الدورة التدريبية: الأمن في بيئات الذكاء الاصطناعي وتعلم الآلة



14 - 18 ديسمبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #SM9061_424495

مقدمة الدورة التدريبية / لمحة عامة:

يمثل الذكاء الاصطناعي وتعلم الآلة تحولًا جذريًا في مختلف القطاعات، ولكن مع هذا التطور تبرز تحديات أمنية فريدة تتطلب استراتيجيات حماية متخصصة. تهدف هذه الدورة التدريبية المتطورة، التي يقدمها BIG BEN Training Center، إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتأمين أنظمة الذكاء الاصطناعي وتعلم الآلة ضد التهديدات والهجمات السيبرانية. ستغطي الدورة الجوانب الحيوية لأمن الذكاء الاصطناعي، بدءًا من فهم نقاط الضعف في النماذج والخوارزميات، مرورًا بتأمين البيانات التدريبية، وصولًا إلى حماية الأنظمة المنتجة من الهجمات العدائية. تستند هذه الدورة إلى أحدث الأبحاث والمعايير الناشئة في مجال أمن الذكاء الاصطناعي، مستلهمة من أعمال أكاديميين بارزين مثل البروفيسور Dawn Song (دون سونغ)، أحد أبرز الباحثين في مجال أمن الكمبيوتر والذكاء الاصطناعي، والتي ساهمت أبحاثها بشكل كبير في فهم نقاط الضعف في نماذج تعلم الآلة وكيفية حمايتها. تهدف الدورة إلى تمكين المهنيين من بناء أنظمة ذكاء اصطناعي آمنة وموثوقة، تحافظ على سلامة البيانات، وتضمن دقة القرارات، وتحمي الابتكارات من المخاطر السيبرانية المتزايدة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الذكاء الاصطناعي وعلماء البيانات.
- متخصصو الأمن السيبراني.
- مدراء المنتجات والحلول القائمة على الذكاء الاصطناعي.
- المهندسون المعماريون للأنظمة.
- الباحثون في مجال الذكاء الاصطناعي والأمن.
- مدراء تكنولوجيا المعلومات.
- المسؤولون عن الامتثال والمخاطر.
- المطورون العاملون على تطبيقات الذكاء الاصطناعي.

القطاعات والصناعات المستهدفة:

- شركات التكنولوجيا وتطوير البرمجيات.
- المؤسسات المالية والبنوك (الخدمات المالية المدعمة بالذكاء الاصطناعي).
- قطاع الرعاية الصحية والطب الحيوي.
- شركات السيارات ذاتية القيادة.
- قطاع الدفاع والأمن.
- شركات التجارة الإلكترونية والتحليل البياني.
- الجهات الحكومية التي تستخدم أنظمة الذكاء الاصطناعي.
- شركات الاستشارات التقنية.

الأقسام المؤسسية المستهدفة:

- قسم البحث والتطوير (R&D).
- قسم الأمن السيبراني وأمن المعلومات.
- قسم الذكاء الاصطناعي وتعلم الآلة.
- قسم تكنولوجيا المعلومات.
- قسم إدارة المنتجات.
- إدارة المخاطر والامتثال.
- قسم الهندسة.
- القيادة التنفيذية.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم التهديدات والهجمات الشائعة ضد أنظمة الذكاء الاصطناعي.
- تأمين البيانات التدريبية ونماذج تعلم الآلة.
- تطبيق تقنيات الدفاع ضد الهجمات العدائية.
- تقييم نقاط الضعف الأمنية في خوارزميات الذكاء الاصطناعي.
- حماية خصوصية البيانات في بيئات تعلم الآلة.
- بناء أنظمة ذكاء اصطناعي آمنة وموثوقة.
- الامتثال للوائح ومعايير أمن الذكاء الاصطناعي.
- إدارة المخاطر المتعلقة بالذكاء الاصطناعي.
- مراقبة واكتشاف التهديدات في الوقت الفعلي.
- التعامل مع الحوادث الأمنية في أنظمة الذكاء الاصطناعي.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية متطورة تجمع بين المعرفة النظرية العميقة والتطبيق العملي الموجه، بهدف تمكين المشاركين من تأمين أنظمة الذكاء الاصطناعي وتعلم الآلة. ستتضمن المنهجية محاضرات تفاعلية تستعرض أحدث التهديدات والهجمات السيبرانية التي تستهدف نماذج الذكاء الاصطناعي، بالإضافة إلى استراتيجيات الدفاع المتقدمة. سيتم التركيز على دراسات الحالة الواقعية لهجمات عدائية على أنظمة الذكاء الاصطناعي وكيفية تحليلها والتخفيف من آثارها. سيشارك المتدربون في ورش عمل تطبيقية تستخدم بيئات محاكاة، حيث سيتمكنون من اختبار نماذج الذكاء الاصطناعي ضد الهجمات، وتطبيق ضوابط أمنية، وتقييم فعالية الدفاعات. تهدف هذه المنهجية إلى تزويد المشاركين بالمهارات العملية والتحليلية اللازمة لتصميم، وتطوير، ونشر أنظمة ذكاء اصطناعي آمنة وموثوقة، مما يحمي الابتكار ويضمن سلامة البيانات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى أمن الذكاء الاصطناعي وتعلم الآلة

- مفاهيم الذكاء الاصطناعي وتعلم الآلة.
- أهمية الأمن في أنظمة الذكاء الاصطناعي.
- أنواع التهديدات والهجمات على نماذج الذكاء الاصطناعي.
- نقاط الضعف الشائعة في خوارزميات تعلم الآلة.
- المتطلبات الأخلاقية والقانونية لأمن الذكاء الاصطناعي.
- المخاطر المرتبطة بالبيانات والنموذج.
- الذكاء الاصطناعي كمحرك للتهديدات والأمن.

الوحدة الثانية: تأمين البيانات التدريبية وسلامة النموذج

- أمن البيانات في دورة حياة الذكاء الاصطناعي.
- هجمات تلوث البيانات (Data Poisoning Attacks).
- تقنيات الحماية ضد تلوث البيانات.
- ضمان سلامة البيانات التدريبية.
- أمن الخصوصية في تعلم الآلة (Privacy-preserving ML).
- التعلم الفيدرالي وأمنه.
- تقييم جودة وسلامة مجموعة البيانات.

الوحدة الثالثة: الدفاع ضد الهجمات العدائية (Adversarial Attacks)

- أنواع الهجمات العدائية على نماذج الذكاء الاصطناعي.
- هجمات الالتفاف (Evasion Attacks).
- هجمات الاختراق (Exploration Attacks).
- تقنيات الدفاع ضد الهجمات العدائية.
- الكشف عن الأمثلة العدائية.
- صلابة النماذج (Model Robustness).
- تدريب النماذج المقاومة للهجمات.

الوحدة الرابعة: حماية الأنظمة المنتجة وإدارة الثغرات

- تأمين البنية التحتية لعمليات الذكاء الاصطناعي (MLOps Security).
- إدارة الثغرات الأمنية في تطبيقات الذكاء الاصطناعي.
- أمن الواجهات البرمجية (APIs) للذكاء الاصطناعي.
- مراقبة أداء النماذج والكشف عن الانحرافات.
- إدارة التغيير في نماذج الذكاء الاصطناعي.
- الاستجابة للحوادث الأمنية في أنظمة الذكاء الاصطناعي.
- التدقيق الأمني لنظم الذكاء الاصطناعي.

الوحدة الخامسة: أخلاقيات الأمن والتوجهات المستقبلية

- أخلاقيات الذكاء الاصطناعي وأمنه.
- التحيز في نماذج الذكاء الاصطناعي وآثاره الأمنية.
- الذكاء الاصطناعي التفسيري (Explainable AI) في الأمن.
- التحديات الأمنية للذكاء الاصطناعي التوليدي.
- اللوائح والمعايير الناشئة لأمن الذكاء الاصطناعي.
- البحث والتطوير في أمن الذكاء الاصطناعي.
- مستقبل الأمن في بيئات الذكاء الاصطناعي.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور المتسارع للذكاء الاصطناعي وتغلغله في كافة جوانب حياتنا، كيف يمكن للمتخصصين في الأمن السيبراني والذكاء الاصطناعي ضمان ثقة المستخدمين وسلامة المجتمعات، مع الحفاظ على قدرة هذه التقنيات على الابتكار والتطور، دون أن تصبح بحد ذاتها نقاط ضعف أمنية مستغلة من قبل الجهات الخبيثة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتركيزها المتخصص والعميق على الأمن في بيئات الذكاء الاصطناعي وتعلم الآلة، وهو مجال حديث وحيوي يتطلب فهمًا فريدًا يجمع بين الأمن وعلوم البيانات. يقدم BIG BEN Training Center محتوى أكاديميًا متطورًا، يستند إلى أحدث الأبحاث والاكتشافات في هذا المجال، مما يضمن حصول المشاركين على معرفة حديثة ومتقدمة. ما يميز هذه الدورة هو دمجها للجوانب النظرية والعملية، من خلال استعراض أنواع الهجمات العدائية وكيفية الدفاع عنها، وتأمين البيانات التدريبية، وحماية النماذج المنتجة. بدلاً من مجرد سرد المفاهيم، توفر الدورة رؤى عملية حول كيفية بناء أنظمة ذكاء اصطناعي آمنة وموثوقة، وكيفية التعامل مع التحديات الأخلاقية والقانونية، مما يجعلها ضرورية للمهنيين الذين يسعون لقيادة الابتكار في عصر الذكاء الاصطناعي مع ضمان أعلى مستويات الأمان.