التدريبية: الأمن في بيئات الذكاء الاصطناعي

وتعلم الآلة الدورة

اغسطس ٢٠٢٦ ٠٧ - ٠٣

برلين

(للشخص الواحد) ٤٩٠٠ €

Ref: #SM9061_334280

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

- الاصطناعي. فهم التهديدات والهجمات الشائعة ضد أنظمة الذكاء
- تأمين البيانات التدريبية ونماذج تعلم الآلة.
- تطبيق تقنيات الدفاع ضد الهجمات العدائية.
- الاصطناعي. تقييم نقاط الضعف الأمنية في خوارزميات الذكاء
- 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.
- الاصطناعي. التعامل مع الحوادث الأمنية في أنظمة الذكاء

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

وتعلم الآلة الوحدة الأولى: مقدمة إلى أمن الذكاء الاصطناعي

- 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.

النموذج الوحدة الثانية: تأمين البيانات التدريبية وسلامة

- 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.

الثغرات الوحدة الرابعة: حماية الأنظمة المنتجة وإدارة

- 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.

المستقبلية الوحدة الخامسة: أخلاقيات الأمن والتوجهات

- 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:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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