QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1205

دورة أمن وخصوصية الذكاء الاصطناعي

حوكمة وأخلاقيات ومخاطر الذكاء الاصطناعي
الذكاء الاصطناعي وتطبيقاته

المدة
5 ايام

طريقة التقديم
حضوري

المكان
باكو، أذربيجان

التواريخ
٩-٣١ نوفمبر ٢٠٢٦

شركة كويست ترينينج

quest-training.com

تفاصيل الموعد المجدول

المدينة	باكو، أذربيجان
التاريخ	٩–٣١ نوفمبر ٢٠٢٦
طريقة التقديم	حضوري
رسوم الدورة	٣٥٠٫٥ €

نظرة عامة على الدورة

تُعد دورة أمن وخصوصية الذكاء الاصطناعي (Course Training Privacy & Security AI) برنامجاً تدريبياً احترافياً متكاملاً يهدف إلى تزويد القيادات التنفيذية، والمديرين، ومتخصصي الذكاء الاصطناعي، والأمن السيبراني، وحوكمة البيانات، وحماية الخصوصية، وتقنية المعلومات، وإدارة المخاطر، والامتثال، والشؤون القانونية بالمعرفة والمهارات اللازمة لحماية أنظمة الذكاء الاصطناعي والبيانات المرتبطة بها من التهديدات الأمنية والمخاطر المتعلقة بالخصوصية. ومع التوسع السريع في تبني تقنيات الذكاء الاصطناعي في مختلف القطاعات، أصبحت حماية النماذج والبيانات والبنية التحتية للذكاء الاصطناعي من أهم الأولويات لضمان استمرارية الأعمال، والحفاظ على ثقة العملاء، والامتثال للمتطلبات التنظيمية.

تعتمد الجهات الحكومية، والوزارات، والهيئات العامة، والبنوك والمؤسسات المالية، وشركات النفط والغاز، والمؤسسات الصناعية، والمؤسسات الصحية، والمؤسسات التعليمية، وشركات الاتصالات، وشركات النقل والخدمات اللوجستية، والشركات الكبرى على تطبيقات الذكاء الاصطناعي لتحليل البيانات، وأتمتة العمليات، ودعم اتخاذ القرار، وتحسين الخدمات، وزيادة الكفاءة التشغيلية. إلا أن هذه الأنظمة تواجه مخاطر متزايدة تشمل الهجمات السيبرانية، وسرقة البيانات، وتسميم البيانات، والهجمات على النماذج، والتلاعب بالمخرجات، وتسرب المعلومات الحساسة، وانتهاك الخصوصية، وضعف ضوابط الوصول، مما يتطلب تبني استراتيجيات متقدمة لأمن وخصوصية الذكاء الاصطناعي.

يركز هذا البرنامج على بناء إطار متكامل لحماية أنظمة الذكاء الاصطناعي من خلال تغطية أمن النماذج، وأمن

البيانات، وحوكمة البيانات، والخصوصية، وإدارة الهوية والصلاحيات، وإدارة المخاطر، والذكاء الاصطناعي المسؤول، والأمن السيبراني، والتشفير، وإدارة الثغرات، ومراقبة الأنظمة، والاستجابة للحوادث، والامتثال التنظيمي، وأفضل الممارسات الدولية الخاصة بحماية حلول الذكاء الاصطناعي عبر دورة حياتها الكاملة.

وتجمع دورة أمن وخصوصية الذكاء الاصطناعي بين المفاهيم النظرية والتطبيقات العملية من خلال ورش عمل، وتمارين تفاعلية، ودراسات حالة واقعية تساعد المشاركين على تقييم المخاطر الأمنية، وتصميم ضوابط فعالة، وتطوير استراتيجيات حماية متكاملة لأنظمة الذكاء الاصطناعي. وبنهاية الدورة سيتمكن المشاركون من تعزيز أمن تطبيقات الذكاء الاصطناعي، وحماية البيانات، وتقليل المخاطر، وتحقيق الامتثال التنظيمي، ودعم الاستخدام الآمن والمسؤول للذكاء الاصطناعي.

أهداف الدورة

- تحليل التهديدات الأمنية والمخاطر المتعلقة بخصوصية الذكاء الاصطناعي.
- تطوير استراتيجيات متكاملة لحماية أنظمة الذكاء الاصطناعي والبيانات.
- تقييم مخاطر الأمن السيبراني والخصوصية المرتبطة بتطبيقات الذكاء الاصطناعي.
- تطبيق أفضل الممارسات لحماية النماذج والبيانات والبنية التحتية للذكاء الاصطناعي.
- تصميم ضوابط أمنية وإجراءات فعالة لإدارة الهوية والصلاحيات والوصول.
- تحسين ممارسات حوكمة البيانات، وحماية الخصوصية، والامتثال التنظيمي.
- تعزيز قدرة المؤسسة على اكتشاف التهديدات والاستجابة للحوادث المتعلقة بالذكاء الاصطناعي.
- تنفيذ آليات لمراقبة الأنظمة الذكية وقياس فعاليتها الأمنية بصورة مستمرة.
- تقييم مستوى نضج أمن وخصوصية الذكاء الاصطناعي داخل المؤسسة.
- مواءمة أمن الذكاء الاصطناعي مع استراتيجيات الأمن السيبراني، وإدارة المخاطر، والحوكمة المؤسسية.

الفئة المستهدفة

صُممت هذه الدورة للرؤساء التنفيذيين، ومديري تقنية المعلومات، ومديري الأمن السيبراني، ومديري أمن المعلومات، ومديري الذكاء الاصطناعي، ومديري البيانات، ومديري التحول الرقمي، ومديري الحوكمة، ومديري الامتثال، ومديري إدارة المخاطر، ومديري التدقيق الداخلي، ومسؤولي حماية البيانات، وعلماء البيانات، ومهندسي الذكاء الاصطناعي، ومهندسي تعلم الآلة، ومهندسي البرمجيات، والاستشاريين، وجميع المسؤولين عن حماية وإدارة أنظمة الذكاء الاصطناعي.

كما تستهدف العاملين في الجهات الحكومية، والوزارات، والهيئات العامة، والبنوك والمؤسسات المالية، وشركات النفط والغاز، والمؤسسات الصناعية، والمؤسسات الصحية، والمؤسسات التعليمية، وشركات الاتصالات، وشركات النقل والخدمات اللوجستية، والجهات التنظيمية، والشركات الاستشارية، والشركات متعددة الجنسيات التي تعتمد على حلول الذكاء الاصطناعي في عملياتها اليومية.

وتناسب الدورة أيضاً مسؤولي استمرارية الأعمال، وإدارة الجودة، والشؤون القانونية، والابتكار، والبحث والتطوير، وإدارة المشاريع، وحوكمة البيانات، وإدارة البنية التحتية الرقمية، وجميع المهنيين الراغبين في تطوير قدراتهم في أمن وخصوصية الذكاء الاصطناعي.

مخرجات التعلم

- بنهاية هذه الدورة سيكون المشاركون قادرين على:
- شرح المبادئ الأساسية لأمن وخصوصية الذكاء الاصطناعي.
- تحديد وتحليل التهديدات الأمنية ونقاط الضعف في أنظمة الذكاء الاصطناعي.
- تطوير إطار مؤسسي لحماية تطبيقات الذكاء الاصطناعي والبيانات.
- تصميم ضوابط أمنية لحماية النماذج، والبيانات، والبنية التحتية الرقمية.
- تطبيق ممارسات الأمن السيبراني، وحوكمة البيانات، وحماية الخصوصية، والامتثال التنظيمي.

- تنفيذ آليات لإدارة الهوية، والتحكم في الوصول، والتشفير، والاستجابة للحوادث.
- مراقبة أداء الأنظمة الذكية واكتشاف التهديدات وتحليلها بصورة مستمرة.
- دمج أمن وخصوصية الذكاء الاصطناعي ضمن الحوكمة المؤسسية وإدارة المخاطر.
- إعداد خطط للتعافي من الحوادث وتعزيز المرونة التشغيلية لأنظمة الذكاء الاصطناعي.
- إعداد خارطة طريق لتطوير منظومة مؤسسية متكاملة لأمن وخصوصية الذكاء الاصطناعي.
- المحاور التدريبية:

محاور الدورة

اليوم الأول

أساسيات أمن وخصوصية الذكاء الاصطناعي

- مقدمة في أمن الذكاء الاصطناعي وحماية الخصوصية.
- التهديدات السيبرانية التي تستهدف أنظمة الذكاء الاصطناعي.
- دورة حياة أمن الذكاء الاصطناعي.
- مبادئ حوكمة البيانات والخصوصية.
- ورشة عمل لتحديد المخاطر الأمنية في مشاريع الذكاء الاصطناعي.

اليوم الثاني

حماية البيانات والنماذج

- حماية البيانات الحساسة.
- إدارة الهوية والصلاحيات والتحكم في الوصول.
- أمن نماذج الذكاء الاصطناعي.

اليوم الثاني — تابع

- التشفير وإدارة المفاتيح.
- تطبيق عملي لتقييم أمن نموذج ذكاء اصطناعي.

اليوم الثالث

الحوكمة والامتثال

- حوكمة أمن الذكاء الاصطناعي.
- المتطلبات القانونية والتنظيمية لحماية البيانات.
- إدارة المخاطر والامتثال.
- الذكاء الاصطناعي المسؤول والخصوصية.
- ورشة عمل لتطوير إطار مؤسسي لأمن وخصوصية الذكاء الاصطناعي.

اليوم الرابع

المراقبة والاستجابة للحوادث

- مراقبة الأنظمة الذكية واكتشاف التهديدات.
- إدارة الثغرات الأمنية.
- الاستجابة للحوادث والتعافي.
- التحسين المستمر واختبارات الأمن.
- تطبيق عملي لتنفيذ ضوابط أمنية متقدمة.

اليوم الخامس

بناء استراتيجية مؤسسية لأمن وخصوصية الذكاء الاصطناعي

- مستقبل أمن الذكاء الاصطناعي والتحديات الناشئة.
- أفضل الممارسات العالمية في حماية أنظمة الذكاء الاصطناعي.
- دمج أمن الذكاء الاصطناعي ضمن استراتيجيات الأمن السيبراني والتحول الرقمي.
- إدارة التغيير وبناء ثقافة أمنية داخل المؤسسة.
- ورشة عمل ختامية لإعداد استراتيجية مؤسسية متكاملة لأمن وخصوصية الذكاء الاصطناعي تشمل أمن النماذج، وأمن البيانات، وحوكمة البيانات، وحماية الخصوصية، وإدارة الهوية والصلاحيات، والأمن السيبراني، والتشفير، وإدارة الثغرات، والاستجابة للحوادث، وإدارة المخاطر، والامتثال التنظيمي، والذكاء الاصطناعي المسؤول، وإدارة دورة حياة النماذج، والمراقبة المستمرة، والتدقيق، وقياس الأداء، والتحسين المستمر، بما يضمن تطوير وتشغيل واستخدام أنظمة ذكاء اصطناعي آمنة وموثوقة ومتوافقة مع المتطلبات التنظيمية، ويعزز المرونة التشغيلية، والثقة، والابتكار، والتميز المؤسسي وفق أفضل الممارسات العالمية.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: https://quest-training.com/courses/ai-security-privacy-training-course

الموقع الإلكتروني: https://quest-training.com

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440