JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية

24 – 28 أكتوبر 2027

القاهرة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية

المرجع: 1051_39631 **التاريخ:** 24 – 28 أكتوبر 2027 **المكان:** القاهرة **الرسوم:** GBP 4000

مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية دورة تدريبية مدتها أسبوع لقادة المخاطر والامتثال والإشراف على الذكاء الاصطناعي، يعد فيها المشاركون ملف ضمان موردي الذكاء الاصطناعي. فمعظم المؤسسات اليوم تشغل نماذج لم تبنها بنفسها، لكنها تبقى مسؤولة عن نتائجها أمام العملاء ومجالس الإدارة. وتقدم جوبيتر برايم للتدريب مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية بوصفها ممارسة لإثبات أن الذكاء الاصطناعي المشترى خاضع للضوابط.

لماذا تهم مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية الآن

يلتقي ضغطان عند حدود العلاقة مع المورد. فالمزودون يضيفون خصائص توليدية وتنبؤية إلى منتجات متعاقد عليها أصلا، دون تقييم جديد للمخاطر في كثير من الأحيان. ومجالس الإدارة ولجان التدقيق تطلب جردا يبين كل نموذج خارجي ومالكه ودرجة تعرضه. والمؤسسة التي تضبط مورديها تستطيع التبديل أو الإيقاف بثقة، أما غيرها فترث إخفاقات لا تستطيع تفسيرها. وتستند الدورة إلى معيار ISO/IEC 42001 لنظام إدارة الذكاء الاصطناعي، وإلى إطار NIST AI RMF لإدارة مخاطر الذكاء الاصطناعي.

المستفيدون من مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية

- المختصون الذين يحدثون سجل مخاطر الذكاء الاصطناعي ويقررون معالجة النماذج الخارجية
- المختصون الذين يطابقون ضوابط الموردين مع السياسات الداخلية وبنود نظام الإدارة
- المسؤولون عن استبيانات التأهيل والعناية الواجبة لموردي البرمجيات والبيانات
- المدققون الذين يختبرون كفاية أدلة المزودين لدعم الضمان المعلن
- المستشارون الذين يعدون أوراق لجان الإشراف حول الذكاء الاصطناعي المضمن والمسند خارجيا

تستفيد المؤسسة أكثر حين يحضر معا موظفو المشتريات والشؤون القانونية وأمن المعلومات والمخاطر، لأن كلا منهم يملك جزءا من البنود والاختبارات وشروط الخروج.

قدرات مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية

ينتقل المشاركون من الثقة بادعاءات المورد إلى امتلاك أدلة قابلة للاختبار عن كل نموذج خارجي.

- بناء جرد للنماذج الخارجية والمضمنة بالمالك والغرض والفئة — لجان الإشراف
- تقييم ردود الموردين حول بيانات التدريب والتقييم وسجل الحوادث — قرارات التأهيل
- صياغة بنود تعاقدية لإشعار تغيير النموذج وحقوق التدقيق واستخدام البيانات — الشؤون القانونية والمشتريات
- اختبار أدلة المورد مثل بطاقات النماذج وتقارير التقييم من حيث الكفاية — التدقيق الداخلي
- مواءمة ضوابط الموردين مع ISO/IEC 42001 ووظائف NIST AI RMF — قادة الامتثال
- تصميم مؤشرات المراقبة وخطط الخروج لموردي الفئة العليا — مالكو المخاطر

مصطلحات مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية الأساسية

- نموذج الطرف الثالث — نموذج ذكاء اصطناعي يبنيه أو يدربه أو يستضيفه مزود خارجي وتستخدمه المؤسسة في عملياتها.
- خاصية الذكاء الاصطناعي المضمنة — قدرة ذكاء اصطناعي تضاف إلى برمجيات مشتراة، غالبا دون قرار شراء منفصل.
- تصنيف المخاطر إلى فئات — ترتيب الموردين في مستويات تدقيق بحسب أثرهم في الأفراد والعمليات والسمعة.
- أدلة الضمان — وثائق ونتائج اختبارات وإقرارات يقدمها المورد لإثبات أن ضوابطه تعمل فعلا.
- إشعار تغيير النموذج — واجب تعاقدي يلزم المزود بتنبيه المشتري قبل إعادة تدريب النموذج أو استبداله.
- تعرض التركز — الاعتماد على نموذج أساسي واحد أو مزود واحد في خدمات عديدة في الوقت نفسه.

مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية يوما بيوم

اليوم 1: مشهد الذكاء الاصطناعي الخارجي

- خريطة سلسلة توريد مزودي النماذج الأساسية والمنصات والتطبيقات — موقع المساءلة
- اكتشاف خصائص الذكاء الاصطناعي المضمنة في الاشتراكات القائمة — قرارات التعرض الخفي
- حقول جرد النماذج الخارجية وملكيتها — خيارات الرؤية لدى اللجان
- بنود علاقات الموردين في ISO/IEC 42001 — قرارات نطاق نظام الإدارة
- اعتبارات الأطراف الثالثة في NIST AI RMF — تحديد أولويات الإشراف

اليوم 2: التصنيف والعناية الواجبة

- مصفوفة تصنيف المخاطر بحسب الأثر — عمق التدقيق لكل مورد
- تصميم استبيان العناية الواجبة للذكاء الاصطناعي — معايير قبول التأهيل
- فحص مصدر بيانات التدريب وتراخيصها — التعرض في الملكية الفكرية
- مراجعة تقارير التقييم واختبارات التحيز — قبول ادعاءات أداء المورد
- أسئلة الأمن وموقع البيانات للنماذج المستضافة — خيارات حماية المعلومات

اليوم 3: العقود ومطابقة الضوابط

- بنود إشعار تغيير النموذج وإعادة التدريب — استقرار النتائج
- شروط حقوق التدقيق والإقرارات وتسليم الأدلة — قرارات الوصول إلى الضمان
- مطابقة ضوابط المورد مع سياسة الذكاء الاصطناعي الداخلية — خيارات معالجة الفجوات
- المسؤولية والإبلاغ عن الحوادث وتعويضات الخدمة — توزيع كلفة إخفاق النماذج
- خطط الخروج وقابلية النقل واستبدال النموذج — الجاهزية للتبديل

اليوم 4: المراقبة المستمرة والإشراف

- مؤشرات المخاطر الرئيسية للنماذج الخارجية — حدود التصعيد للمالكين
- أخذ عينات المخرجات وفحص الانجراف في نماذج المورد — قرارات استمرار الاستخدام
- تحليل تعرض التركز عبر المزودين — المرونة والتنويع
- فرز حوادث المورد والاستجابة المشتركة — خيارات الاحتواء
- حزمة تقارير لجنة الإشراف — رسائل الضمان لمجلس الإدارة

اليوم 5: تطبيق ملف ضمان موردي الذكاء الاصطناعي

- تصنيف حالة مورد فعلية من القطاع البنكي — تطبيق مصفوفة اليوم 2
- تنقيح عقد ذكاء اصطناعي في الرعاية الصحية — تطبيق بنود اليوم 3
- اختبار أدلة المورد مقابل الضوابط المطابقة — حكم الكفاية للتدقيق الداخلي
- استعراض خطة المراقبة بالمؤشرات — تطبيق حدود اليوم 4
- استكمال ملف ضمان موردي الذكاء الاصطناعي — الجاهزية لاعتماد اللجنة

تطبيق مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية بعد الدورة

- إجراء مسح لخصائص الذكاء الاصطناعي المضمنة في اشتراكات البرمجيات وتصنيف كل اكتشاف في جرد النماذج الخارجية.
- إرسال استبيان العناية الواجبة المعاد تصميمه إلى موردين من الفئة العليا واختبار أدلتهما.

أسئلة حول مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية

ما مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية، ولماذا تهم الآن؟

هي ممارسة ضبط نماذج الذكاء الاصطناعي التي تشتريها مؤسستك بدلا من بنائها. وتهم الآن لأن الموردين يضيفون خصائص الذكاء الاصطناعي بسرعة، بينما تبقى أنت مسؤولا عن النتائج.

من الأدوار الأكثر استفادة من تدريب مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية؟

يستفيد أكثر قادة المخاطر والامتثال والإشراف على الذكاء الاصطناعي. كما يستفيد موظفو المشتريات والشؤون القانونية والأمن والتدقيق الداخلي.

كيف تختلف مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية عن دورة عامة في الإشراف على الذكاء الاصطناعي؟

تركز على حدود العلاقة مع المورد. فالدورة العامة تتناول السياسات والنماذج الداخلية بصورة واسعة، أما هذه فتتعمق في التصنيف والعناية الواجبة والعقود والأدلة الخاصة بالنماذج الخارجية.

ماذا تعود به من تدريب مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية؟

تعود بملف مكتمل لمورد فعلي واحد لنموذج خارجي. ويضم فئة المخاطر والضوابط المطابقة وملاحظات البنود وخطة المراقبة.

مخاطر موردي الذكاء الاصطناعي وضمان النماذج الخارجية: الطريق إلى الأمام

يمنح ملف ضمان موردي الذكاء الاصطناعي لجنة الإشراف مكانا واحدا للحكم على نموذج خارجي. وأول استخدام له هو تقرير بقاء مورد من الفئة العليا أو تعديل شروطه أو خروجه، وهو قرار يتخذه مالكو المخاطر والمشتريات والتدقيق الداخلي معا. وبعد هذا القرار الأول تستحق مصفوفة التصنيف المراجعة، لأن خصائص الموردين تتغير أسرع من العقود.