JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي

25 يوليو – 5 أغسطس 2027

كوالالمبور

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي

المرجع: 14_361 **التاريخ:** 25 يوليو – 5 أغسطس 2027 **المكان:** كوالالمبور **الرسوم:** GBP 8500

حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي دورة تدريبية متقدمة مدتها أسبوعين لقادة حوكمة البيانات ومسؤولي الخصوصية ومالكي البيانات ومديري مخاطر الذكاء الاصطناعي، يخرج منها المشاركون بإطار حوكمة بيانات الذكاء الاصطناعي يغطي مجموعات البيانات التي تقف خلف نماذجهم. فكل نموذج يرث جودة بيانات تدريبه وحالة الموافقة عليها وتحيزاتها، لذلك تظهر ضوابط البيانات الضعيفة اليوم في صورة تنبؤات معيبة وانتهاكات للخصوصية. وتقدم جوبيتر برايم للتدريب هذه الدورة في حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي لأمناء تلك البيانات.

لماذا تهم حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي الآن

تشكل ثلاث قوى واقع حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي اليوم: نماذج تدرب على مجموعات بيانات ضخمة متعددة المصادر يغيب عنها غالبا مصدر واضح، وتوقعات حماية البيانات التي امتدت إلى الاستدلال ومخرجات النماذج، وأصحاب البيانات والمدققون الذين يسألون كيف استخدمت سجلاتهم الشخصية في تدريب نظام ما. المؤسسة التي تحسن التعامل معها تتتبع كل مجموعة تدريب وتبرر مشروعية استخدامها وتثبت جودتها، أما من يسيء التعامل معها فيعيد تدريب نماذجه على بيانات ملوثة أو يواجه شكاوى لا يملك ردا عليها. وتأتي الأمثلة من السجلات الصحية ومعاملات الخدمات المالية. وتستند الدورة إلى ISO/IEC 42001 لأنظمة إدارة الذكاء الاصطناعي وإلى إطار NIST لإدارة مخاطر الذكاء الاصطناعي AI RMF.

المستفيدون من حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي

- قادة حوكمة البيانات الذين يحددون الملكية والإشراف والسياسات لمجموعات بيانات المؤسسة
- مسؤولو الخصوصية المسؤولون عن الأساس النظامي للمعالجة وسجلات الموافقة وتقييمات الأثر
- مالكو البيانات وأمناؤها المساءلون عن جودة مجالاتهم ومسار بياناتها وصلاحيات الوصول إليها
- مديرو مخاطر الذكاء الاصطناعي وبرامجه الذين يعتمدون مجموعات البيانات للتدريب والإطلاق
- مديرو أمن المعلومات الذين يحمون مسارات البيانات ومخازن الخصائص ومكونات النماذج

تتحقق الفائدة الكبرى حين يحضر مكتب الخصوصية ومكتب حوكمة البيانات ومالكو منتجات الذكاء الاصطناعي في مؤسسة واحدة معا، ويتفقون على ضوابط مشتركة لمجموعات البيانات.

قدرات حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي

يتعلم المشاركون التعامل مع كل مجموعة بيانات للتدريب أو الاستدلال بوصفها أصلا محكوما له مالك وغرض مشروع وملف جودة وتاريخ قابل للتتبع.

- تصميم نموذج تشغيلي لحوكمة البيانات يحدد ملكية بيانات تدريب الذكاء الاصطناعي — رئيس البيانات
- تقييم أدلة جودة البيانات ومسارها ومصدرها قبل تدريب النماذج — مجالس اعتماد مجموعات البيانات
- تطبيق الخصوصية بالتصميم وإخفاء الهوية والبيانات الاصطناعية على بيانات الذكاء الاصطناعي — مسؤولو الخصوصية
- حساب احتمال إعادة التعرف على الأفراد والتحيز في مجموعات البيانات المرشحة — مراجعو مخاطر النماذج
- تحديد ضوابط أمن مسارات بيانات الذكاء الاصطناعي ومخازن الخصائص — قادة أمن المعلومات
- بناء إطار حوكمة بيانات يضم السياسات والأدوار ونقاط الفحص — اللجنة التنفيذية للبيانات

مصطلحات حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي الأساسية

- مسار البيانات — سجل يبين منشأ البيانات وطريقة تحويلها والأنظمة والنماذج التي استهلكتها.
- مصدر البيانات — دليل موثق على منبع مجموعة البيانات وطريقة جمعها والحقوق المرتبطة باستخدامها في الذكاء الاصطناعي.
- الخصوصية بالتصميم — إدماج ضمانات حماية البيانات في أنظمة الذكاء الاصطناعي منذ أول قرار تصميمي لا بعد الإطلاق.
- الترميز المستعار — استبدال المعرفات المباشرة برموز بحيث لا يمكن ربط السجل بشخص دون مفتاح منفصل.
- تقييم أثر حماية البيانات DPIA — تقييم منظم لمخاطر الخصوصية الناشئة عن نشاط معالجة مع تدابير التخفيف.
- البيانات الاصطناعية — سجلات مولدة تحاكي الخصائص الإحصائية للبيانات الحقيقية دون نسخ أفراد فعليين.

حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي يوما بيوم

اليوم 1: الضغوط على البيانات خلف الذكاء الاصطناعي

- رسم سلسلة إمداد بيانات الذكاء الاصطناعي — المصادر والوسطاء والأنظمة الداخلية
- توقعات حماية البيانات في تدريب النماذج — الغرض والتناسب
- إخفاقات النزاهة في النماذج المنشورة — بيانات ملوثة أو متقادمة أو خاطئة الوسم
- خريطة أصحاب المصلحة لمجموعات البيانات — أصحاب البيانات والجهات الرقابية والمدققون
- التقييم الذاتي لنضج البيانات — خط أساس لجاهزية الذكاء الاصطناعي

اليوم 2: النماذج التشغيلية لحوكمة البيانات

- نماذج الحوكمة المركزية والموزعة والهجينة — خيارات حقوق القرار
- أدوار المالك والأمين والحافظ — المساءلة عن بيانات التدريب
- ميثاق مجلس حوكمة البيانات — صلاحيات التصعيد والاعتماد
- هرمية سياسات البيانات ومعاييرها — قواعد ملزمة لاستخدام الذكاء الاصطناعي
- مسرد الأعمال وفهرس البيانات الوصفية — معنى مشترك بين الفرق

اليوم 3: جودة البيانات ومسارها

- أبعاد جودة البيانات — أهداف الدقة والاكتمال والحداثة والاتساق
- تحليل خصائص البيانات وقواعد التحقق — بوابة قبل تدريب النماذج
- الالتقاط الآلي لمسار البيانات — تتبع الخصائص حتى الأنظمة المصدر
- بطاقات أداء جودة البيانات — أولويات المعالجة لمالكي البيانات
- مواءمة البيانات الرئيسية والمرجعية — كيانات متسقة عبر النماذج

اليوم 4: مصدر بيانات التدريب وحقوق استخدامها

- صحائف توثيق مجموعات البيانات — المنشأ والتكوين والحدود
- تراخيص بيانات الأطراف الخارجية وحقوق استخدامها — قرارات الاقتناء
- مخاطر البيانات المجمعة من الويب والبيانات المفتوحة — حقوق النشر والموافقة
- سلاسل توريد الوسم — جودة التعليقات التوضيحية وظروف العاملين
- إدارة نسخ مجموعات البيانات وقواعد الاحتفاظ — إمكانية إعادة إنتاج التدريب

اليوم 5: الخصوصية بالتصميم في الذكاء الاصطناعي

- تقليل البيانات في اختيار الخصائص — اختبارات ضرورة السمات
- تقييد الغرض والاستخدام الثانوي — إعادة استخدام السجلات في التدريب
- تقنيات تعزيز الخصوصية — التعلم الموحد والخصوصية التفاضلية
- مخاطر عكس النموذج واستنتاج العضوية — ضوابط خصوصية المخرجات
- متطلبات الخصوصية في مواصفات تصميم الأنظمة — اعتماد الهندسة

اليوم 6: إخفاء الهوية والبيانات الاصطناعية

- إخفاء الهوية مقابل الترميز المستعار — الوضع النظامي للبيانات المحولة
- أساليب إخفاء الهوية الجماعي وتنويع القيم الحساسة والتعميم — اختبار إعادة التعرف
- أساليب توليد البيانات الاصطناعية — موازنة الدقة والخصوصية
- اختبار منفعة البيانات منزوعة الهوية — أثرها في دقة النماذج
- مصفوفة قرار إتاحة مجموعات البيانات — داخلية أو للشركاء أو عامة

اليوم 7: الموافقة والأساس النظامي وتقييمات أثر حماية البيانات

- اختيار الأساس النظامي لمعالجة الذكاء الاصطناعي — الموافقة أو العقد أو المصلحة المشروعة
- سجلات الموافقة ومعالجة سحبها — الأثر في النماذج المدربة
- منهجية تقييم أثر حماية البيانات لأنظمة الذكاء الاصطناعي — تقدير المخاطر وخطط التخفيف
- طلبات حقوق أصحاب البيانات — الوصول والمحو وطلبات التفسير
- نقل البيانات عبر الحدود لتدريب النماذج — خيارات ضمانات النقل

اليوم 8: التحيز والتمثيل في مجموعات البيانات

- تحيز العينة وفجوات التغطية — اختبار التمثيل
- تحيز الوسم والتمييز التاريخي — مراجعة الحقيقة المرجعية
- المتغيرات البديلة للخصائص المحمية — قرارات استبعاد الخصائص
- إعادة التوازن وإعادة الترجيح والزيادة — خيارات تصحيح البيانات
- توثيق التحيز في بطاقات النماذج — الإفصاح للمراجعين

اليوم 9: أمن مسارات الذكاء الاصطناعي ونزاهتها

- تهديدات تسميم البيانات والمدخلات العدائية — نماذج تهديد المسارات
- التحكم في الوصول والتشفير لمخازن الخصائص — تصميم الحد الأدنى من الصلاحيات
- فحوص النزاهة بالتجزئة ومجموعات البيانات الموقعة — كشف العبث
- ضوابط البيانات في ISO/IEC 42001 — أدلة نظام إدارة الذكاء الاصطناعي
- وظيفتا التحديد والقياس في NIST AI RMF — مدخلات سجل مخاطر البيانات

اليوم 10: تطبيق إطار حوكمة بيانات الذكاء الاصطناعي

- النموذج التشغيلي وتوزيع الأدوار — تطبيق نموذج الحوكمة المختار
- قائمة فحص اعتماد مجموعات البيانات — بوابات الجودة والمصدر والأساس النظامي
- مكتبة ضوابط الخصوصية والتحيز — ربط الأساليب بمستويات المخاطر
- مقاييس المراقبة وتصميم مسار التدقيق — التأكيد المستمر
- إطار حوكمة بيانات الذكاء الاصطناعي — العرض على اللجنة التنفيذية للبيانات

تطبيق حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي بعد الدورة

- إعداد صحيفة توثيق وتتبع مسار لمجموعة بيانات تغذي نموذجا قائما، ورفع فجوات المصدر أو الأساس النظامي إلى مالك البيانات
- إجراء تقييم أثر حماية البيانات لحالة استخدام مخططة، يشمل اختبار إعادة التعرف على مستخلص بيانات التدريب المقترح

أسئلة حول حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي

ما حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي ولماذا تهم الآن؟

حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي هي ضبط من يملك البيانات التي تدرب أنظمة الذكاء الاصطناعي وتغذيها ومن يحق له استخدامها وكيف تحمى. وتهم الآن لأن النماذج تضخم أي خلل أو تحيز أو استخدام غير مشروع مخفي في بياناتها.

من الأكثر استفادة من تدريب حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي؟

قادة حوكمة البيانات ومسؤولو الخصوصية ومالكو البيانات ومديرو مخاطر الذكاء الاصطناعي هم الأكثر استفادة. فهم يعتمدون مجموعات البيانات ويجيبون عن طلبات أصحابها ويثبتون مشروعية استخدامها، ويحتاجون إلى أساليب مشتركة لاختبار الجودة والمصدر والخصوصية.

بم يختلف تدريب حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي المتقدم عن دورة حوكمة الذكاء الاصطناعي؟

يركز هذا التدريب على مجموعات البيانات لا على إشراف مجلس الإدارة على الذكاء الاصطناعي ككل. ستعمل على مسار البيانات ومصدرها وإخفاء الهوية والموافقة واختبار التحيز، بعمق يناسب متخصصين يديرون وظائف البيانات أو الخصوصية.

ماذا تعود به من تدريب حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي؟

تعود بإطار حوكمة بيانات الذكاء الاصطناعي. يحدد الإطار النموذج التشغيلي وبوابات اعتماد مجموعات البيانات وضوابط الخصوصية والتحيز وتدابير أمن المسارات ومقاييس المراقبة التي يمكن للجنتك التنفيذية للبيانات اعتمادها.

حوكمة البيانات والخصوصية والنزاهة في الذكاء الاصطناعي: الطريق إلى الأمام

يحدد إطار حوكمة بيانات الذكاء الاصطناعي أولا مجموعات البيانات المسموح بدخولها إلى تدريب النماذج وشروط ذلك. وتستخدمه لجان البيانات ومسؤولو الخصوصية ومالكو منتجات الذكاء الاصطناعي لاعتماد مجموعات البيانات أو رفضها أو معالجتها. وبعد أول دورة اعتماد تستحق نتائج المصدر وإعادة التعرف مراجعة جديدة، لأن مصادر البيانات الخارجية الجديدة تكشف غالبا فجوات لم تتوقعها الضوابط الأولى.