

إدارة مخاطر الذكاء الاصطناعي والامتثال: تدقيق الأنظمة الذكية عبر دورة الحياة

23 – 27 أغسطس 2027

ميونخ

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

إدارة مخاطر الذكاء الاصطناعي والامتثال: تدقيق الأنظمة الذكية عبر دورة الحياة

المرجع: 51_86379 **التاريخ:** 23 – 27 أغسطس 2027 **المكان:** ميونخ **الرسوم:** 5700 Euro

نظرة عامة

تواجه المنظمات التي تعتمد على التقنيات المؤتمتة تحديات تشغيلية ترتبط بموثوقية النماذج والتحيز الخوارزمي وسلسلة نسب البيانات والأمن التشغيلي. تركز هذه الدورة على ترسيخ منهجيات إدارة مخاطر الذكاء الاصطناعي والامتثال عبر مختلف مراحل تطوير الأنظمة وتشغيلها، وتتيح للمشاركين تقييم البنية التحتية الحاسوبية وفحص سلامة بيانات التدريب وإجراء تدقيق الأنظمة الذكية والتحقق من آليات الرقابة البشرية. يستعرض البرنامج مسارات التدقيق الفني ومؤشرات المخاطر وضوابط الحوكمة لضمان شفافية القرارات المؤتمتة ومساءلتها ومرونتها التشغيلية. تقدم هذه الدورة بواسطة أجايل للتدريب.

الفئة المستهدفة

- مدراء أمن المعلومات ومدراء إدارة المخاطر المؤسسية المعنيون بتقييم أنظمة اتخاذ القرار المؤتمتة.
- المدققون الداخليون والخارجيون المسؤولون عن فحص حوكمة الخوارزميات وتدفقات معالجة البيانات.
- مسؤولو الامتثال والخبراء القانونيون المعنيون بمتابعة متطلبات الشفافية والمعايير النظامية.
- مهندسو الأنظمة ومعمارية تعلم الآلة المنفذون لأطر الضوابط الفنية.
- أعضاء لجان الحوكمة المشرفون على الاستخدام الأخلاقي والسلامة التشغيلية لأنظمة الذكاء الاصطناعي.

الإدارات والقطاعات المستهدفة

يخدم هذا البرنامج الكوادر الفنية والرقابية في القطاعات التي تعتمد على مسارات عمل مؤتمتة لاتخاذ القرارات.

- إدارات أمن المعلومات وإدارة المخاطر في الخدمات المصرفية والمالية
- إدارات الامتثال والتدقيق الداخلي في الرعاية الصحية وعلوم الحياة
- فرق علوم البيانات وهندسة البرمجيات في الاتصالات وتقنية المعلومات
- إدارات الجودة والسلامة التشغيلية في التصنيع والروبوتات المستقلة
- لجان الحوكمة المؤسسية والجهات الرقابية التقنية في القطاع العام

أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- إجراء مراجعات فنية منظمة لتدقيق الأنظمة الذكية خلال كامل مراحل تشغيلها.
- تطبيق ضوابط تشغيلية تتوافق مع الأطر الدولية لإدارة مخاطر الذكاء الاصطناعي.
- تنفيذ عمليات تدقيق خوارزمية لاكتشاف التحيز وانجراف البيانات وضعف القابلية للتفسير في مخرجات النماذج.
- تقييم العتاد الحاسوبي ومعالجة الحوسبة الطرفية وواجهات الاستشعار لتحديد الثغرات الأمنية.
- فحص مسارات البيانات وتتبع مصدرها وتطبيق تحويلات الحفاظ على الخصوصية في البيئات الموزعة.
- صياغة تقارير حوكمة وتدقيق مدعومة بتصنيف مستويات المخاطر وخطط الإجراءات التصحيحية.

جدول الدورة

اليوم 1: أسس مخاطر وحوكمة الذكاء الاصطناعي

- المفاهيم الجوهرية لأطر إدارة مخاطر الذكاء الاصطناعي والمعايير القياسية الدولية للحوكمة
- هياكل المساءلة والمسؤولية التشغيلية في عمليات اتخاذ القرار المؤتمتة
- استقلالية المدقق ومعايير التقييم وبروتوكولات جمع الأدلة الإثباتية
- تحديد مواصفات الأنظمة الجديرة بالثقة عبر مقاييس الشفافية والقابلية للتفسير والتنبؤ
- تحديد نطاق مهام التدقيق بالاعتماد على حالات الاستخدام التشغيلي ومستويات تصنيف المخاطر
- مواءمة المتطلبات النظامية الأساسية مع التزامات السياسات المؤسسية الداخلية

اليوم 2: تدقيق البنية التحتية وحوكمة البيانات

- تقييم البنية التحتية لوحدات المعالجة المتخصصة والبيئات السحابية الموزعة
- أمن العتاد ومخاطر معايرة أجهزة الاستشعار وثغرات التقاط البيانات في الحوسبة الطرفية
- جودة البيانات والتحقق من مصادرها وضوابط حوكمة البيانات التدريبية الاصطناعية
- تقييم أثر الخصوصية وتطبيق ضوابط الحد الأدنى من البيانات وسياسات الاحتفاظ بها
- قوائم مكونات البرمجيات وتقييم موردي الطرف الثالث في سلاسل إمداد الذكاء الاصطناعي
- ضوابط نقل البيانات عبر الحدود وتوكيد أمن المعماريات السحابية الموزعة

اليوم 3: التحقق من النماذج والذكاء الاصطناعي القابل للتفسير

- تقييم المخاطر الخوارزمية لنماذج التعلم الخاضع للإشراف وغير الخاضع للإشراف والتعلم المعزز
- مراجعة عمليات الضبط الدقيق للنماذج ونقاط التحقق ومؤشرات انجراف الأداء التشغيلي
- اكتشاف فرط التخصيص وتقييم قدرة النموذج على التعميم واختبارات استقرار الشروط الحدية
- تدقيق العدالة وتطبيق مسارات اكتشاف التحيز وتقنيات قياس التفاوت في النتائج
- أدوات الذكاء الاصطناعي القابل للتفسير وتقييم وضوح المخرجات وطرق إسناد الخصائص
- فحص معماريات التعلم الموحد وسلوكيات نماذج الذكاء الاصطناعي التوليدي

اليوم 4: الأمن والضوابط والرقابة البشرية

- مراجعات الأمن السيبراني لأنظمة الذكاء الاصطناعي واكتشاف التسلل واختبارات تسميم النماذج والمراوغة
- تقييم واجهات الاستخدام التي تجمع بين التوصيات المؤتمتة وضوابط تدخل المشغلين
- المرونة التشغيلية وإجراءات تكرار الأنظمة البديلة ومعايير الأمان المادي
- تقييم آليات الضبط المؤتمتة الهرمية والمستندة إلى رصد السلوك
- نماذج حوكمة الرقابة البشرية المباشرة والإشرافية وحالات التشغيل الذاتي الكامل
- مسارات إخراج الأنظمة من الخدمة وآليات الحماية التلقائية ومحفزات الإيقاف الطارئ

اليوم 5: توكيد دورة الحياة وإعداد تقارير التدقيق

- دمج قوائم التحقق المعيارية لمكونات العتاد ومسارات البيانات والخوارزميات
- مراجعة التوثيق عبر سجلات التدريب ومستودعات الشيفرات البرمجية وسجلات العمليات التشغيلية
- بناء أطر السياسات الداخلية وبوابات الرقابة المستمرة عبر حوكمة دورة حياة النماذج
- مراجعات الجاهزية التشغيلية بالاستناد إلى مؤشرات التوكيد المعتمدة مهنيا
- هيكلة تقارير التدقيق الدفاعية ومصفوفات تصنيف شدة المخاطر وملفات الأدلة الداعمة
- صياغة خطط المعالجة التصحيحية وتقديم العروض التقديمية للجان الحوكمة وأصحاب المصلحة

التمارين التطبيقية

ينفذ المشاركون تدريبات عملية مستندة إلى محاكاة واقعية لتقييم الأدلة الفنية وإعداد تقارير الضوابط.

- نشاط مقترح: إجراء تقييم للتحيز الخوارزمي على نموذج تصنيف تجريبي باستخدام مقاييس التكافؤ.
- نشاط مقترح: تنفيذ تدقيق لمسار البيانات والتحقق من سلسلة النسب وتوثيق الموافقة وسجلات التنقية.
- نشاط مقترح: تصميم مصفوفة تصعيد للرقابة البشرية لمعالجة إخفاقات القرارات التشغيلية المؤتمتة.
- نشاط مقترح: إعداد مسودة تقرير لنتائج تدقيق الأنظمة الذكية تتضمن مستويات الشدة والإجراءات التصحيحية.

الأسئلة الشائعة

ما المؤهلات أو المتطلبات المسبقة المطلوبة من المشاركين قبل الالتحاق بالدورة؟

لا توجد متطلبات مسبقة إلزامية، إلا أن المشاركين ذوي الخبرة في مجالات إدارة المخاطر أو التدقيق أو الامتثال أو تطوير الذكاء الاصطناعي أو الأمن السيبراني أو الحوكمة القانونية سيحققون أقصى استفادة. يفضل الإلمام بأسس نظم تقنية المعلومات الحديثة ومبادئ خصوصية البيانات.

كم تبلغ مدة الجلسات اليومية وما إجمالي الساعات التدريبية للدورة؟

تمتد جلسات كل يوم إلى قرابة 4 إلى 5 ساعات تدريبية تتضمن فترات استراحة وأنشطة تطبيقية وتفاعلية. ويبلغ إجمالي مدة البرنامج التدريبي على مدار أسبوع نحو 20 إلى 25 ساعة تدريبية مكثفة.

ما الفرق بين تدقيق نظام الذكاء الاصطناعي وتقييم الامتثال للوائح الذكاء الاصطناعي؟

يشمل تدقيق نظام الذكاء الاصطناعي فحص الأداء التشغيلي وسلامة الخوارزميات والشفافية والمرونة عبر كامل مراحل التشغيل، في حين يركز تقييم الامتثال بصورة مباشرة على استيفاء المتطلبات النظامية الإلزامية. يزود هذا البرنامج المهنيين بالقدرة على قياس مدى موثوقية النظام متجاوزا مجرد فحص بنود الامتثال الأساسية.

الخاتمة

يتعين على المنظمات التي توظف التقنيات المؤتمتة إثبات سلامة أنظمتها ومساءلتها ونزاهتها التشغيلية. يكتسب المشاركون عبر إتقان بروتوكولات التدقيق الفني وفحص البنية التحتية والتحقق من سلامة النماذج القدرة على حماية العمليات من المخاطر غير المتوقعة وترسيخ منظومة رقابية متينة وموثوقة للمؤسسة.