مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الذكاء الاصطناعي في تعزيز الأمن السيبراني

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 30 – 3 / 3 – 4 / 2025.

مقدمة :

في ظل تزايد الهجمات السيبرانية وتطور أساليبها، أصبح الذكاء الاصطناعي (AI) من الأدوات الضرورية لتعزيز الأمن السيبراني. تعتمد المؤسسات اليوم على الذكاء الاصطناعي لتحليل كميات هائلة من البيانات، واكتشاف التهديدات المحتملة، واتخاذ إجراءات استباقية لحماية الأنظمة والشبكات. يتيح الذكاء الاصطناعي القدرة على التصدي للهجمات المتقدمة بشكل أسرع وأكثر دقة من الأساليب التقليدية. يهدف برنامج "الذكاء الاصطناعي في تعزيز الأمن السيبراني" إلى تزويد المشاركين بالمهارات والمعرفة اللازمة لاستخدام الذكاء الاصطناعي في حماية الأنظمة، واكتشاف التهديدات السيبرانية، وتطوير استراتيجيات دفاعية مبتكرة.

أهداف الورشة:

- فهم مفهوم الذكاء الاصطناعي وتطبيقاته في الأمن السيبراني.
- التعرف على أبرز تقنيات الذكاء الاصطناعي المستخدمة في الكشف عن التهديدات والاستجابة لها (مثل تعلم الآلة، معالجة اللغة الطبيعية، تحليل السلوك).
- إتقان مهارات استخدام أدوات الذكاء الاصطناعي في تحليل البيانات الأمنية الضخمة.
- تطوير القدرة على توقع الهجمات المحتملة واتخاذ إجراءات وقائية.
- تصميم وتنفيذ استراتيجيات دفاعية استباقية تعتمد على الذكاء الاصطناعي.
- فهم التحديات الأخلاقية والقانونية المتعلقة باستخدام الذكاء الاصطناعي في الأمن السيبراني.
- تطبيق المعرفة المكتسبة في تطوير حلول أمنية مبتكرة قائمة على الذكاء الاصطناعي.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى الذكاء الاصطناعي في الأمن السيبراني

- مفهوم الذكاء الاصطناعي وأنواعه (تعلم الآلة، معالجة اللغة الطبيعية، رؤية الكمبيوتر).
- تطبيقات الذكاء الاصطناعي في الأمن السيبراني (الكشف عن التهديدات، تحليل البيانات، الاستجابة للحوادث).
- مزايا وتحديات استخدام الذكاء الاصطناعي في الأمن السيبراني.
- ورشة عمل: التعرف على أدوات الذكاء الاصطناعي مفتوحة المصدر في الأمن السيبراني.

اليوم التدريبي الثاني:

الكشف عن التهديدات باستخدام تعلم الآلة

- مفهوم تعلم الآلة وأنواعه (تعلم مُشرف، تعلم غير مُشرف، تعلم مُعزز).
- تطبيق تعلم الآلة في الكشف عن البرمجيات الخبيثة، والتصيد الاحتيالي، والهجمات الأخرى.
- تقييم أداء نماذج تعلم الآلة وتحسينها.
- ورشة عمل: بناء نموذج بسيط للكشف عن البرمجيات الخبيثة باستخدام تعلم الآلة.

اليوم التدريبي الثالث:

تحليل البيانات الأمنية الضخمة

- مفهوم البيانات الضخمة وأهميتها في الأمن السيبراني.
- تحديات جمع وتحليل البيانات الأمنية الضخمة.
- استخدام أدوات الذكاء الاصطناعي في تحليل البيانات الأمنية (مثل SIEM، UEBA).
- استخلاص رؤى قيمة من البيانات الأمنية لاتخاذ قرارات استباقية.
- ورشة عمل: تحليل سجلات أحداث أمنية باستخدام أدوات الذكاء الاصطناعي.

اليوم التدريبي الرابع:

التنبؤ بالهجمات والاستجابة لها

- استخدام الذكاء الاصطناعي في التنبؤ بالهجمات المحتملة.
- تحليل سلوك المستخدمين والأنظمة للكشف عن الأنشطة المشبوهة.
- أتمتة الاستجابة للحوادث الأمنية.
- ورشة عمل: تطوير سيناريو هجوم سيبراني وتطبيق استراتيجيات الاستجابة باستخدام الذكاء الاصطناعي.

اليوم التدريبي الخامس:

التحديات والحلول وأفضل الممارسات

- التحديات الأخلاقية والقانونية المتعلقة باستخدام الذكاء الاصطناعي في الأمن السيبراني.
- أفضل الممارسات في استخدام الذكاء الاصطناعي في الأمن السيبراني.
- التوجهات المستقبلية في هذا المجال.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.
- إعداد خطط عمل فردية لتطبيق المعرفة المكتسبة.

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.