دورة دمج واجهات برمجة النماذج اللغوية الكبيرة: البنية والاختبار والتشغيل

26 – 30 يوليو 2027

كيب تاون

دورة دمج واجهات برمجة النماذج اللغوية الكبيرة: البنية والاختبار والتشغيل

المرجع: 818_38303 **التاريخ:** 26 – 30 يوليو 2027 **المكان:** كيب تاون **الرسوم:** GBP 4800

ملخص البرنامج

دمج واجهات برمجة النماذج اللغوية الكبيرة محور دورة تدريبية تمتد أسبوع لقادة التقنية ومعماريي الحلول ومالكي المنتجات، ويخرج منها كل مشارك بخطة تصميم وتشغيل لدمج النموذج اللغوي في تطبيق واحد. تربط منظمات كثيرة خدمات النماذج اللغوية بأنظمة العملاء والمالية والخدمات أسرع مما تستطيع اختبارها وتأمينها وتمويلها. وينتقل البرنامج من فهم سلوك هذه الواجهات إلى تصميم تدفق البيانات وضوابط التهديدات والاختبار، ثم إلى التكلفة والمراقبة وترتيبات المورد التي تبقي الخدمة الحية موثوقة. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في دمج واجهات برمجة النماذج اللغوية الكبيرة لمجموعات من منظمات مختلفة.

المبررات المؤسسية

تضيف البنوك وشركات التأمين وتجار التجزئة والجهات العامة خدمات النماذج اللغوية إلى منتجات تتعامل مع سجلات العملاء وقراراتهم. وتحدد خيارات الواجهة المبكرة تكلفة الخدمة ومخاطرها وموثوقيتها سنوات طويلة. ومن يحسن مساءلة التصاميم وخطط الاختبار وشروط المورد يتجنب إعادة العمل المكلفة، ويمنع خروج البيانات من المنظمة بالخطأ.

- موثوقية التسليم: تتحسن حين يصمم التعامل مع الأعطال وحدود معدل الطلبات والبدائل قبل الإطلاق.
- التعرض الأمني: ينخفض حين تربط ضوابط المدخلات والمخرجات بفئات التهديد المعروفة.
- تكلفة التشغيل: تبقى متوقعة حين يقاس الاستخدام ويسقف ويراجع بالقيمة.

المبادئ والأساس المعرفي

- قائمة OWASP Top 10 for LLM Applications أبرز عشرة مخاطر لتطبيقات النماذج اللغوية: تسرد مخاطر مثل حقن التعليمات ومعالجة المخرجات غير الآمنة والصلاحيات الزائدة، وتطبق في الجلستين 3 و4 على ربط التهديدات بالضوابط.
- المعيار ISO/IEC 42001 نظام إدارة الذكاء الاصطناعي: يحدد نظام إدارة للذكاء الاصطناعي، ويطبق في الجلستين 1 و5 على المساءلة وضبط التغيير.
- المعيار ISO/IEC 27001 إدارة أمن المعلومات: يحدد إدارة أمن المعلومات، ويطبق في الجلسة 2 على تصنيف البيانات وحدود الوصول.

المشاركون المستهدفون

- قادة التقنية الذين يعتمدون دمج النماذج اللغوية ويتحملون مخاطر التسليم.
- معماريو الحلول الذين يصممون الواجهات وتدفقات البيانات والبدائل.
- مالكو المنتجات الذين يحددون ما يجوز للخدمة فعله وما لا يجوز.
- مديرو الأمن والموردين الذين يضعون الضوابط وشروط المورد.

تشمل البيئات المعتادة القطاع المصرفي والتأمين وتجارة التجزئة والخدمات العامة.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم تصميم واجهة من حيث تعرض البيانات وسلوك الأعطال.
2. سيكون المشاركون قادرين على بناء خريطة تدفق بيانات بتصنيف وحدود وصول.
3. سيكون المشاركون قادرين على تشخيص نقاط الضعف الأمنية في التعليمات والمخرجات والوصول إلى الأدوات.
4. سيكون المشاركون قادرين على تصميم خطة اختبار تقيس جودة الإجابات وتكشف التراجع.
5. سيكون المشاركون قادرين على ترتيب أولويات ضوابط التكلفة وحدود معدل الطلبات بحسب نمط الاستخدام.
6. سيكون المشاركون قادرين على تبرير تصميم الدمج وخطة التشغيل أمام الراعي.

هيكل البرنامج

اليوم 1: أسس دمج واجهات برمجة النماذج اللغوية الكبيرة

ماذا تفعل واجهة النموذج اللغوي، وأين يمكن أن تفشل؟

- ورقة تشريح الطلب والاستجابة
- فهرس أنماط الدمج
- شبكة قرار البناء أو الشراء أو الضبط
- جرد أنماط الإخفاق
- خريطة المساءلة وفق ISO/IEC 42001

اليوم 2: تدفقات البيانات وتصميم الواجهة

أي البيانات يجوز أن تغادر المنظمة، وعبر أي مسار؟

- جدول تصنيف البيانات
- مخطط تدفق البيانات
- مصفوفة ضبط الوصول وفق ISO/IEC 27001
- مراجعة موضع البوابة
- قواعد الاحتفاظ والتسجيل

اليوم 3: ضوابط التعليمات والمخرجات والتهديدات

كيف يمنع إساءة استخدام الخدمة والتلاعب بها؟

- بطاقات سيناريوهات حقن التعليمات
- قائمة فحص معالجة المخرجات
- مصفوفة ربط المخاطر بالضوابط وفق OWASP
- سجل صلاحيات الأدوات
- ورقة تصميم مرشح المحتوى

اليوم 4: الاختبار والتكلفة والتشغيل

كيف تبقى الخدمة دقيقة وميسورة التكلفة ومتاحة؟

- مجموعة اختبار جودة الإجابات
- خطة اختبار التراجع
- سياسة حدود معدل الطلبات وإعادة المحاولة
- نموذج تكلفة الطلب الواحد
- مراجعة مستوى خدمة المورد

اليوم 5: خطة تصميم وتشغيل دمج النموذج اللغوي لتطبيق واحد

هل تتكامل الأدوات السابقة في خطة يستطيع الراعي اعتمادها؟

- تطبيق مخطط تدفق البيانات من الجلسة 2
- اختبار مصفوفة ربط المخاطر بالضوابط من الجلسة 3
- فحص نموذج تكلفة الطلب الواحد من الجلسة 4
- التدرب على تحدي مراجعة التصميم
- إنجاز خطة تصميم الدمج وتشغيله

المنهجية

يقوم البرنامج على تحليل الحالات من مواد جاهزة لتطبيقين، أحدهما مساعد استفسارات العملاء في بنك والآخر خدمة تلخيص المستندات في جهة حكومية. يراجع المشاركون تصاميم الواجهات ونتائج الاختبار وشروط المورد، ويتحدى بعضهم خيارات بعض، ويدافعون عن خطتهم أمام زملاء يؤدون دور جهة اعتماد التصميم.

- نشاط مقترح: تتبع سجل عميل واحد عبر التصميم وتحديد مواضع تسربه المحتملة.
- نشاط مقترح: كتابة ثلاث حالات حقن تعليمات وتحديد الضابط الذي يوقف كلا منها.
- نشاط مقترح: حساب تكلفة شهر من الاستخدام ووضع سقف مع حد تنبيه.

المخرج الختامي

يعد كل مشارك خطة تصميم وتشغيل لدمج النموذج اللغوي في تطبيق واحد. وتضم الخطة خريطة تدفق البيانات ومصفوفة التهديدات والضوابط وخطة الاختبار وسياسة التكلفة وحدود معدل الطلبات ومراجعة المورد. وتستخدم في العمل لإحاطة الراعي ووضع شروط للمورد وتوجيه الإصدار الأول.

الأسئلة الشائعة

هل تناسب دورة تدريبية في دمج واجهات برمجة النماذج اللغوية الكبيرة القادة الذين لا يكتبون الشيفرة؟

نعم، إذ يدرس دمج واجهات برمجة النماذج اللغوية الكبيرة عبر تصاميم جاهزة وقوالب. ويفترض البرنامج مسؤولية عن توجيه البناء أو اعتماده، دون مهارات برمجة.

على أي معايير يقوم دمج واجهات برمجة النماذج اللغوية الكبيرة؟

يقوم دمج واجهات برمجة النماذج اللغوية الكبيرة على قائمة OWASP Top 10 for LLM Applications للتهديدات، والمعيار ISO/IEC 42001 لإدارة الذكاء الاصطناعي، والمعيار ISO/IEC 27001 لأمن المعلومات.

كيف تستخدم خطة دمج واجهات برمجة النماذج اللغوية الكبيرة في العمل؟

تستخدم خطة تصميم الدمج وتشغيله لإحاطة الراعي، ووضع شروط المورد، والاتفاق على حدود الاختبار والتكلفة، وتوجيه الإصدار الأول.

بماذا يختلف دمج واجهات برمجة النماذج اللغوية الكبيرة عن برنامج في حوكمة الذكاء الاصطناعي؟

يركز دمج واجهات برمجة النماذج اللغوية الكبيرة على الواجهات وتدفقات البيانات والاختبار وتشغيل تطبيق واحد، بينما يركز برنامج حوكمة الذكاء الاصطناعي على السياسات والجرد والرقابة عبر أنظمة كثيرة.