



THE ROAD TO ML(SEC)OPS:

Accelerate AI/ML initiatives responsibly by bridging the gap between DevOps, SecOps, and MLOps

To accelerate, secure, and scale AI/ML initiatives, organizations must normalize the management of ML models and artifacts under the same development, security, and operational principles they apply to traditional software development. Treating AI/ML as part of the overall software development lifecycle also reduces silos and enhances collaboration across departments – critical to the sustained success of any business.

This is the road to MLSecOps!

WELCOME TO THE ML DEVELOPMENT LIFECYCLE

1



PLANNING

Define project objectives, understand the problem domain, and identify required resources, including data, tools, and team members, while also considering potential security risks and compliance regulations that must be addressed throughout the lifecycle.

2



DATA ENGINEERING

Collect, clean, and transform raw data into a structured format suitable for analysis and modeling. Pay attention to data governance practices, such as ensuring data privacy, integrity, and adherence to security protocols during data collection and handling.

3



MODEL TRAINING

Develop and select machine learning algorithms suited to the problem, adhering to secure coding practices, version control, and documentation for reproducibility. Train and refine the model using the dataset, implement automated testing and CI/CD workflows, and apply security measures to protect training data. Use experiment management to track and analyze experiments for informed decision-making.

4



MODEL VALIDATION

Evaluate the trained model against a separate dataset to assess its performance, accuracy, and generalizability. This evaluation involves various techniques, such as cross-validation and hyperparameter tuning, to ensure the model meets the desired standards and can effectively make predictions on unseen data.

5



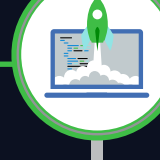
PACKAGING

Organize the trained model and its dependencies into a deployable package, ensuring proper versioning and configuration management, crucial elements of both DevOps and security, to facilitate secure and efficient deployment.

DEPLOYMENT

Deploy the packaged model into a live environment, where DevOps practices such as continuous integration and deployment (CI/CD) are utilized alongside standard security measures to ensure that the deployment process is secure and reliable.

6



7



MODEL INFERENCE

After the release, the model generates predictions based on real-time data, with configurable parameters. Focus on building scalable and reliable inference applications to ensure optimal performance and responsiveness, while implementing access controls and security monitoring to safeguard against unauthorized use, aligning with security best practices.

MONITORING

Continuously assess the model's performance, track metrics, employ logging and monitoring tools for anomalies, and apply security measures to protect the system from potential threats or data breaches, ensuring adherence to both operational and security guidelines. The need for a model retrain trigger is also continuously evaluated, as model degradation over time is expected.

7



If you're curious about how to integrate DevOps, SecOps, and MLOps into your organization's AI/ML strategy or would like more insights into the JFrog Platform for ML model management, **book a demo** today.

[Book a JFrog ML demo](#)