JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة معمارية أنظمة الذكاء الاصطناعي وحوكمتها

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة معمارية أنظمة الذكاء الاصطناعي وحوكمتها

معمارية أنظمة الذكاء الاصطناعي وحوكمتها دورة تدريبية مدتها أسبوع لمعماريي المؤسسات ومالكي منصات الذكاء الاصطناعي وقادة تقنية المعلومات ومديري المخاطر التقنية، يخرج منها المشاركون بمعمارية مرجعية وخريطة ضوابط لنظام إنتاجي واحد. ومع انتقال نماذج تعلم الآلة من بيئات التجربة إلى المنصات الأساسية، أصبح ترابط خطوط البيانات ومخازن الخصائص ونقاط خدمة النماذج هو ما يحدد أمان تعديل كل نموذج وتدقيقه. تقدم جوبيتر برايم للتدريب دورة معمارية أنظمة الذكاء الاصطناعي وحوكمتها.

لماذا تهم معمارية أنظمة الذكاء الاصطناعي وحوكمتها الآن

ثلاث قوى ترفع أهمية معمارية أنظمة الذكاء الاصطناعي وحوكمتها: تحول محافظ النماذج من تجارب محدودة إلى عشرات نقاط الخدمة الإنتاجية، وفرق أمن تواجه مسارات هجوم جديدة مثل حقن الأوامر وتسميم البيانات، ومدققون يطلبون أدلة على الضوابط في كل مرحلة من دورة حياة النموذج. المؤسسة التي تبني الضوابط داخل منصتها تستطيع إعادة تدريب النماذج والتراجع عنها وتفسيرها بسرعة، أما التي تضيفها لاحقا فترث تكاملات هشة ونقاطا عمياء. تستند الدورة إلى معيار ISO/IEC 42001 لنظم إدارة الذكاء الاصطناعي، وإلى إطار إدارة مخاطر الذكاء الاصطناعي NIST AI RMF.

المستفيدون من معمارية أنظمة الذكاء الاصطناعي وحوكمتها

- المسؤولون عن التصاميم المستهدفة لمنصات البيانات وطبقات التكامل واستضافة النماذج
- القادة المساءلون عن ميزانيات منصات الذكاء الاصطناعي واختيار الموردين ومستويات الخدمة
- المهندسون الذين يشغلون خطوط عمليات تعلم الآلة وسجلات النماذج وأتمتة النشر
- المختصون بتقييم التهديدات السيبرانية للنماذج ومجموعات التدريب ونقاط الاستدلال
- فرق المخاطر والتأكيد التي تختبر عمل ضوابط الذكاء الاصطناعي كما صممت

تستفيد الوظيفة التقنية المركزية أكثر عندما يحضر أعضاؤها من المعمارية وهندسة المنصات ومخاطر التقنية معا ويتفقون على مجموعة واحدة من نقاط الضبط.

قدرات معمارية أنظمة الذكاء الاصطناعي وحوكمتها

يتدرب المشاركون على قراءة منصة الذكاء الاصطناعي بوصفها طبقات من المكونات، وعلى وضع ضابط ومالك ودليل على كل طبقة.

- تصميم معمارية مرجعية متعددة الطبقات لتدريب النماذج وخدمتها ومراقبتها — مجالس مراجعة المعمارية
- تحديد متطلبات تتبع أصل البيانات ومخزن الخصائص وسجل النماذج — مالكو المنصات
- بناء بوابات إصدار لعمليات تعلم الآلة تتضمن الاعتماد والاختبار والتراجع — قادة الهندسة
- تقييم التهديدات على النماذج ونقاط الاستدلال بنمذجة تهديدات منظمة — مسؤولو الأمن
- مواءمة ضوابط دورة الحياة مع بنود ISO/IEC 42001 ووظائف NIST AI RMF — المدققون الداخليون
- حساب عتبات المراقبة للانحراف وزمن الاستجابة والتكلفة — مالكو الخدمات والشركاء الماليون

مصطلحات معمارية أنظمة الذكاء الاصطناعي وحوكمتها الأساسية

- المعمارية المرجعية — مخطط قابل لإعادة الاستخدام يبين المكونات والواجهات ونقاط الضبط المعيارية لبناء أنظمة الذكاء الاصطناعي في المؤسسة.
- سجل النماذج — فهرس بإصدارات النماذج المدربة وأصلها واعتماداتها وحالة نشرها.
- عمليات تعلم الآلة — ممارسات وأتمتة تنقل النماذج بموثوقية من التجربة إلى الإنتاج وتحافظ عليها.
- مخزن الخصائص — خدمة مشتركة تخزن متغيرات مدخلات النماذج وتوثقها وتقدمها بشكل متسق للتدريب والاستدلال.
- انحراف النموذج — تراجع تدريجي في دقة النموذج مع تغير بيانات المدخلات الحية أو العلاقات الواقعية.
- خريطة الضوابط — مصفوفة تربط كل مرحلة من دورة الحياة بضوابطها ومالكيها وأدلتها لأغراض التأكيد.

معمارية أنظمة الذكاء الاصطناعي وحوكمتها يوما بيوم

اليوم 1: مشهد المنصات ومراحل دورة الحياة

- نموذج مراحل دورة حياة الذكاء الاصطناعي — مواضع نشوء المخاطر من القرارات المعمارية
- جرد المنصات بوضعها الحالي — الخطوط المكررة والنماذج غير المعلنة
- مقارنة البناء أو الشراء أو الخدمة المدارة — استراتيجية استضافة النماذج
- مبادئ المعمارية لأحمال الذكاء الاصطناعي — قابلية النقل والتتبع والتكلفة
- نطاق نظام الإدارة وفق ISO/IEC 42001 — حدود منظومة الذكاء الاصطناعي

اليوم 2: خطوط البيانات وطبقات هندسة الخصائص

- أنماط خطوط الاستيعاب والتحويل — الاختيار بين الدفعات والتدفق المستمر
- تتبع أصل البيانات ومصدرها — مسار تدقيق مجموعات التدريب
- تصميم مخزن الخصائص — الاتساق بين التدريب والاستدلال
- قواعد جودة البيانات وعقودها — قبول التغذيات الواردة أو رفضها
- تقنيات حماية الخصوصية — الإخفاء وتقليل البيانات داخل الخطوط

اليوم 3: خدمة النماذج وعمليات تعلم الآلة والأمن

- سجل النماذج وإدارة الإصدارات — الاعتماد قبل الترقية إلى الإنتاج
- بوابات الإصدار في التكامل والنشر المستمرين للنماذج — الاختبار والاعتماد والتراجع
- أنماط الخدمة بالدفعات والزمن الحقيقي والحافة — موازنة زمن الاستجابة والتكلفة
- نمذجة التهديدات لنقاط خدمة الذكاء الاصطناعي — التسميم والتهرب وحقن الأوامر
- التحكم في الوصول وإدارة الأسرار — حماية مكونات النماذج

اليوم 4: المراقبة والتأكيد والمساءلة

- لوحات الانحراف وزمن الاستجابة والتكلفة — عتبات إعادة التدريب
- وظائف NIST AI RMF للحوكمة والرسم والقياس والإدارة — ملكية الضوابط
- بطاقات النماذج وتوثيق الأنظمة — أدلة للمدققين
- الاستجابة لحوادث إخفاق النماذج — التصعيد ومفاتيح الإيقاف
- العناية الواجبة بالنماذج وواجهات البرمجة من أطراف خارجية — تأكيد الموردين

اليوم 5: ممارسة المعمارية المرجعية وخريطة الضوابط

- نموذج مراحل دورة الحياة من اليوم 1 — تحديد نطاق نظام إنتاجي واحد
- طبقات الخطوط والخصائص من اليوم 2 — نقاط فحص أصل البيانات
- بوابات الإصدار ونموذج التهديدات من اليوم 3 — الضوابط الأمنية
- عتبات المراقبة من اليوم 4 — جدول أدلة التأكيد
- المعمارية المرجعية للذكاء الاصطناعي وخريطة الضوابط — حزمة تصميم جاهزة لمجلس الإدارة

تطبيق معمارية أنظمة الذكاء الاصطناعي وحوكمتها بعد الدورة

- مطابقة نموذج حي واحد، مثل خدمة تقييم الائتمان أو توقع الطلب، مع نموذج مراحل دورة الحياة وتسجيل الثغرات في تتبع الأصل أو بوابات الإصدار.
- إدارة جلسة نمذجة تهديدات لروبوت محادثة يخدم العملاء أو نقطة استدلال وإضافة الإجراءات المتفق عليها إلى قائمة أعمال المنصة.

أسئلة حول معمارية أنظمة الذكاء الاصطناعي وحوكمتها

ما معمارية أنظمة الذكاء الاصطناعي وحوكمتها ولماذا تهم الآن؟

معمارية أنظمة الذكاء الاصطناعي وحوكمتها هي تصميم المنصات بحيث يحمل كل خط بيانات ونموذج ونقطة خدمة ضوابط ومالكين واضحين. وتهم الآن لأن أعداد النماذج تتزايد بسرعة، والمدققون وفرق الأمن ينتظرون أدلة قابلة للتتبع عبر دورة الحياة.

من المستفيد من تدريب معمارية أنظمة الذكاء الاصطناعي وحوكمتها؟

يستفيد معماريو المؤسسات ومالكو منصات الذكاء الاصطناعي ومهندسو عمليات تعلم الآلة ومديرو مخاطر التقنية. ويرى كل منهم كيف تصنع قرارات التصميم في الخطوط والسجلات وطبقات الخدمة ثغرات ضبط أو تزيلها قبل أن يضطر غيرهم إلى معالجتها.

كيف تختلف معمارية أنظمة الذكاء الاصطناعي وحوكمتها عن دورة في سياسات الذكاء الاصطناعي أو أخلاقياته؟

تعمل الدورة على مستوى المنصة والمكونات لا على مستوى السياسات. تصمم السجلات وبوابات الإصدار وعتبات المراقبة ونماذج التهديدات وتربط الضوابط بها، بدلا من صياغة المبادئ أو مواثيق اللجان.

ماذا تعود به من تدريب معمارية أنظمة الذكاء الاصطناعي وحوكمتها؟

تعود بمعمارية مرجعية للذكاء الاصطناعي وخريطة ضوابط لنظام إنتاجي واحد، تبين المكونات وتدفقات البيانات ونقاط الضبط والمالكين والأدلة، وتكون جاهزة للعرض على مجلس مراجعة المعمارية أو لجنة التدقيق.

معمارية أنظمة الذكاء الاصطناعي وحوكمتها: الطريق إلى الأمام

تدعم المعمارية المرجعية للذكاء الاصطناعي وخريطة الضوابط أول قرار في المنصة: أي ثغرات الضبط تغلق قبل الإصدار التالي للنموذج. يستخدمها المعماريون ومالكو المنصات والمدققون سجلا مشتركا للتصميم. وبعد أول إصدار يمر عبر البوابات الجديدة، تستحق عتبات الانحراف وفحوص النماذج الخارجية مراجعة جديدة، لأن الحركة الحية وتحديثات الموردين تكشف نقاط ضعف لم يتوقعها التصميم.