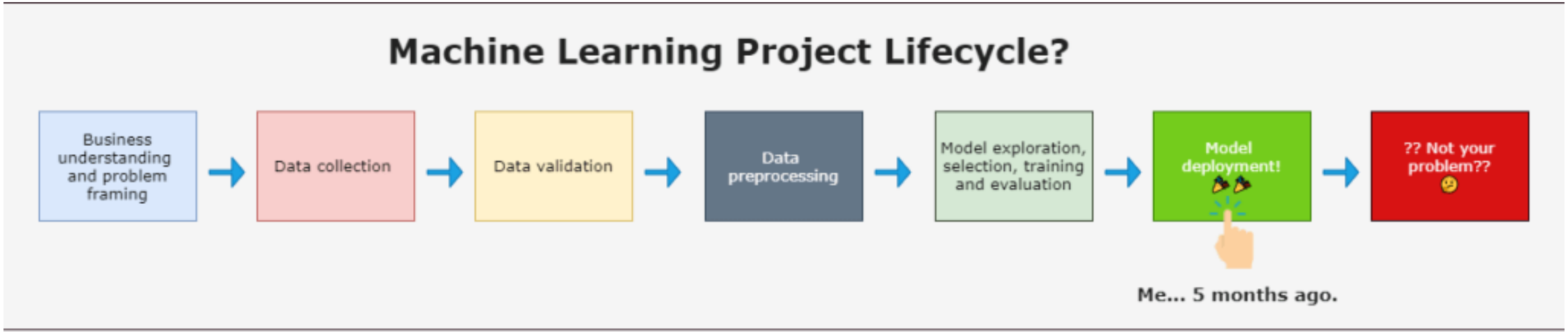
TÉCNICAS QUE USAREMOS PARA AJUSTAR O MODIFICAR NUESTROS MODELOS EN CASO DE NO OBTENER EL RESULTADO ESPERADO.

A1 R3

Consideremos el ciclo de un proyecto con ML

¿Se pueden hacer cambios “on the run”?, la respuesta es si, de hecho es lo deseable puesto que los datos son dinámicos y los requerimientos tienden a variar según la circunstancias.

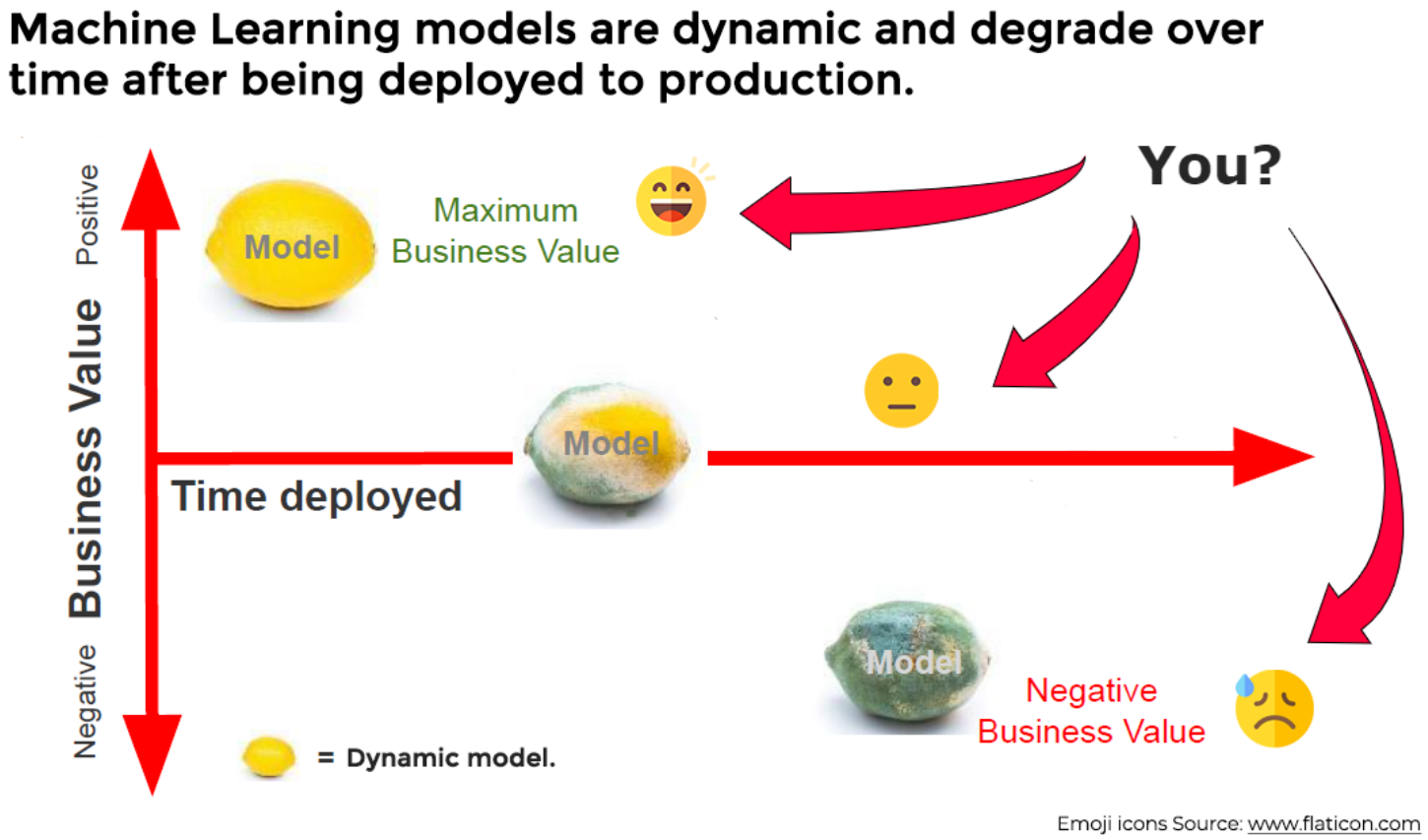
El proceso no acaba una vez implementado… va más allá.



Si el negocio va bien, saldrán cambios necesarios de forma automática.

los modelos de aprendizaje autom
degradan con el tiempo. Son dinám
sensibles a los cambios reales en el
real.

Desde el momento en que implemer
modelo en producción, comienza a
degradarse en términos de rendimi
modelo está en su mejor momento j
antes de ser implementado en
producción. **Esta es la razón por
la implementación no debe se
paso final.**



Emoji icons Source: www.flaticon.com

Porque hay que monitorear y hacer cambios?

	Desafio de producción	Preguntas clave
1	Cambios en la distribución de datos	¿Por qué hay cambios repentinos en los valores de mis funciones?
2	Modelo de propiedad en producción	¿Quién es el propietario del modelo en producción? ¿El equipo de DevOps? ¿Ingenieros? ¿Científicos de datos?
3	Sesgo de entrenamiento-servicio	¿Por qué el modelo está dando malos resultados en producción a pesar de nuestras rigurosas pruebas e intentos de validación durante el desarrollo?
4	Desviación del modelo/concepto	¿Por qué mi modelo estaba funcionando bien en producción y de repente el rendimiento disminuyó con el tiempo?
5	Modelos de caja negra	¿Cómo puedo interpretar y explicar las predicciones de mi modelo de acuerdo con el objetivo comercial y las partes interesadas relevantes?
6	Adversarios concertados	¿Cómo puedo garantizar la seguridad de mi modelo? ¿Mi modelo está siendo atacado?
7	Preparación del modelo	¿Cómo compararé los resultados de las versiones más nuevas de mi modelo con las versiones en producción?
8	Problemas de salud de la tubería	¿Por qué falla mi canalización de entrenamiento cuando se ejecuta? ¿Por qué un trabajo de reciclaje tarda tanto en ejecutarse?
9	Sistema de bajo rendimiento	¿Por qué la latencia de mi servicio predictivo es muy alta? ¿Por qué obtengo latencias muy diferentes para mis diferentes modelos?
10	Casos de eventos extremos (Outliers)	¿Cómo podré seguir el efecto y el rendimiento de mi modelo en situaciones extremas y no planificadas?
11	Problemas de calidad de datos	¿Cómo puedo asegurarme de que los datos de producción se procesen de la misma manera que los datos de entrenamiento?

Para qué monitorear?

Esencialmente, el objetivo de monitorear sus modelos en producción es:

- Para detectar problemas con su modelo y el sistema que sirve su modelo en producción antes de que comiencen a generar valor comercial negativo,
- Para tomar medidas clasificando y solucionando problemas de modelos en producción o las entradas y los sistemas que los habilitan,
- Para garantizar que sus predicciones y resultados puedan ser explicados e informados,
- Para garantizar que el proceso de predicción del modelo sea transparente para las partes interesadas relevantes para una gobernanza adecuada,
- Finalmente, proporcionar un camino para mantener y mejorar el modelo en producción.

Su aplicación de aprendizaje automático no es solo el modelo, sino todo lo que habilita su modelo en producción, incluida la infraestructura, los datos de entrada, los recursos y otros servicios ascendentes y descendentes.

Qué monitorear?

Para responder a las preguntas anteriores, necesita algunos criterios de selección de métricas. **El éxito para una empresa podría significar un sistema completo en el que su modelo solo juega un papel pequeño.**

Para perfeccionar y ser específico con sus criterios de selección de métricas, puede seguir algunas de estas mejores prácticas (créditos a Lina Weichbrodt por esto):

- Elija una métrica comparable entre modelos,
- Simple y fácil de entender,
- Se puede recopilar en tiempo real,
- Permite alertas accionables sobre problemas.

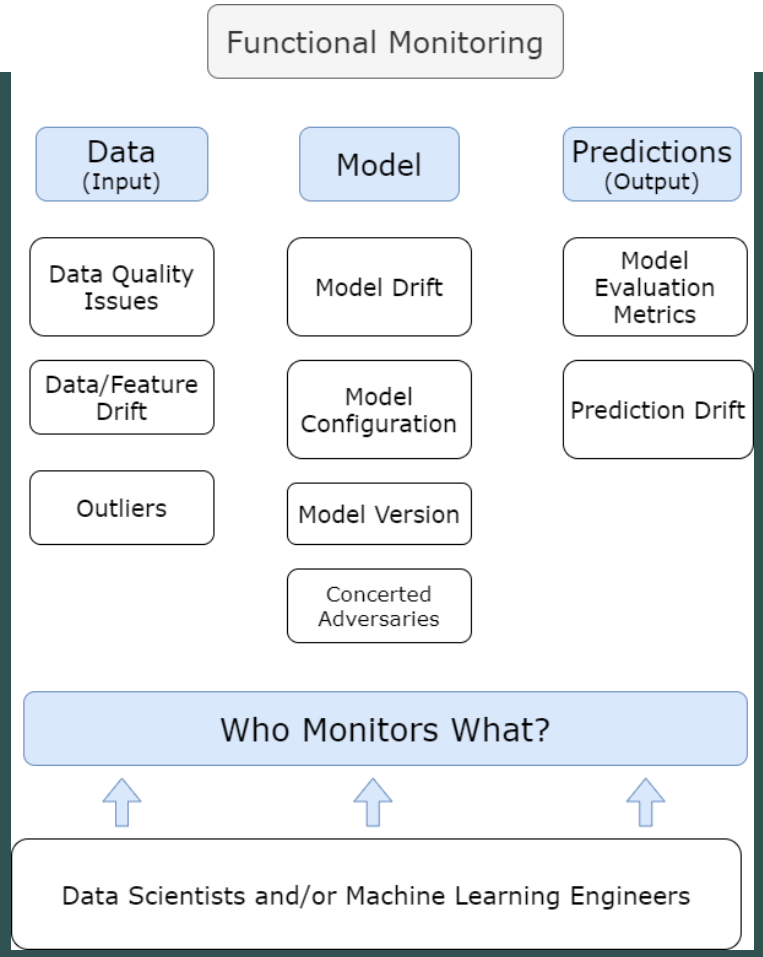
Para pensar en lo que significa el éxito para un negocio, también hay que pensar en lo que califica como una buena experiencia de usuario. Luego, **piense en cómo su modelo contribuye a esa buena experiencia de usuario en el contexto de todo el sistema; su modelo generalmente no es la solución principal para los problemas de UX** .

Qué cosas pueden salir mal tanto en producción como en desarrollo?

- **Monitoreo de nivel funcional** : monitoreo del rendimiento del modelo, entradas (datos) y salidas (predicciones).
- **Supervisión a nivel operativo** : supervisión a nivel de sistema y de recursos.

Aspectos a considerar.

1. Problemas de calidad de datos
    1. Preprocesamiento mal
    2. Cambios en requerimientos
    3. Corrupción o perdida de la fuente.
2. Desviación de datos/características
3. Valores atípicos



Problema 1 y soluciones.

Técnicas de detección de problemas de calidad de datos

En algunos otros casos, es posible que una canalización de datos no pueda ingerir datos de una fuente porque los datos no están disponibles, tal vez debido a cambios en una fuente de datos anterior o porque los datos no se están registrando. Puede haber casos en los que la fuente de datos ascendente esté dañada o le falten funciones. Es imperativo monitorear problemas como estos, ya que sin duda afectarán el rendimiento general de su sistema.

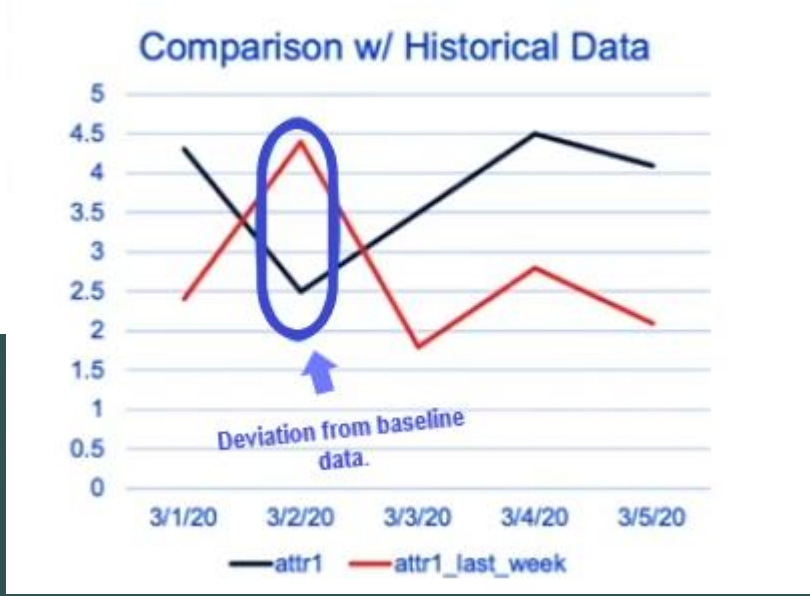
Escribir pruebas para detectar problemas de calidad de datos. Algunas verificaciones de calidad de datos incluyen:

- Prueba de datos de entrada para duplicados,
- Prueba de datos de entrada para valores faltantes,
- Detectar errores de sintaxis,
- Detectar errores de formato y tipo de datos,
- Comprobación del esquema en busca de errores semánticos en términos de nombres de características,
- Perfiles de datos efectivos para dependencias complejas en la canalización de datos,
- Comprobaciones generales de integridad; ¿Cumplen los datos los requisitos de los servicios finales o de los consumidores?

Posibles soluciones tras detectar problemas de calidad de datos

- Proporcione una alerta después de un cambio de esquema.
- Asegúrese de que los propietarios de los datos implementen prácticas adecuadas de validación de datos.
- Asegúrese de que todos sean conscientes de su función para llevar los datos a la canalización y habilite una comunicación eficaz entre los propietarios de datos para que, cuando se realice un cambio en la fuente de datos, los propietarios del modelo y otros propietarios de servicios estén al tanto.

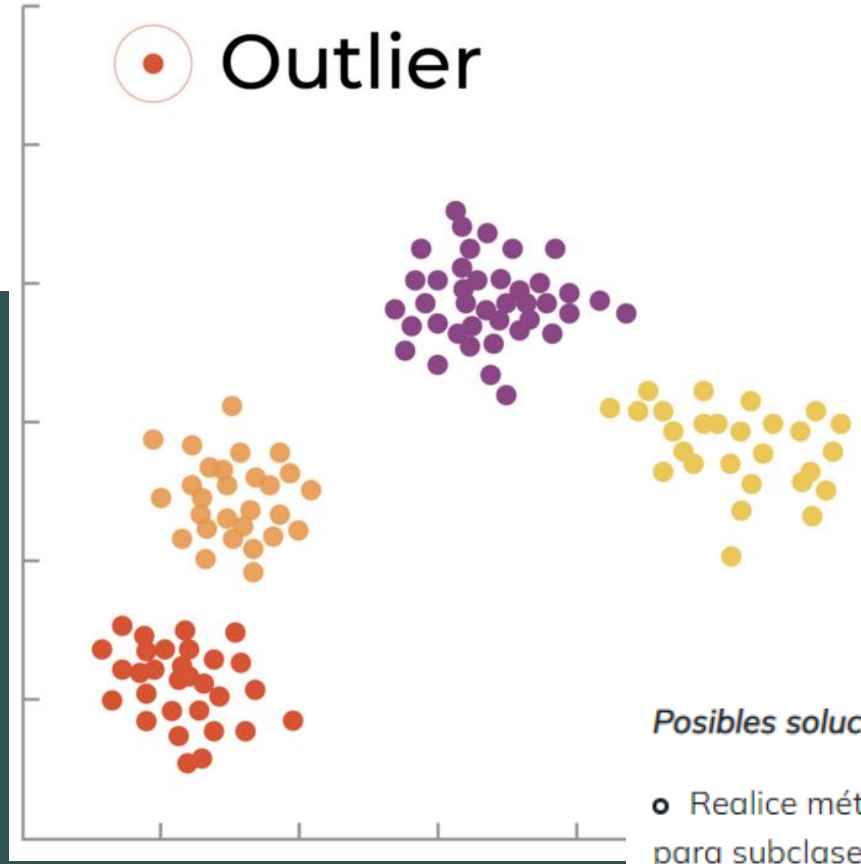
Problema 2 y soluciones.



Posibles soluciones tras la detección de Data Drift

- La solución más plausible es activar una alerta y enviar una notificación al propietario del servicio. Es posible que desee utilizar una herramienta de orquestación para iniciar un trabajo de capacitación con datos de producción y, si el cambio de distribución es realmente grande, es posible que desee crear otro modelo con sus datos nuevos.
- A menudo, sus nuevos datos no serán lo suficientemente grandes para volver a entrenar su modelo o remodelarlo. Por lo tanto, podría combinar y preparar sus nuevos datos con datos históricos (entrenamiento) y luego, durante el reentrenamiento, asignar pesos más altos a las características que se desviaron significativamente entre sí.

Problema 3 y soluciones.

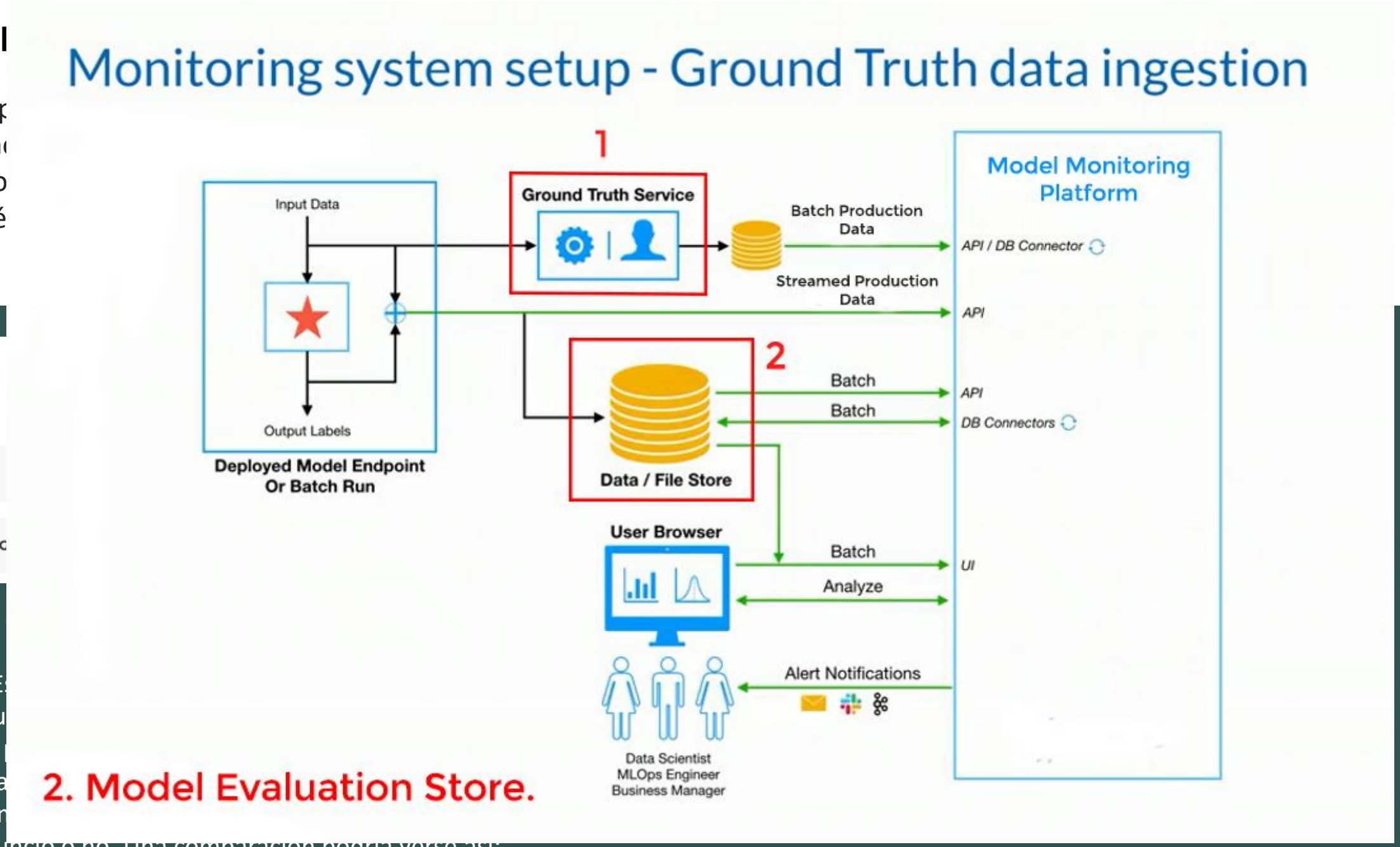


Posibles soluciones después de la detección de valores atípicos

- Realice métodos de segmentación de datos en subconjuntos de datos para verificar el rendimiento del modelo para subclases específicas de predicciones. Puede automatizar este proceso a medida que su modelo realiza y registra predicciones en un almacén de evaluación utilizando su herramienta de monitoreo.
- Si su modelo sigue teniendo un desempeño deficiente según sus métricas, es posible que desee considerar evaluar el modelo en su estado actual y luego entrenar un nuevo modelo retador.
- Documente el problema y rastree si se trata de un valor atípico estacional o un valor atípico extremo y único para que pueda elaborar una estrategia sobre cómo solucionar dichos problemas en el futuro.

P

Sup
sin
mo
mé



Un

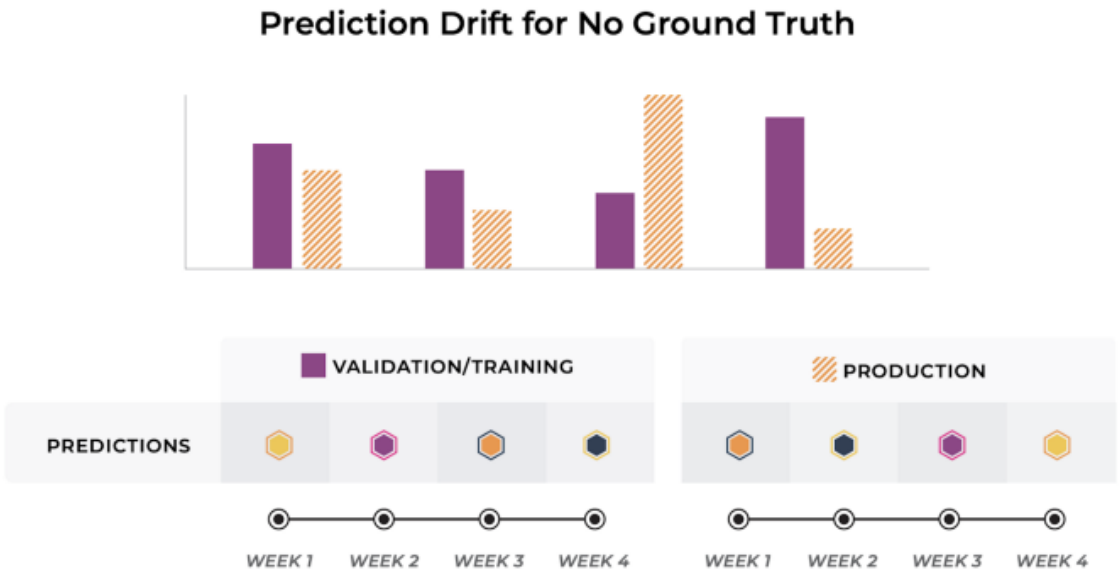
"¿E
Si u
las
una
tien
anuncio o no. Una comparación podría verse así:

Predicciones y correcciónes.

Modelos de puntuación cuando la realidad básica NO está disponible: desviación de la predicción

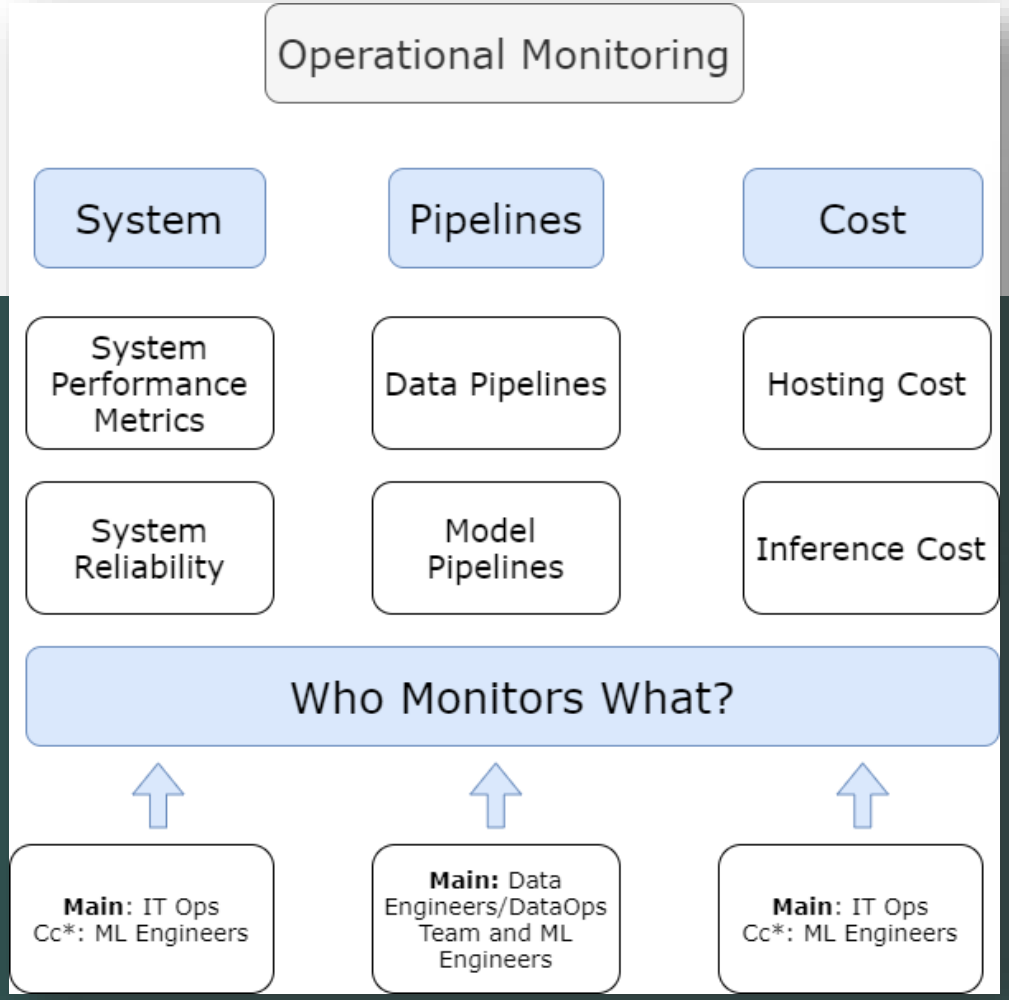
¿Qué pasa cuando la verdad del terreno no está disponible o está comprometida? Usamos la distribución de resultados de predicción como un indicador de rendimiento porque, con suerte, se ha establecido de acuerdo con el KPI empresarial.

Con suerte, su plataforma de monitoreo está configurada de tal manera que las predicciones del modelo también se registran en un almacén de evaluación del modelo. Un almacén de evaluación de modelos contiene la respuesta del modelo (una firma de las decisiones del modelo) a cada pieza de datos de entrada para cada versión del modelo, en cada entorno. De esta manera, podrá monitorear las predicciones del modelo a lo largo del tiempo y comparar la distribución usando métricas estadísticas como la distancia de Hellinger (HDDDM) , la divergencia de Kullback-Leibler y el índice de estabilidad de la población (PSI) .



Fuente

Monitoreo de operación.



Supervisar el rendimiento de su sistema/aplicación puede ayudarlo a responder preguntas como:

- ¿Esta aplicación cumple con los requisitos de tiempo de actividad?
- ¿Está atendiendo las solicitudes lo suficientemente rápido?
- ¿Está utilizando eficientemente los recursos y ahorrando costos?
- ¿Qué hay de los cambios en las dependencias del código, puede manejarlo?
- ¿Cumple con los requisitos de escalabilidad?
- ¿Cuáles son sus limitaciones de servicio?

- **Utilización de CPU/GPU** cuando el modelo calcula predicciones sobre los datos entrantes de cada llamada a la API; le dice cuánto consume su modelo por solicitud.
- **Utilización de memoria** para cuando el modelo almacena datos en caché o los datos de entrada se almacenan en caché en la memoria para un rendimiento de E/S más rápido.
- Número de **solicitudes fallidas** por un evento/operación.
- Número total de **llamadas a la API** .
- **Tiempo de respuesta** del servidor de modelos o servicio de predicción.

Buenas prácticas para técnicas de acción ante contingencias.

- **Concéntrese en las personas primero** . Si crea una cultura en la que los datos también se tratan como el producto en su organización, lo más probable es que las personas se inclinen a tomar posesión del producto para

Mejores prácticas para el monitoreo de modelos

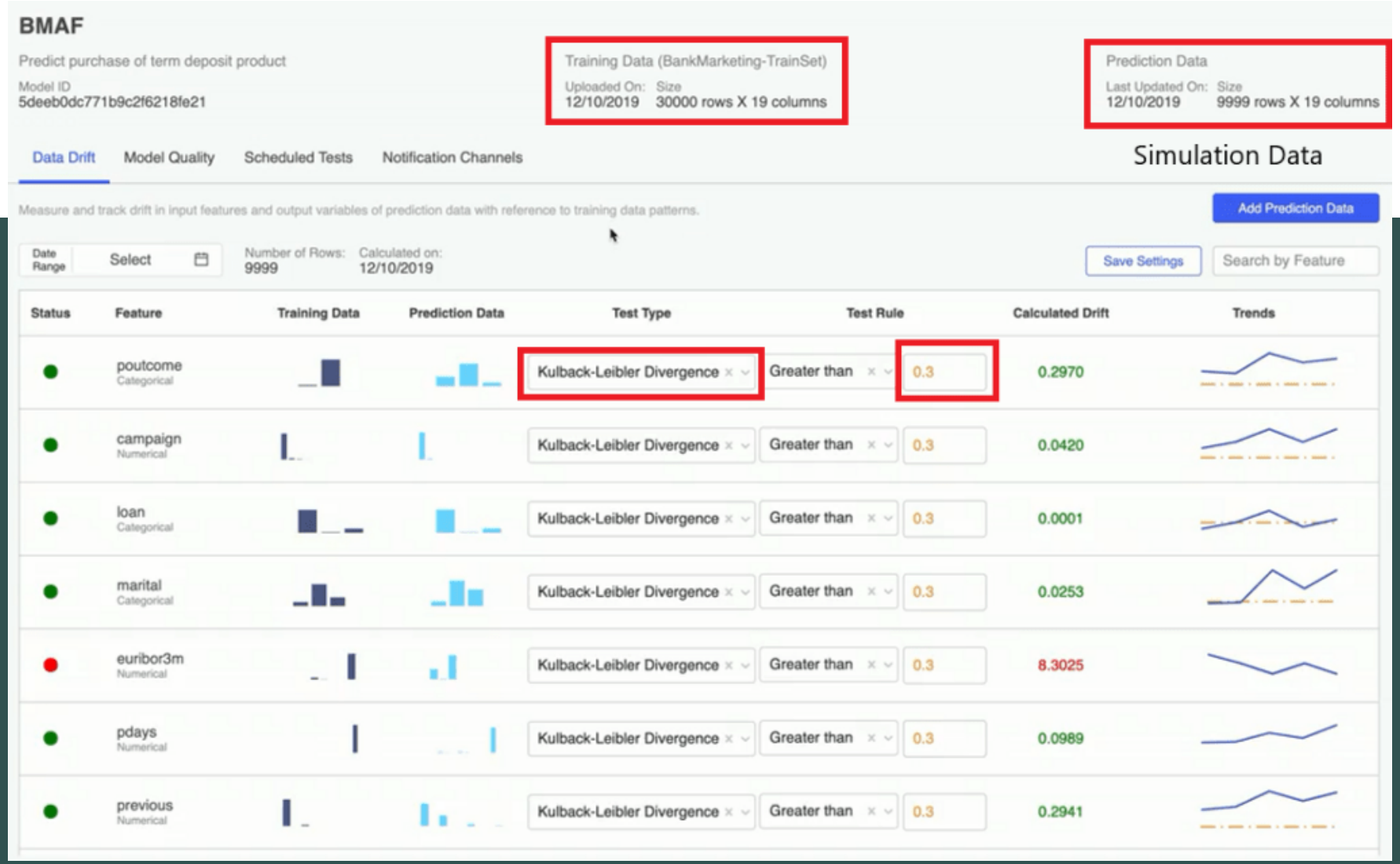
Mejores prácticas para monitorear predicciones/resultados

- La desviación de la predicción puede ser un buen indicador de rendimiento para las métricas del modelo, especialmente cuando no se puede recopilar información real, pero no debe usarse como la única métrica.
- Realice un seguimiento de los resultados irrazonables de su modelo. Por ejemplo, su modelo de clasificación que predice la clase incorrecta para un conjunto de entradas con una puntuación de confianza alta, o su modelo de regresión que predice una puntuación negativa (cuando la puntuación de la métrica base debe ser 0) para un conjunto determinado de características.

- Anime a su equipo a documentar adecuadamente su marco de solución de problemas y cree un marco para pasar de alertas a acciones y solución de problemas para un mantenimiento eficaz del modelo .

Software para el análisis de fatiga.

Nos envia alertas dependiendo del rendimiento.



Es como el software para evaluar resistencias a ataques o para evaluar capacidad de balance de carga.