JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه

2 – 6 مايو 2027

كوالالمبور

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه

المرجع: 57361_1559 **التاريخ:** 2 – 6 مايو 2027 **المكان:** كوالالمبور **الرسوم:** GBP 4900

اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه دورة تدريبية مدتها أسبوع لمديري التقنية وقادة حوكمة تقنية المعلومات ومسؤولي المخاطر الذين يحتاجون إلى رصد أدوات الذكاء الاصطناعي غير المعتمدة في المؤسسة، واستبدال الحظر المطلق بخطة اكتشاف الذكاء الاصطناعي الخفي وتمكينه. فالموظفون يلصقون اليوم العقود والشيفرات وسجلات العملاء في روبوتات المحادثة العامة وإضافات المتصفح أسرع مما تستطيع المشتريات مراجعته. تقدم جوبيتر برايم للتدريب هذه الدورة للقادة الذين يحولون الاستخدام الخفي إلى إنتاجية آمنة ومرئية.

لماذا يهم اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه الآن

تدفع ثلاث قوى انتشار الذكاء الاصطناعي غير المعتمد: موظفون يبحثون عن صياغة وبرمجة وتلخيص أسرع مما تتيحه الأنظمة المعتمدة، وموردو برمجيات يفعلون ميزات توليدية داخل أدوات مرخصة أصلا، وعملاء ومدققون يسألون أين ذهبت المعلومات السرية. المؤسسة التي تكشف هذا الاستخدام وتقدم بدائل معتمدة تكسب الإنتاجية وتحافظ على حدود بياناتها، أما التي تكتفي بالمنع فتدفع الاستخدام إلى مزيد من الخفاء. وتبني الدورة ضوابطها على معيار نظام إدارة الذكاء الاصطناعي ISO/IEC 42001 وإطار إدارة مخاطر الذكاء الاصطناعي NIST AI RMF، وتحولهما إلى قرارات اكتشاف وسياسات ودليل أدوات.

المستفيدون من اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه

- قادة التقنية الذين يقررون خدمات الذكاء الاصطناعي التي ترخصها المؤسسة وتدعمها
- قادة حوكمة تقنية المعلومات الذين يحتفظون بقوائم التطبيقات وموافقات التغيير
- مسؤولو المخاطر وأمن المعلومات المسؤولون عن تصنيف البيانات وضوابط التسرب
- مختصو حماية البيانات الذين يقيمون البيانات الشخصية المتجهة إلى النماذج الخارجية
- سفراء التحول الرقمي في وحدات الأعمال الذين ينقلون ما يحتاجه الموظفون فعلا

تستفيد المؤسسات أكثر حين يحضر ممثلو التقنية والأمن والأعمال معا، لأن سياسة الاستخدام المقبول ودليل الأدوات المعتمدة لا ينجحان إلا إذا عكسا الرغبة في المخاطرة والطلب الحقيقي للموظفين في آن واحد.

قدرات اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه

يغادر المشاركون قادرين على رؤية الاستخدام الخفي والحكم عليه بإنصاف وتوجيهه إلى مسارات معتمدة.

- تطبيق قياسات الشبكة والخدمات السحابية والمتصفح لرصد خدمات الذكاء الاصطناعي غير المعتمدة — لمالكي قوائم الأصول
- تقييم حالات الاستخدام الخفي حسب حساسية البيانات وقيمة الأعمال وشروط المورد — للجان المخاطر
- تصميم سياسة استخدام مقبول بقواعد بيانات حمراء وصفراء وخضراء واضحة — للموظفين والمديرين المباشرين
- تحديد ضوابط منع تسرب البيانات وتصفية المطالبات — لعمليات الأمن
- بناء دليل أدوات معتمدة بمسارات طلب ومراجعة — للمشتريات ومكاتب خدمة تقنية المعلومات
- صياغة رسالة عفو وتمكين تجعل الاستخدام الخفي مرئيا — للموظفين وممثليهم

مصطلحات اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه الأساسية

- الذكاء الاصطناعي الخفي — استخدام الموظفين أدوات أو نماذج أو ميزات ذكاء اصطناعي دون موافقة الجهات المسؤولة عنها أو علمها.
- سياسة الاستخدام المقبول — قواعد تحدد الأدوات التي يجوز للموظفين استخدامها، ومع أي بيانات، وبأي شروط.
- منع تسرب البيانات — ضوابط تفحص المحتوى الخارج من المؤسسة وتمنع المعلومات الحساسة أو تنبه إليها.
- دليل الأدوات المعتمدة — قائمة منشورة بخدمات الذكاء الاصطناعي الموافق عليها مع الاستخدامات المسموحة وحدود البيانات وخطوات الطلب.
- وسيط أمان الوصول السحابي — نقطة ضبط تراقب استخدام الموظفين للتطبيقات السحابية وتحكمه، بما فيها خدمات الذكاء الاصطناعي.
- عفو الذكاء الاصطناعي — دعوة محددة المدة للموظفين للإفصاح عن الأدوات التي يستخدمونها دون عقوبة حتى تقيم مخاطرها.

اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه يوما بيوم

اليوم 1: لماذا ينتشر الاستخدام الخفي

- دوافع الذكاء الاصطناعي الخفي — فجوات الإنتاجية وراء الأدوات غير المعتمدة
- الميزات التوليدية المدمجة في البرمجيات المرخصة — التوسع الصامت
- سيناريوهات التهديد — تسرب البيانات والملكية الفكرية وحقن المطالبات
- نطاق ISO/IEC 42001 وأدواره — موقع الاستخدام الخفي منه
- مقارنات حالات قطاعية — مكاتب المحاماة والمصانع

اليوم 2: أساليب الاكتشاف

- قياسات الشبكة ونظام أسماء النطاقات — رصد الحركة نحو خدمات الذكاء الاصطناعي
- تقارير وسيط أمان الوصول السحابي — تقدير حجم استخدام التطبيقات السحابية
- قوائم إضافات المتصفح والأجهزة الطرفية — كشف التعرض عبر الإضافات
- استبيانات الموظفين وحملات العفو — إظهار الاستخدام المعلن ذاتيا
- تصميم سجل الاستخدام الخفي — تدوين الأدوات والمستخدمين وأنواع البيانات

اليوم 3: التقييم والسياسة

- ربط تصنيف البيانات — قواعد المطالبات الحمراء والصفراء والخضراء
- شروط الموردين وبنود تدريب النماذج — الحكم على الاحتفاظ وإعادة الاستخدام
- وظيفتا الرسم والقياس في NIST AI RMF — تقييم كل حالة استخدام
- صياغة سياسة الاستخدام المقبول — قواعد واضحة يتبعها الموظفون
- مسارات الاستثناء والتصعيد — معالجة الحالات الحدية بسرعة

اليوم 4: الضوابط والتمكين

- منع تسرب البيانات وتصفية المطالبات — حجب رفع المحتوى الحساس
- بوابات الذكاء الاصطناعي المؤسسية والنسخ الخاصة — بدائل أكثر أمانا من الأدوات العامة
- هيكل دليل الأدوات المعتمدة — خطوات الطلب والمراجعة والتجديد
- دمج التراخيص ووضوح التكلفة — إنهاء الاشتراكات المكررة
- رسائل التوعية وشبكات السفراء — تغيير السلوك دون تخويف

اليوم 5: ممارسة خطة اكتشاف الذكاء الاصطناعي الخفي وتمكينه

- خط الأساس للاكتشاف في المؤسسة محل الدراسة — تطبيق أساليب اليوم 2
- درجات المخاطر وبنود السياسة — تطبيق تقييم اليوم 3
- خيارات الضوابط والدليل — تطبيق بدائل التمكين من اليوم 4
- مقاييس الرصد ودورة المراجعة — إبقاء السجل محدثا
- خطة اكتشاف الذكاء الاصطناعي الخفي وتمكينه — الخطة النهائية لاعتماد القيادة

تطبيق اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه بعد الدورة

- إجراء مسح للقياسات والاستبيانات مدته أسبوعان لبناء أول سجل للاستخدام الخفي بالأدوات والمستخدمين وأنواع البيانات.
- نشر مسودة دليل أدوات معتمدة تضم ثلاث خدمات ومسار طلب، ثم جمع الملاحظات من السفراء.

أسئلة حول اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه

ما اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه ولماذا يهم الآن؟

هو رصد الاستخدام غير المعتمد للذكاء الاصطناعي وتوجيهه إلى خيارات آمنة ومعتمدة. ويهم الآن لأن الموظفين يتبنون الأدوات العامة أسرع من المراجعات، فتتعرض البيانات السرية للخطر بينما نادرا ما يغير الحظر وحده السلوك.

من يستفيد أكثر من اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه؟

يستفيد أكثر قادة التقنية وقادة حوكمة تقنية المعلومات ومسؤولو المخاطر والأمن ومختصو حماية البيانات وسفراء التحول الرقمي. فكل منهم يرى جزءا مختلفا من الاستخدام الخفي، والمنهج المشترك ينتج سجلا أدق وسياسة أعدل.

كيف يختلف اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه عن دورة سياسة استخدام الذكاء الاصطناعي التوليدي؟

يتجاوز كتابة القواعد. ترصد فيه الاستخدام الفعلي عبر القياسات والعفو، وتقيم كل حالة، وتطلق بدائل معتمدة، بينما تركز دورة السياسة على صياغة المبادئ وبيانات الأخلاقيات ونصوص الاستخدام المسموح.

ماذا تعود به من دورة اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه؟

تعود بخطة مرحلية تضم أساليب الاكتشاف وتصميم السجل وبنود السياسة والضوابط التقنية ودليل الأدوات المعتمدة. وتمنح القيادة مسارا عمليا من تعرض مجهول إلى استخدام منتج ومنضبط.

اكتشاف الذكاء الاصطناعي الخفي وتمكين استخدامه: الطريق إلى الأمام

تحدد خطة اكتشاف الذكاء الاصطناعي الخفي وتمكينه أولا أي الأدوات غير المعتمدة تحجب أو يسمح بها مؤقتا أو تستبدل بخدمات معتمدة. يستخدمها قادة التقنية لترتيب أولويات الترخيص، ومسؤولو الأمن لضبط الضوابط، والسفراء لتوجيه زملائهم. وبعد أول مراجعة ربع سنوية للسجل يستحق الدليل مراجعة جديدة، فالميزات المدمجة الجديدة وطلبات الموظفين تغير الطلب بسرعة.