



مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

تقنيات التعرف على الأنماط لتحليل البيانات الأمنية.

مكان الإنعقاد : الإمارات العربية المتحدة - دبي

تاريخ الإنعقاد : 04 - 08 / 05 / 2025.





مقدمة :

تُشكل البيانات الأمنية موردًا حيويًا لفهم التهديدات و اتخاذ القرارات الاستباقية لحماية المجتمعات و المؤسسات. و تُعد تقنيات التعرف على الأنماط أداة فعّالة لاستخراج المعلومات القيمة من هذه البيانات و الكشف عن الصلات الخفية بينها. يأتي هذا البرنامج التدريبي "تقنيات التعرف على الأنماط لتحليل البيانات الأمنية" ليُقدم للمشاركين رحلة غنية في أحدث تقنيات التعرف على الأنماط و تطبيقاتها في مجال الأمن . سيتعلم المشاركون كيفية تحليل البيانات الأمنية من مصادر مُختلفة، و استخدام الخوارزميات المتقدمة لاكتشاف الأنماط و التنبؤ بالمخاطر الأمنية بفعالية. سيُساهم هذا البرنامج في تطوير مهارات التحليل و اتخاذ القرارات لدى العاملين في المجال الأمني، و تمكينهم من استخدام أحدث التقنيات لضمان أمن و سلامة المجتمع

أهداف الورشة:

- فهم مفهوم التعرف على الأنماط و أهميته في تحليل البيانات الأمنية .
- التعرف على مُختلف تقنيات التعرف على الأنماط و الخوارزميات المستخدمة .
- تحليل أنواع مُختلفة من البيانات الأمنية (نصوص، صور، فيديو، إشارات .)
- تطبيق تقنيات التعرف على الأنماط لاكتشاف التهديدات و السلوكيات المُريبة .
- استخدام أدوات و برمجيات التعرف على الأنماط لتحليل البيانات الأمنية .
- تقييم فعالية تقنيات التعرف على الأنماط في مُختلف التطبيقات الأمنية .
- تطوير مهارات التحليل و اتخاذ القرارات بناءً على النتائج المُستخرجة من البيانات



محتويات الورشة:

اليوم الأول:

- مقدمة في التعرف على الأنماط و تحليل البيانات الأمنية :
 - مفهوم التعرف على الأنماط و أنواعه.
 - مصادر البيانات الأمنية و تحديات تحليلها.
 - أخلاقيات استخدام تقنيات التعرف على الأنماط في الأمن.
- تقنيات التعلم الآلي للتعرف على الأنماط :
 - التعلم الخاضع للإشراف (التصنيف، التنبؤ).
 - التعلم غير الخاضع للإشراف (التجميع، اكتشاف الشذوذ).
 - تقييم أداء نماذج التعلم الآلي.

اليوم الثاني:

- التعرف على الأنماط في البيانات النصية :
 - تحليل المشاعر و تحديد المواضيع.
 - الكشف عن اللغة المسيئة و التهديدات.
 - استخراج المعلومات و تحليل الشبكات الاجتماعية.
- التعرف على الأنماط في الصور و الفيديو :
 - التعرف على الوجوه و الأشخاص.
 - كشف الأجسام و الأحداث المرئية.
 - تحليل سلوك الحشود و التنبؤ بالأحداث.



اليوم الثالث:

- التعرف على الأنماط في الإشارات و البيانات الحسية :
 - تحليل إشارات الاتصالات و الكشف عن التشويش.
 - مراقبة الأنظمة الصناعية و الكشف عن الأعطال.
 - تحليل البيانات الطبية و التنبؤ بالأمراض.
- التعامل مع البيانات الضخمة في التطبيقات الأمنية :
 - تخزين و معالجة البيانات الضخمة.
 - تقنيات تحليل البيانات الضخمة الموزعة.
 - تصور و تفسير النتائج.

اليوم الرابع:

- أدوات و برمجيات التعرف على الأنماط :
 - مكتبات التعلم الآلي (Scikit-learn)، TensorFlow، PyTorch.
 - أدوات تحليل البيانات (Tableau)، Power BI.
 - منصات تحليل البيانات الضخمة (Hadoop)، Spark.
- تطبيقات التعرف على الأنماط في مُختلف المجالات الأمنية :
 - مكافحة الجريمة و الإرهاب.
 - أمن المطارات و المنافذ الحدودية.
 - الأمن السيبراني.



اليوم الخامس:

• ورش عمل و تمارين تطبيقية :

- تحليل مُختلف أنواع البيانات الأمنية باستخدام تقنيات التعرف على الأنماط.
- تطبيق الخوارزميات المتقدمة لاكتشاف الأنماط و التنبؤ بالمخاطر.
- مناقشة تحديات و حلول التعرف على الأنماط في التطبيقات الأمنية.

• تقييم و اختتام البرنامج :

- اختبار المهارات المكتسبة خلال البرنامج.
- تقييم البرنامج و تقديم التغذية الراجعة.
- مناقشة الخطوات المستقبلية لتطوير مهارات المشاركين في مجال التعرف على الأنماط

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.