRAIN
One-click training
Hyperparameter optimization
DEPLOY
One-click deployment
Fully managed hosting with auto-scaling

ML Operationalization with IBM Cloud Pak For Data

Support for **Python, Scikit Learn, R, R Studio, Jupyter Notebook, Jupyter Hub, Spark, Tensor Flow**



Consuming Applications (Infusing AI)

Data Sources

Data Sources

Data Sources

Data Source Connections

Virtualized Data/Views (DV)

Monitoring (WOS)

Scoring (WML)

Model Deployment (WML)

Auto AI

Notebooks

Decision Optimization

Model Development (Watson Studio)

Refinery

Notebooks

Modeler

Data Preparation (Watson Studio)

Cataloging & Governance of Data/Assets (WKC)

Cloud Pak For Data

Continuous Integration & Deployment (CI/CD Service)

DEV Env
- ✓ Data Provisioning
- ✓ Data Preparation
- ✓ Model Development

Data Scientist

Data Steward

Data Engineer

UAT/Pre-Prod Env
- ✓ Model Deployment
- ✓ Model Validation
- ✓ Model Retraining

Data Engineer

Data Scientist

PROD Env
- ✓ Model Deployment
- ✓ Scoring
- ✓ Model Monitoring

Data Engineer

Data Scientist

Open Hybrid Multicloud Platform

Red Hat OpenShift

Red Hat Enterprise Linux

IBM public cloud

AWS

Microsoft Azure

Google Cloud

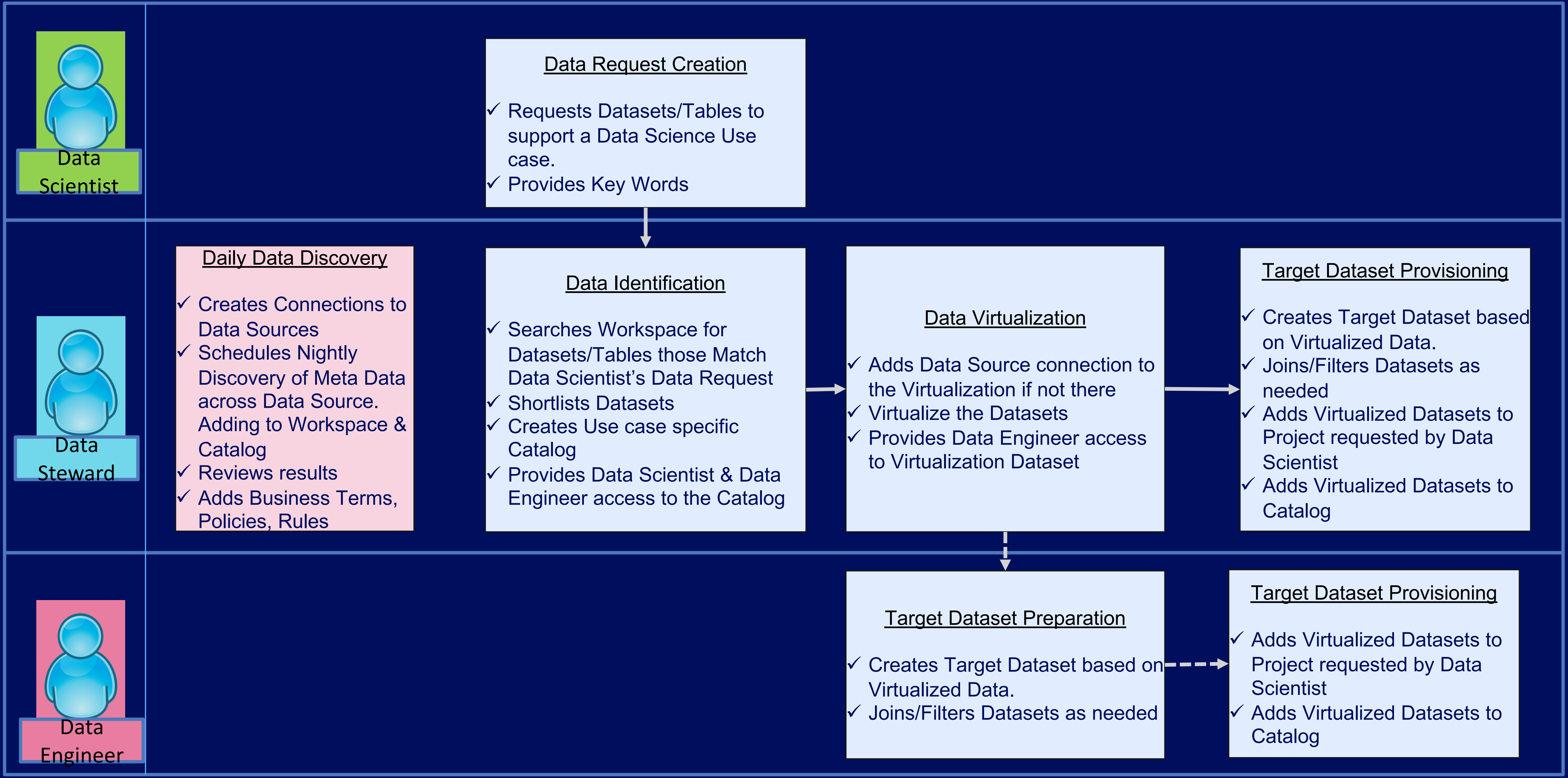
Private

IBM Z
IBM LinuxOne
IBM Power
IBM Storage

Endpoints

WS – Watson Studio
WML – Watson Machine Learning
WOS – Watson Open Scale
WKC – Watson Knowledge Catalog
DV – Data Virtualization
CI/CD – Continuous Integration &Deployment

ML Ops In Action (1/2) - Data Provisioning and Governance



Data Request Creation

- ✓ Requests Datasets/Tables to support a Data Science Use case.
- ✓ Provides Key Words

Daily Data Discovery

- ✓ Creates Connections to Data Sources
- ✓ Schedules Nightly Discovery of Meta Data across Data Source. Adding to Workspace & Catalog
- ✓ Reviews results
- ✓ Adds Business Terms, Policies, Rules

Data Identification

- ✓ Searches Workspace for Datasets/Tables those Match Data Scientist's Data Request
- ✓ Shortlists Datasets
- ✓ Creates Use case specific Catalog
- ✓ Provides Data Scientist & Data Engineer access to the Catalog

Data Virtualization

- ✓ Adds Data Source connection to the Virtualization if not there
- ✓ Virtualize the Datasets
- ✓ Provides Data Engineer access to Virtualization Dataset

Target Dataset Provisioning

- ✓ Creates Target Dataset based on Virtualized Data.
- ✓ Joins/Filters Datasets as needed
- ✓ Adds Virtualized Datasets to Project requested by Data Scientist
- ✓ Adds Virtualized Datasets to Catalog

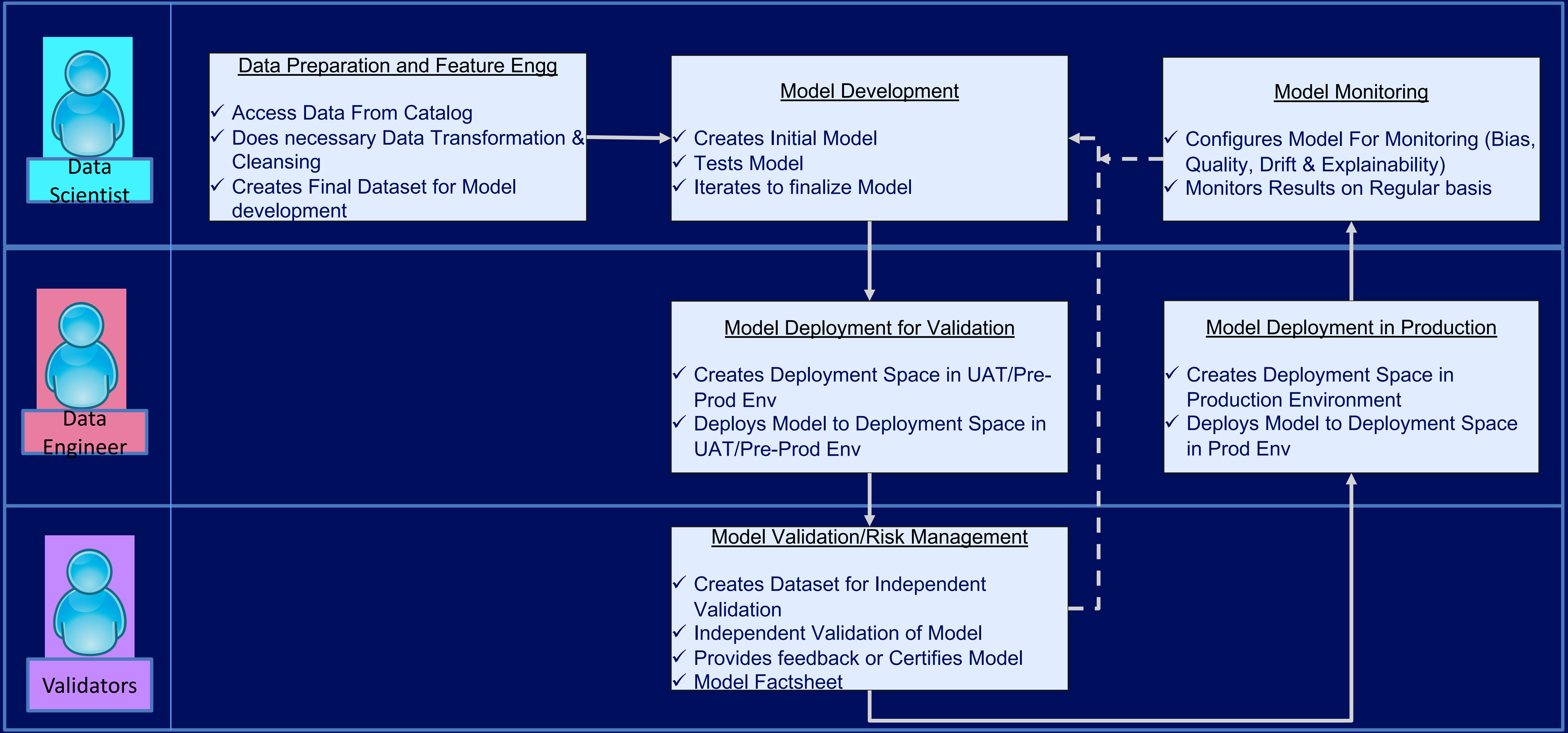
Target Dataset Preparation

- ✓ Creates Target Dataset based on Virtualized Data.
- ✓ Joins/Filters Datasets as needed

Target Dataset Provisioning

- ✓ Adds Virtualized Datasets to Project requested by Data Scientist
- ✓ Adds Virtualized Datasets to Catalog

ML Ops In Action (2/2) - Model Development, Deployment & Monitoring



Data Scientist

Data Preparation and Feature Engg

- ✓ Access Data From Catalog
- ✓ Does necessary Data Transformation & Cleansing
- ✓ Creates Final Dataset for Model development

Model Development

- ✓ Creates Initial Model
- ✓ Tests Model
- ✓ Iterates to finalize Model

Model Monitoring

- ✓ Configures Model For Monitoring (Bias, Quality, Drift & Explainability)
- ✓ Monitors Results on Regular basis

Data Engineer

Model Deployment for Validation

- ✓ Creates Deployment Space in UAT/Pre-Prod Env
- ✓ Deploys Model to Deployment Space in UAT/Pre-Prod Env

Model Deployment in Production

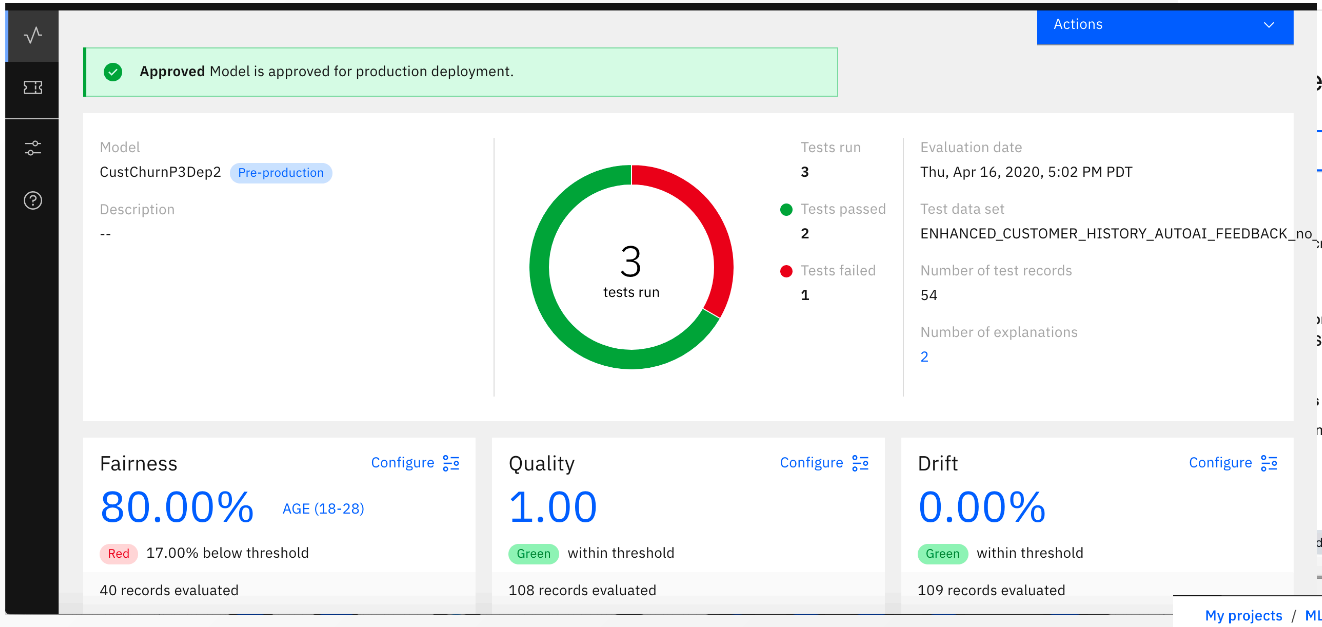
- ✓ Creates Deployment Space in Production Environment
- ✓ Deploys Model to Deployment Space in Prod Env

Validators

Model Validation/Risk Management

- ✓ Creates Dataset for Independent Validation
- ✓ Independent Validation of Model
- ✓ Provides feedback or Certifies Model
- ✓ Model Factsheet

ML Ops - Demonstration



Actions

Approved Model is approved for production deployment.

Model
CustChurnP3Dep2 Pre-production

Description
--

3
tests run

Tests run
3

Tests passed
2

Tests failed
1

Evaluation date
Thu, Apr 16, 2020, 5:02 PM PDT

Test data set
ENHANCED_CUSTOMER_HISTORY_AUTOAI_FEEDBACK_no

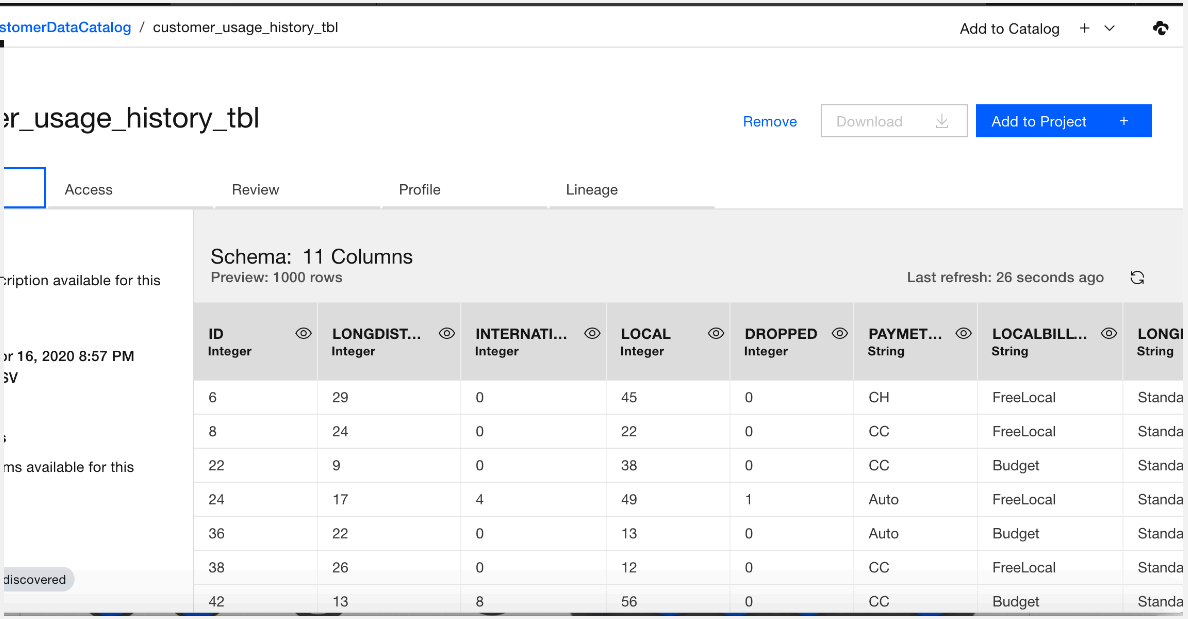
Number of test records
54

Number of explanations
2

Fairness Configure
80.00% AGE (18-28)
Red 17.00% below threshold
40 records evaluated

Quality Configure
1.00
Green within threshold
108 records evaluated

Drift Configure
0.00%
Green within threshold
109 records evaluated



Catalogs / CustomerDataCatalog / customer_usage_history_tbl

Add to Catalog +

er_usage_history_tbl

Remove Download Add to Project +

Access Review Profile Lineage

cription available for this

or 16, 2020 8:57 PM
SV

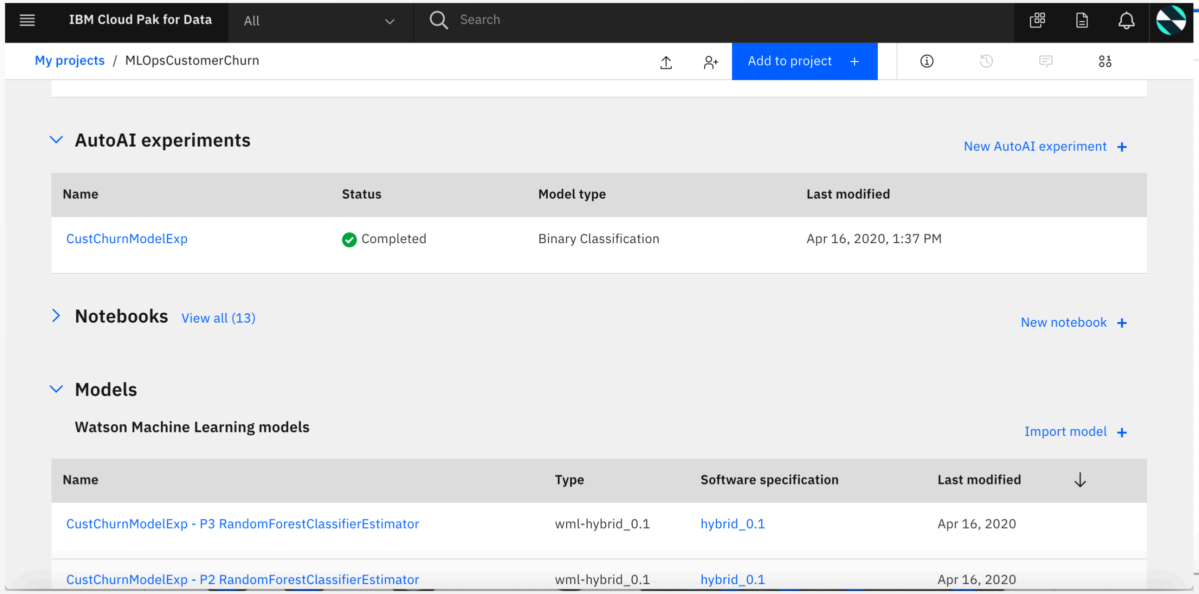
ms available for this

discovered

Schema: 11 Columns
Preview: 1000 rows

Last refresh: 26 seconds ago

ID Integer	LONGDIST... Integer	INTERNATI... Integer	LOCAL Integer	DROPPED Integer	PAYMET... String	LOCALBILL... String	LONGI String
6	29	0	45	0	CH	FreeLocal	Standa
8	24	0	22	0	CC	FreeLocal	Standa
22	9	0	38	0	CC	Budget	Standa
24	17	4	49	1	Auto	FreeLocal	Standa
36	22	0	13	0	Auto	Budget	Standa
38	26	0	12	0	CC	FreeLocal	Standa
42	13	8	56	0	CC	Budget	Standa



IBM Cloud Pak for Data All Search

My projects / MLOpsCustomerChurn

Add to project +

AutoAI experiments

New AutoAI experiment +

Name	Status	Model type	Last modified
CustChurnModelExp	Completed	Binary Classification	Apr 16, 2020, 1:37 PM

Notebooks View all (13)

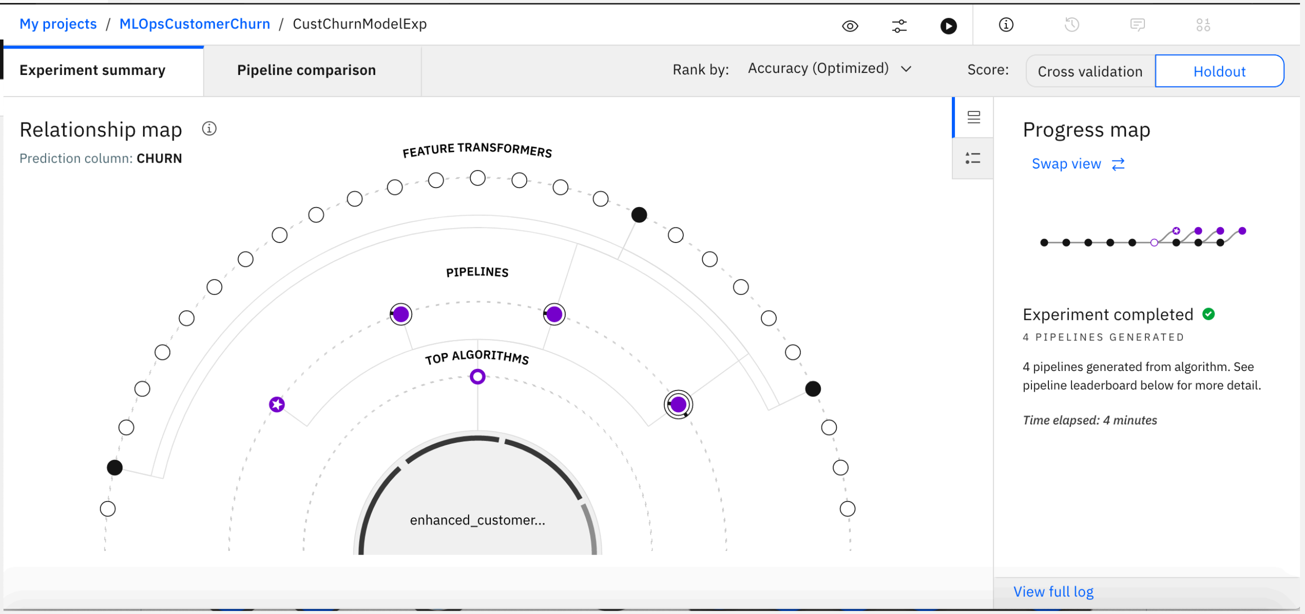
New notebook +

Models

Watson Machine Learning models

Import model +

Name	Type	Software specification	Last modified
CustChurnModelExp - P3 RandomForestClassifierEstimator	wml-hybrid_0.1	hybrid_0.1	Apr 16, 2020
CustChurnModelExp - P2 RandomForestClassifierEstimator	wml-hybrid_0.1	hybrid_0.1	Apr 16, 2020



My projects / MLOpsCustomerChurn / CustChurnModelExp

Experiment summary Pipeline comparison

Rank by: Accuracy (Optimized)

Score: Cross validation Holdout

Relationship map
Prediction column: CHURN

Progress map
Swap view

Experiment completed
4 PIPELINES GENERATED
4 pipelines generated from algorithm. See pipeline leaderboard below for more detail.
Time elapsed: 4 minutes

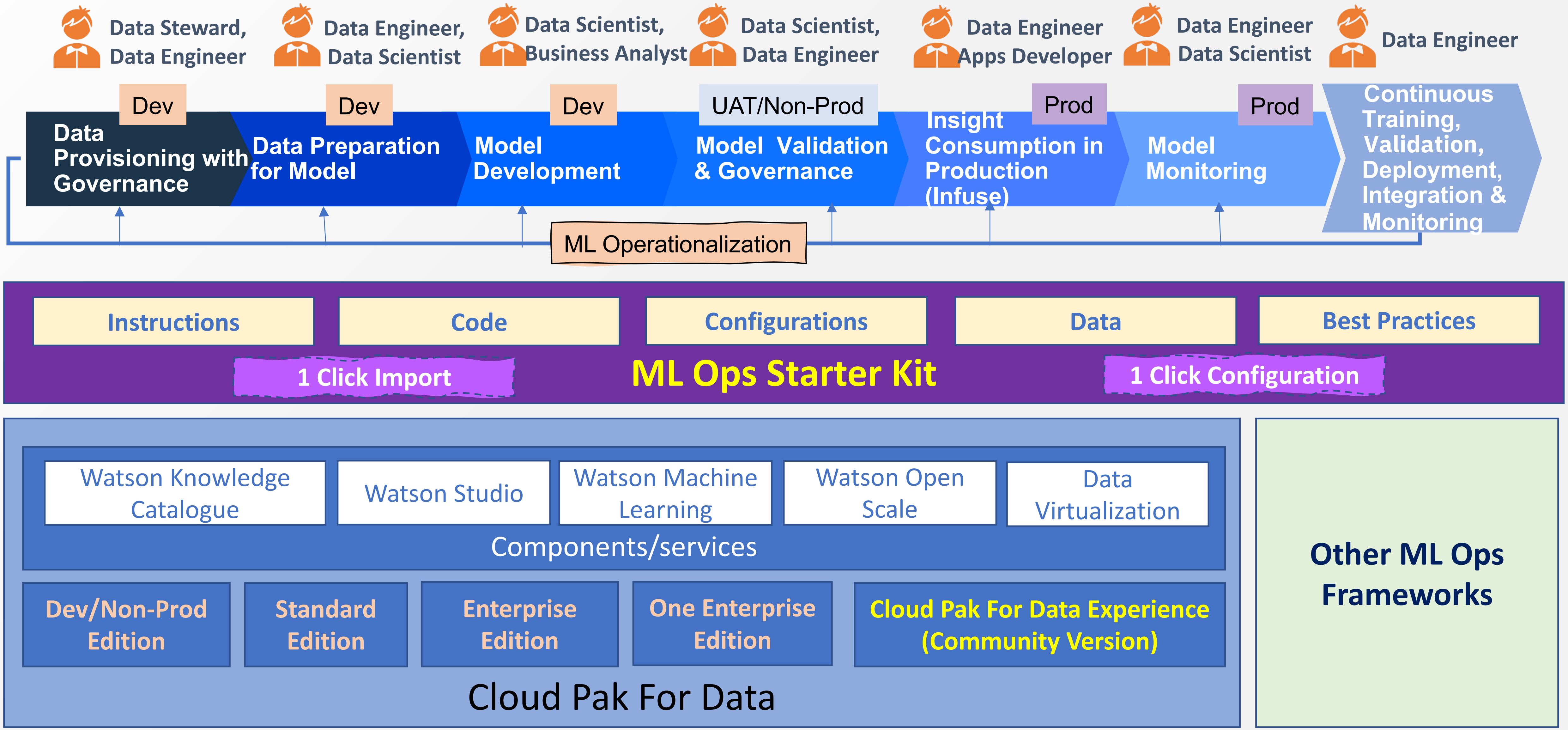
View full log

ML Ops – Self paced Hands On

- Go to IBM Cloud Architecture Center - https://www.ibm.com/cloud/architecture/architectures/dataAIArchitecture/solutions
- Click on the tile 'Drive business results from your machine learning Models' in Solution section
- In the next page click on Get the Code – this will take you to Public Github fro MLOps
- Go through the ReadMe. In How to get Started section click on the link for Cloud Pak For Data Experience. There you will have the instruction to get your free cluster for Cloud Pak For Data. Follow the instruction and get your Cloud Pak For Data Experience cluster (takes 5 minutes)
- Go through the rest of the steps in section 'How to get Started' to get started with your self paced Hands On

Getting Started with ML Operationalization using ML Ops Starter Kit

End 2 End framework to help get started with ML Operationalization



Data Steward, Data Engineer

Dev

Data Provisioning with Governance

Data Engineer, Data Scientist

Dev

Data Preparation for Model

Data Scientist, Business Analyst

Dev

Model Development

Data Scientist, Data Engineer

UAT/Non-Prod

Model Validation & Governance

Data Engineer Apps Developer

Prod

Insight Consumption in Production (Infuse)

Data Engineer Data Scientist

Prod

Model Monitoring

Data Engineer

Continuous Training, Validation, Deployment, Integration & Monitoring

ML Operationalization

Instructions

Code

Configurations

Data

Best Practices

1 Click Import

ML Ops Starter Kit

1 Click Configuration

Watson Knowledge Catalogue

Watson Studio

Watson Machine Learning

Watson Open Scale

Data Virtualization

Components/services

Dev/Non-Prod Edition

Standard Edition

Enterprise Edition

One Enterprise Edition

Cloud Pak For Data Experience (Community Version)

Cloud Pak For Data

Other ML Ops Frameworks

Let us Discuss more about ML Ops

Q and A

Join us in https://github.com/ibm-cloud-architecture/refarch-ml-ops

Thank You