JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

# دورة بناء وكلاء الذكاء الاصطناعي واختبارهم

31 يناير – 4 فبراير 2027

القاهرة

info@jupiterprime.uk

**jupiterprime.uk**

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

# دورة بناء وكلاء الذكاء الاصطناعي واختبارهم

**المرجع:** 59_1481 **التاريخ:** 31 يناير – 4 فبراير 2027 **المكان:** القاهرة **الرسوم:** GBP 4000

بناء وكلاء الذكاء الاصطناعي واختبارهم دورة تدريبية مدتها أسبوع لمحللي الأعمال وقادة الأتمتة ومهنيي التحول الرقمي وتقنية المعلومات، ويخرج كل مشارك منها بحزمة النموذج الأولي للوكيل: وكيل يعمل ومجموعة اختباره وتصميم ضوابطه. فالوكلاء الذين يخططون الخطوات ويستدعون أنظمة الأعمال وينجزون المهام دون تدخل ينتقلون من العروض التجريبية إلى العمليات الفعلية. وتقدم هذه الدورة في بناء وكلاء الذكاء الاصطناعي جوبيتر برايم للتدريب.

## لماذا يهم بناء وكلاء الذكاء الاصطناعي الآن

تشكل قوتان بناء الوكلاء اليوم. فالنماذج اللغوية الكبيرة باتت قادرة على استدعاء واجهات البرمجة والاستعلام من قواعد البيانات وتعبئة النماذج، ولذلك تتيح المنصات منخفضة الشيفرة للمحللين تجميع الوكلاء دون فرق هندسية كبيرة. وفي المقابل تقلق وظائف الأمن والمخاطر من وكلاء يتصرفون بناء على معلومات خاطئة أو يسربون البيانات أو ينفذون تعليمات مدسوسة. والفرق التي تبني وكلاء بنطاق واضح وأدوات مختبرة وضوابط محكمة تؤتمت أعمالا متعددة الخطوات مثل فرز المطالبات أو تسجيل الموردين، أما التي تتجاوز التصميم والتقييم فتطلق وكلاء هشين يضعفون الثقة. وتستخدم الدورة إطار NIST AI Risk Management Framework لإدارة مخاطر الذكاء الاصطناعي NIST AI RMF ومعيار ISO/IEC 42001 لنظام إدارة الذكاء الاصطناعي لتأطير ضوابط مخاطر الوكلاء.

## المستفيدون من بناء وكلاء الذكاء الاصطناعي

- المحللون الذين يرسمون عمليات الأعمال ويحددون مواضع تدخل الوكيل
- مختصو الأتمتة الذين يشغلون أدوات أتمتة العمليات الروبوتية أو سير العمل
- ممارسو التحول الرقمي الذين يحولون حالات الاستخدام إلى نماذج أولية عاملة
- مهنيو تقنية المعلومات الذين يربطون الوكلاء بواجهات البرمجة والهوية ومخازن البيانات
- ممارسو الجودة والمخاطر الذين يختبرون سلوك الوكيل قبل إطلاقه

ويحقق مركز التميز في الأتمتة أكبر فائدة عندما يحضر المحللون ومختصو التكامل والمختبرون معا ويبنون وكيلا واحدا من البداية إلى النهاية.

## قدرات بناء وكلاء الذكاء الاصطناعي

يتدرب المشاركون على كل مرحلة من دورة بناء الوكيل، من تحديد نطاق المهمة حتى إثبات سلوكه الآمن تحت الاختبار.

- تحديد هدف الوكيل ونطاقه وأدواته وشروط توقفه — مالكو العمليات
- تصميم بنية المخطط والمنفذ أو الحلقة الواحدة لمهمة متعددة الخطوات — مهندسو الحلول
- بناء استدعاءات أدوات لأنظمة الأعمال بمخططات مدخلات ومخرجات واضحة — فرق التكامل
- تطبيق الذاكرة والاسترجاع ليستخدم الوكيل معرفة حديثة معتمدة — مالكو المحتوى
- اختبار سلوك الوكيل بمجموعة تقييم وأوامر عدائية — مراجعو المخاطر والجودة
- عرض نتائج النموذج الأولي وشروط الإطلاق — لجان توجيه الأتمتة

## مصطلحات بناء وكلاء الذكاء الاصطناعي الأساسية

- وكيل الذكاء الاصطناعي — برنامج يستخدم نموذجا لغويا لتخطيط الخطوات واستدعاء الأدوات والسعي إلى هدف بإشراف محدود.
- استدعاء الأدوات — قدرة النموذج على طلب وظيفة محددة مثل استعلام قاعدة بيانات أو إجراء عبر واجهة برمجة بمدخلات منظمة.
- ذاكرة الوكيل — سياق مخزن يقرؤه الوكيل بين الخطوات أو الجلسات، مثل سجل المحادثة أو المستندات المسترجعة.
- الضابط الوقائي — قاعدة أو فحص يمنع إجراء الوكيل أو يعدله أو يصعده إذا خرج عن الحدود المعتمدة.
- حقن الأوامر — تعليمات مخفية في محتوى يقرؤه الوكيل تحاول تغيير سلوكه أو استخراج البيانات.
- مجموعة التقييم — مجموعة ثابتة من المهام بنتائج متوقعة تقيس دقة الوكيل وسلامته قبل الإطلاق.

## بناء وكلاء الذكاء الاصطناعي يوما بيوم

### اليوم 1: من روبوتات المحادثة إلى الوكلاء

- الوكيل مقابل روبوت المحادثة مقابل أتمتة العمليات الروبوتية — اختيار نوع الأتمتة المناسب
- لوحة تفكيك المهام — تقسيم العملية إلى خطوات للوكيل
- أمثلة من مطالبات التأمين والمشتريات — مواضع ملاءمة الوكلاء
- نطاق الوكيل وشروط توقفه — تقييد الاستقلالية بأمان
- جولة في منصات الوكلاء منخفضة الشيفرة — اختيار بيئة البناء

## اليوم 2: البنى والأدوات

- نمطا الحلقة الواحدة والمخطط والمنفذ — مواءمة البنية مع المهمة
- تعريفات الأدوات ومخططات الوظائف — استدعاءات موثوقة للأنظمة
- موصلات واجهات البرمجة والمصادقة — أدنى صلاحيات ممكنة للوكلاء
- التسليم بين الوكلاء المتعددين — متى يتعاون الوكلاء المتخصصون
- تصميم أمر النظام للوكلاء — الدور والقواعد وصيغة المخرجات

## اليوم 3: الذاكرة والمعرفة والضوابط

- ذاكرة الوكيل قصيرة المدى وطويلة المدى — ما يحفظ وما ينسى
- الاسترجاع من قواعد المعرفة المعتمدة — تأسيس إجابات الوكيل
- ضوابط المدخلات والمخرجات — منع الإجراءات غير الآمنة أو الخارجة عن النطاق
- خطوات الموافقة البشرية — التصعيد قبل الإجراءات غير القابلة للتراجع
- دفاعات حقن الأوامر — تنقية المحتوى غير الموثوق

## اليوم 4: الاختبار وجاهزية الإطلاق

- بناء مجموعة التقييم — مهام عادية وحدية وعدائية
- تسجيل المسار وفحص الخطوات — تتبع أخطاء قرارات الوكيل
- مقاييس الدقة والتكلفة وزمن الاستجابة — عتبات إطلاق الوكلاء
- وظيفة القياس في NIST AI RMF — توثيق أدلة اختبار الوكيل
- خطة مراقبة الوكلاء العاملين — الانحراف والإخفاقات والتراجع

## اليوم 5: ممارسة حزمة النموذج الأولي للوكيل

- جولة بناء مكثفة على حالة استخدام مختارة — تطبيق البنية والأدوات
- تمرين الفريق الأحمر — اختبار الضوابط أمام محاولات الحقن
- تشغيل التقييم ومراجعة الدرجات — تقرير الجاهزية
- عرض الأقران — شرح سلوك الوكيل لمالكي العمليات
- حزمة النموذج الأولي للوكيل — الوكيل النهائي واختباراته وتصميم ضوابطه

## تطبيق بناء وكلاء الذكاء الاصطناعي بعد الدورة

- إعادة بناء النموذج الأولي على عملية داخلية واحدة وتشغيل مجموعة التقييم بحالات حقيقية.
- عرض سجلات المسار ونتائج الضوابط على لجنة توجيه الأتمتة للاتفاق على شروط الإطلاق.

## أسئلة حول بناء وكلاء الذكاء الاصطناعي

### ماذا يفعل مختص بناء وكلاء الذكاء الاصطناعي ولماذا يهم ذلك الآن؟

يصمم مختص بناء وكلاء الذكاء الاصطناعي الوكلاء ويربطهم ويختبرهم لينجزوا مهام متعددة الخطوات. ويهم ذلك الآن لأن المنصات منخفضة الشيفرة جعلت تجميع الوكلاء سهلا، والمؤسسات تحتاج من يجعلهم موثوقين وآمنين.

### من الأدوار الأكثر استفادة من دورة بناء وكلاء الذكاء الاصطناعي؟

يستفيد محللو الأعمال وقادة الأتمتة وممارسو التحول الرقمي ومختصو التكامل أكثر من غيرهم. ويستفيد مختبرو الجودة والمخاطر أيضا، خاصة حين يرسل مركز التميز مجموعة متنوعة.

### كيف تختلف دورة بناء وكلاء الذكاء الاصطناعي عن دورة استراتيجية في الذكاء الاصطناعي الوكيلي؟

هي دورة تطبيقية يبني فيها المشاركون وكيلا ويربطونه ويختبرونه. فالدورة الاستراتيجية تتناول نماذج التشغيل وحالات الأعمال للقادة، أما دورة بناء وكلاء الذكاء الاصطناعي فتركز على البنية واستدعاء الأدوات والضوابط والتقييم.

### ماذا تعود به من دورة بناء وكلاء الذكاء الاصطناعي؟

تعود بحزمة نموذج أولي عاملة. تضم الحزمة إعدادات الوكيل وتعريفات الأدوات وتصميم الضوابط ومجموعة التقييم بدرجاتها وتوصية قصيرة بشأن الإطلاق.

### بناء وكلاء الذكاء الاصطناعي: الطريق إلى الأمام

توجه حزمة النموذج الأولي للوكيل أولا قرار جاهزية عملية مختارة لتجربة وكيل في بيئة محكومة. ويستخدمها المحللون ومختصو التكامل ومراجعو المخاطر للاتفاق على الأدوات والصلاحيات وعتبات الإطلاق. وبعد أول تشغيل فعلي تستحق مجموعة التقييم وقواعد الضوابط مراجعة جديدة، إذ تكشف الطلبات الحقيقية حالات حدية لم يتوقعها أي اختبار سابق في بيئة التطوير.