مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

أنظمة الذكاء الاصطناعي في تحليل التهديدات الأمنية.

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 13 – 17 / 04 / 2025.

مقدمة :

تُشكل التهديدات الأمنية تحديًا مُتزايدًا في ظل التعقيدات التي يشهدها العصر الحالي .وتُعد أنظمة الذكاء الاصطناعي أداة فعّالة لمواجهة هذه التحديات، حيث تُقدم قدرات فائقة في تحليل البيانات واكتشاف الأنماط والتنبؤ بالمخاطر الأمنية .يأتي هذا البرنامج التدريبي "أنظمة الذكاء الاصطناعي في تحليل التهديدات الأمنية "ليُقدم للمؤسسات الحكومية فرصة استثنائية للاستفادة من إمكانيات الذكاء الاصطناعي في تعزيز أمنها و حماية مصالحها .سيتعرف المشاركون على أحدث التقنيات و التطبيقات في هذا المجال، و سيكتسبون المهارات اللازمة لتحليل التهديدات الأمنية باستخدام أنظمة الذكاء الاصطناعي واتخاذ القرارات الاستباقية المناسبة.

أهداف الورشة:

- فهم مبادئ الذكاء الاصطناعي و تطبيقاته في المجال الأمني.
- التعرف على أنواع التهديدات الأمنية و كيفية استخدام الذكاء الاصطناعي في تحليلها.
- تحليل البيانات الأمنية باستخدام تقنيات الذكاء الاصطناعي واستخلاص النتائج.
- استخدام أنظمة الذكاء الاصطناعي في التنبؤ بالمخاطر الأمنية واتخاذ الإجراءات الوقائية.
- تقييم فعالية أنظمة الذكاء الاصطناعي في تحسين الأمن في المؤسسات الحكومية.
- تطوير استراتيجيات أمنية فعّالة باستخدام أنظمة الذكاء الاصطناعي.
- بناء قدرات المؤسسات الحكومية في مجال استخدام الذكاء الاصطناعي لأغراض الأمن.

محتويات الورشة:

اليوم الأول:

- **مقدمة في الذكاء الاصطناعي و تطبيقاته الأمنية :**
  - مفهوم الذكاء الاصطناعي و أنواعه.
  - تطبيقات الذكاء الاصطناعي في مجال الأمن.
  - أخلاقيات استخدام الذكاء الاصطناعي في الأمن.
- **تحليل البيانات الأمنية باستخدام الذكاء الاصطناعي :**
  - جمع و تنظيم البيانات الأمنية.
  - تقنيات تحليل البيانات باستخدام الذكاء الاصطناعي)التعلم الآلي، التعلم العُمق، وغيرها.(
  - استخلاص الأنماط و الرؤى من البيانات الأمنية.

اليوم الثاني:

- **كشف و تصنيف التهديدات الأمنية باستخدام الذكاء الاصطناعي :**
  - أنواع التهديدات الأمنية)الإرهاب، الجريمة المنظمة، الهجمات السيبرانية، وغيرها.(
  - نماذج الذكاء الاصطناعي لتصنيف و تقييم التهديدات.
  - أنظمة الإنذار المُبكر باستخدام الذكاء الاصطناعي.
- **التنبؤ بالمخاطر الأمنية باستخدام الذكاء الاصطناعي :**
  - تقنيات التنبؤ باستخدام الذكاء الاصطناعي)سلاسل Markovالزمنية، شبكات Bayesian، وغيرها.(
  - تطوير نماذج التنبؤ بالمخاطر الأمنية.
  - تقييم دقة نماذج التنبؤ.

اليوم الثالث:

- **اتخاذ القرارات الأمنية باستخدام الذكاء الاصطناعي :**
  - دور الذكاء الاصطناعي في دعم اتخاذ القرارات الأمنية.
  - أنظمة دعم القرارات باستخدام الذكاء الاصطناعي.
  - تحليل السيناريوهات و تقييم الخيارات المتاحة.
- **تطبيقات الذكاء الاصطناعي في مُختلف المجالات الأمنية :**
  - أمن المطارات و المنافذ الحدودية.
  - مكافحة الجريمة و الإرهاب.
  - الأمن السيبراني.

اليوم الرابع:

- **أدوات و تقنيات الذكاء الاصطناعي في تحليل التهديدات الأمنية :**
  - منصات تحليل البيانات الضخمة.
  - أدوات تصور البيانات و تحليل الشبكات الاجتماعية.
  - أنظمة المراقبة بالفيديو باستخدام الذكاء الاصطناعي.
- **تحديات و قيود استخدام الذكاء الاصطناعي في الأمن :**
  - قضايا الخصوصية و حماية البيانات.
  - تحيز البيانات و تأثيره على دقة النماذج.
  - الحاجة إلى كوادر مؤهلة في مجال الذكاء الاصطناعي.

اليوم الخامس:

- **ورش عمل و تمارين تطبيقية :**
  - تحليل حالات دراسية و سيناريوهات أمنية باستخدام أدوات الذكاء الاصطناعي.
  - تطوير نماذج لتحليل و التنبؤ بالمخاطر الأمنية.
  - مناقشة التحديات و الحلول في مجال تطبيق الذكاء الاصطناعي في الأمن.
- **تقييم و اختتام البرنامج :**
  - اختبار المهارات المكتسبة خلال البرنامج.
  - تقييم البرنامج و تقديم التغذية الراجعة.
  - مناقشة الخطوات المستقبلية لتطوير مهارات المشاركين في مجال الذكاء الاصطناعي و الأمن.

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.