مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الذكاء الاصطناعي في تعزيز الأمن السيبراني الحكومي

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 12 – 16 / 01 / 2025.

مقدمة :

في ظل التطور المتسارع للهجمات السيبرانية وزيادة تعقيدها، يبرز الذكاء الاصطناعي كأداة حيوية لتعزيز الأمن السيبراني الحكومي. توفر هذه الدورة المتقدمة استكشافًا معمقًا لكيفية استخدام الذكاء الاصطناعي في الكشف عن التهديدات السيبرانية، والاستجابة لها، والوقاية منها، مما يساهم في بناء دفاعات قوية ومرنة لحماية الأصول والبيانات الحكومية الحساسة. ستغطي الدورة مجموعة واسعة من المواضيع، بدءًا من أساسيات الأمن السيبراني والذكاء الاصطناعي وصولًا إلى تطبيقات الذكاء الاصطناعي المتقدمة في مكافحة الهجمات السيبرانية المعقدة.

أهداف الورشة:

- فهم المفاهيم الأساسية للأمن السيبراني والذكاء الاصطناعي.
- استكشاف تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات السيبرانية والاستجابة لها.
- تطوير استراتيجيات لاستخدام الذكاء الاصطناعي في تعزيز الأمن الوقائي.
- فهم التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي في الأمن السيبراني.
- تطبيق أدوات وتقنيات الذكاء الاصطناعي في تحليل البيانات الأمنية واكتشاف الأنماط.
- بناء نماذج ذكاء اصطناعي للتنبؤ بالتهديدات السيبرانية ومنعها.
- تطوير خطط استجابة فعالة للحوادث السيبرانية باستخدام الذكاء الاصطناعي.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة في الأمن السيبراني والذكاء الاصطناعي

- المفاهيم الأساسية للأمن السيبراني وأنواع التهديدات السيبرانية.
- مقدمة في الذكاء الاصطناعي وتقنياته الرئيسية (التعلم الآلي، الشبكات العصبية، معالجة اللغة الطبيعية).
- نظرة عامة على دور الذكاء الاصطناعي في تعزيز الأمن السيبراني.

اليوم التدريبي الثاني:

الذكاء الاصطناعي في الكشف عن التهديدات والاستجابة لها

- استخدام الذكاء الاصطناعي في تحليل سلوك المستخدم واكتشاف الأنشطة المشبوهة.
- تطبيق التعلم الآلي في تحليل البيانات الأمنية واكتشاف الأنماط الخفية.
- استخدام الذكاء الاصطناعي في الاستجابة الآلية للحوادث السيبرانية.
- دراسة حالات واقعية لاستخدام الذكاء الاصطناعي في الكشف عن التهديدات والاستجابة لها.

اليوم التدريبي الثالث:

الذكاء الاصطناعي في الأمن الوقائي

- بناء نماذج ذكاء اصطناعي للتنبؤ بالتهديدات السيبرانية ومنعها.
- استخدام الذكاء الاصطناعي في تحليل الثغرات الأمنية وتقييم المخاطر.
- تطبيق الذكاء الاصطناعي في تعزيز أمن الشبكات والأنظمة.
- دراسة حالات واقعية لاستخدام الذكاء الاصطناعي في الأمن الوقائي.

اليوم التدريبي الرابع:

التحديات والفرص في استخدام الذكاء الاصطناعي في الأمن السيبراني

- التحديات الأخلاقية والقانونية المتعلقة باستخدام الذكاء الاصطناعي في الأمن السيبراني.
- سباق التسلح بين المهاجمين والمدافعين في استخدام الذكاء الاصطناعي.
- الفرص المستقبلية لتطوير واستخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني.
- جلسة نقاش حول مستقبل الذكاء الاصطناعي في الأمن السيبراني الحكومي.

اليوم التدريبي الخامس:

ورشة عمل وتطبيق عملي

- ورشة عمل لتطبيق المفاهيم والمهارات المكتسبة على سيناريوهات واقعية.
- استخدام أدوات وتقنيات الذكاء الاصطناعي في تحليل البيانات الأمنية.
- بناء نماذج بسيطة للكشف عن التهديدات السيبرانية.
- تقييم أداء النماذج واقتراح تحسينات.

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.