# التدريبية: التعلم الموحد - تعزيز خصوصية في الذكاء الاصطناعي (Federated Learning) الدورة البيانات

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

دوسلدورف

(للشخص الواحد) € ٤٢٠٠

Ref: #AI8066_245905

## مقدمة الدورة التدريبية / لمحة عامة:

الذكاء تعزيز :(Learning التدريبية المتخصصة حول التعلم الموحد (Federated يقدم BIG BEN Training Center هذه الدورة البيانات، ومديري المنتجات، والمختصين في الاصطناعي، وهي مصممة لمهندسي الذكاء الاصطناعي، خصوصية البيانات في الضخمة، أصبحت لـتطوير نماذج ذكاء اصطناعي (AI) دون المساس الأمن السيبراني والخصوصية، والباحثين الذين يسعون وعلماء ونشر حلول الذكاء الاصطناعي، خاصة في الخصوصية والأمان من أكبر التحديات التي تواجه بخصوصية البيانات. في عصر البيانات الآلي (Machine يوفر التعلم الموحد حلاً مبتكراً لهذه التحديات من القطاعات الحساسة مثل الرعاية الصحية والمالية. تطوير إلى تجميع البيانات الخام في موقع مركزي. على مجموعات بيانات موزعة محلياً دون (Learning خلال تمكين تدريب نماذج التعلم مختلفة، وتقنيات تعزيز وكيفية عمله، ومميزاته وتحدياته، وتطبيقاته ستغطي الدورة مفاهيم التعلم الموحد الأساسية، الحاجة والتشفير المتماثل (Differential Privacy) الخصوصية المرتبطة به مثل الخصوصية التفاضلية العملية في سيناريوهات الخصوصية في كيفية تصميم وتنفيذ أنظمة التعلم الموحد، وتحسين سيتعلم المشاركون .(Homomorphic Encryption) وبناء حلول ذكاء اصطناعي مشاريعهم. تهدف الدورة إلى تمكين المختصين من فهم أدائها، وضمان الامتثال لمتطلبات الآمنة والمسؤولة. نستلهم في هذه تحافظ على الخصوصية، والمساهمة في تطوير ممارسات إمكانات التعلم الموحد، الدورة من أعمال البروفيسور نيكولاس بابيرني الذكاء الاصطناعي

على أهمية خصوصية الرواد في مجال التعلم الموحد والخصوصية التفاضلية أحد Nicolas Papernot، Nicolas Papernot (Nicolas Papernot)؟ الدورة أمثلة واقعية على كيفية البيانات كعنصر أساسي في نشر الذكاء الاصطناعي على في الذكاء الاصطناعي، والذي يؤكد الخصوصية، مما يعزز فهم المشاركين للجوانب تطبيق التعلم الموحد في الصناعات التي تتطلب أعلى نطاق واسع. ستقدم العملية والتطبيقية. مستويات

## لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مهندسي الذكاء الاصطناعي والتعلم الآلي.
- علماء البيانات.
- مهندسي البرمجيات.
- المختصين في أمن البيانات والخصوصية.
- مديري المنتجات في شركات التكنولوجيا.
- الباحثين في مجال الذكاء الاصطناعي.
- المدراء التقنيين.
- المختصين في الامتثال والتنظيم.
- مهندسي النظم الموزعة.
- المهتمين بالذكاء الاصطناعي المسؤول.

## القطاعات والصناعات المستهدفة:

- الرعاية الصحية (حماية سجلات المرضى).
- الاحتيال).الخدمات المالية (الأمن المصرفي، الكشف عن
- الاتصالات (تحسين الخدمات دون تجميع البيانات).
- الأجهزة المحمولة).التكنولوجيا والمستهلك (لوحات المفاتيح الذكية،
- القطاع الحكومي (خصوصية المواطنين).
- السيارات (القيادة الذاتية الآمنة).
- التصنيع (الصيانة التنبؤية للآلات).
- البحث والتطوير.
- التجارة الإلكترونية (توصيات المنتجات).
- التأمين.

## الأقسام المؤسسية المستهدفة:

- قسم الذكاء الاصطناعي والتعلم الآلي.
- قسم أمن المعلومات والخصوصية.
- قسم البحث والتطوير (R&D).
- قسم تطوير المنتجات.
- قسم الامتثال القانوني والتنظيمي.
- قسم علم البيانات.
- قسم هندسة البرمجيات.
- قسم إدارة البيانات.
- قسم الابتكار.
- قسم الاستراتيجية التقنية.

## أهداف الدورة التدريبية:

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

- فهم المبادئ الأساسية للتعلم الموحد وكيفية عمله.
- التمييز بين التعلم الموحد وطرق التدريب الموزعة الأخرى.
- تحديد مميزات وتحديات تطبيق التعلم الموحد.
- استكشاف تطبيقات التعلم الموحد في مختلف الصناعات.
- فهم آليات الخصوصية التفاضلية ودورها في التعلم الموحد.
- التعرف على التشفير المتماثل وتطبيقاته في التعلم الموحد.
- تصميم معماريات التعلم الموحد لمشاريع واقعية.
- التعامل مع أدوات وأطر عمل التعلم الموحد (مثل TensorFlow Federated).
- تقييم المخاطر المتعلقة بالخصوصية والأمان في أنظمة التعلم الموحد.
- بناء نماذج ذكاء اصطناعي تحافظ على خصوصية البيانات بفعالية.

## منهجية الدورة التدريبية:

لبناء حلول منهجية تدريبية متقدمة وتطبيقية، تهدف إلى تزويد يعتمد BIG BEN Training Center في هذه الدورة على محاضرات نظرية معمقة ذكاء اصطناعي تحافظ على خصوصية البيانات باستخدام المشاركين بالمعرفة والمهارات اللازمة لتعزيز الخصوصية، بالإضافة إلى ورش عمل حول المفاهيم الأساسية للتعلم الموحد والتقنيات التعلم الموحد. تشمل المنهجية لحماية أنظمة تعلم موحد بسيطة، وفحص تحدياتها العملية، عملية مكثفة. سيقوم المشاركون بتصميم وتنفيذ المتقدمة التي تتطلب خصوصية عالية، مما البيانات الحساسة. سيتم التركيز على دراسات حالة وتطبيق تقنيات مثل الخصوصية التفاضلية للتعلم الموحد. تتضمن الدورة جلسات عمل جماعي يعزز فهم المشاركين للجوانب العملية والتطبيقية واقعية من الصناعات مهاراتهم في هذا يتلقى المشاركون تغذية راجعة مفصلة ومنتظمة من لتطوير حلول مبتكرة لمشكلات خصوصية البيانات. المجال الحيوي والمتطور المدربين الخبراء لضمان تطوير

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

## الوحدة الأولى: مقدمة إلى التعلم الموحد ومبادئه.

- ونشأته.ا مفهوم التعلم الموحد ((Federated Learning
- البيانات.ا الحاجة إلى التعلم الموحد: تحديات الخصوصية وأمن
- الفرق بين التعلم الموحد والتعلم الموزع التقليدي.ا
- كيف يعمل التعلم الموحد: نظرة عامة على سير العمل.ا
- .ا(Cross-silo أنواع معماريات التعلم الموحد (,Cross-device
- اللامركزية).ا مميزات التعلم الموحد (الخصوصية، الكفاءة،
- التواصل، الأمان).ا تحديات التعلم الموحد (عدم تجانس البيانات،

## الموحد.ا الوحدة الثانية: تقنيات تعزيز الخصوصية في التعلم

- المبادئ والتطبيقات.ا الخصوصية التفاضلية (:Differential Privacy)ا
- البيانات.ا إضافة الضوضاء (Noise Injection)ا لحماية خصوصية
- في التعلم الموحد.ا التشفير المتماثل (Homomorphic Encryption)ا ودوره
- .ا(Computation - SMPC الحساب الآمن متعدد الأطراف (Secure Multi-Party
- الموحد.ا الهندسة المعمارية لحماية الخصوصية في التعلم
- مقارنة بين تقنيات تعزيز الخصوصية.ا
- تنفيذ الخصوصية التفاضلية في نماذج التعلم الموحد.ا

## الوحدة الثالثة: تصميم وتطبيق أنظمة التعلم الموحد.ا

- الموحد.ا اختيار النموذج والخوارزمية المناسبة للتعلم
- الموحد.ا إدارة البيانات غير المتجانسة في بيئات التعلم
- .ا(Strategies استراتيجيات تجميع النماذج (Aggregation
- تحسين التواصل والكفاءة في التعلم الموحد.ا
- .ا(PySyft أطر عمل التعلم الموحد (,TensorFlow Federated
- بناء أول نظام تعلم موحد بسيط.ا
- استكشاف حالات الاستخدام العملية للتعلم الموحد.ا

## الصناعات.ا الوحدة الرابعة: تطبيقات عملية للتعلم الموحد في

- التعلم الموحد في الرعاية الصحية والتشخيص الطبي.ا
- الاحتيال.ا التعلم الموحد في الخدمات المالية والكشف عن
- الذكية.ا التعلم الموحد في الأجهزة المحمولة ولوحات المفاتيح
- التعلم الموحد في أنظمة القيادة الذاتية.ا
- التعلم الموحد في تطبيقات المدن الذكية.ا
- التعلم الموحد في قطاع الاتصالات.ا
- الموحد.ا تحديات خاصة بكل قطاع وكيفية معالجتها بالتعلم

## والاعتبارات الأخلاقية.ا الوحدة الخامسة: مستقبل التعلم الموحد، التحديات،

- الموحد.ا التطورات الحديثة والاتجاهات المستقبلية في التعلم
- التحديات البحثية المفتوحة في التعلم الموحد.ا
- الامتثال التنظيمي والخصوصية (GDPR, HIPAA).ا
- العدالة).ا الاعتبارات الأخلاقية للتعلم الموحد (التحيز،
- التعلم الموحد.ا الذكاء الاصطناعي المسؤول (Responsible AI) ودور
- الاصطناعي.ا تأثير التعلم الموحد على الابتكار في الذكاء
- الخطوات التالية للمهنيين في مجال التعلم الموحد.ا

## الأسئلة المتكررة:ا

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

لا توجد شروط مسبقة.ا

## 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:

ضمان تحقيق التوازن البيانات في تطوير نماذج الذكاء الاصطناعي، كيف مع تزايد الاعتماد على التعلم الموحد كحل لخصوصية أقصى استفادة من البيانات الموزعة لتحسين الأمثل بين الحفاظ على سرية المعلومات الفردية يمكن للمطورين والمنظمين التقنية والتحديات الأخلاقية؟ أداء النماذج، مع الأخذ في الاعتبار التعقيدات وتحقيق

## ما الذي يميز هذه الدورة عن غيرها من الدورات؟

ما يميزنا الموحد، وهو مجال حيوي ومتزايد الأهمية في سياق تتميز هذه الدورة بتقديمها تخصصاً عميقاً في التعلم تحافظ على الخصوصية، مع دمج هو التركيز على الجانب العملي والتطبيقي لبناء خصوصية البيانات وأمن الذكاء الاصطناعي. مبادئه التفاضلية والتشفير المتماثل. نغطي جميع الجوانب أحدث التقنيات لتعزيز الأمان مثل الخصوصية أنظمة ذكاء اصطناعي تركز على تزويد المشاركين الأساسية إلى تصميمه وتطبيقاته في مختلف الصناعات الأساسية والمتقدمة للتعلم الموحد، من الذكاء الاصطناعي التي تتطلب معالجة آمنة للبيانات، بالمهارات اللازمة للمساهمة بفاعلية في مشاريع الحساسة. الدورة المعقد والمطلوب. مما يجعلها ضرورية لأي محترف يسعى ليكون رائداً في وقيادة مبادرات الابتكار مع الالتزام بالخصوصية، هذا المجال