PRODUCTION (1)

Déployer le système dans un environnement réel afin qu'il puisse traiter des données en direct et fournir des résultats exploitables. La phase de production doit inclure la surveillance et la maintenance continue.

Déploiement du système

Prendre des mesures correctives afin d'assurer la performance et la robustesse du modèle et maintenir l'alignement de la pertinence du système aux besoins métier.

Surveillance du système

Supervision en continu de la qualité des données, la performance du modèle et l'intégrité du système.

Maintenance du système

Prendre des mesures correctives afin d'assurer la performance et la robustesse du modèle et maintenir l'alignement de la pertinence du système aux besoins métier.

(1) La phase et les étapes font référence au livrable « Opérationnaliser la gestion des risques » du GT Banque du Hub France IA.

HUB FRANCE .IA

AI Act – Opérationnalisation

PRODUCTION

Préalables nécessaires

- **Description de l'infrastructure de production et des modalités de déploiement**

1. Déploiement

- Définir et dimensionner **l'infrastructure de production** du SIA
- Effectuer une analyse des potentiels risques cyber
- Déployer une infrastructure **CI/CD**
- Déployer l'infrastructure, effectuer les tests unitaires, déployer le modèle en production
- **Mettre à jour le versioning**
- **Compléter la documentation**

2. Surveillance du système

- Définir une stratégie de supervision du SIA et de son intégrité cyber.
- Vérifier les entrées et les sorties du modèle (monitoring)
- Décrire les indicateurs de performance et des seuils d'action, établir le plan de mise à jour et de maintenance du modèle, définir les métriques d'utilisation
- **Définir et mettre en place un contrôle humain**, afin de surveiller le fonctionnement du SIA (données, biais, etc.) (Art. 14.4 a)
- Assurer la tenue des logs automatiques du système (Art. 12 b)
- Évaluer d'autres risques susceptibles d'apparaître (système de surveillance post-commercialisation) (Art. 72.1 & 9.2 c)
- Si incident, ou risque d'incident, signalement aux autorités de surveillance (Art. 20)

3. Maintenance du système

- Go/No Go re-entraînement du modèle ou adaptation du système
- Si nécessaire, mesures correctives (Art. 73)

Boîte à outils

- Stratégie de déploiement d'un SIA (Standard)
- Outils de gestion et de déploiement des modèles (MLflow, Kubeflow, Comet, Bento ML etc.)
- Outils de versioning

- Protocole de surveillance continue
- Outils de gestion des alertes (boîtes mail, ticketing, alertes, notifications)
- Outils de quantification d'incertitudes
- Outils de monitoring de biais
- Système de gestion des logs
- Protocole de signalement des incidents, (v. normes sectorielles)

- Process interne de gestion et maintenance des SIA

Notre *check-list* pour vous aider à opérationnaliser l'AI Act

- *Mise à jour de la* **Documentation technique du système**

- Registre des Logs automatiques du système
- **Protocole de surveillance continue** (Art. 72)
- Rapport sur les résultats des contrôles réguliers (audits)
- **Notice d'utilisation** à l'attention des déployeurs : mesures de suivi/surveillance
- Documentation technique (Annexe IV, .3)

- *Mise à jour de la* **Notice d'utilisation** à l'attention des déployeurs, avec les mesures de maintenance nécessaires pour assurer le bon fonctionnement du système