BLACKBIRD FOR TRAINING

اكتشاف التهديدات والاستجابة لها باستخدام الذكاء الاصطناعي

17 – 21 مايو 2027

باريس (فرنسا)

UK Traininig

PARTNER

www.blackbird-training.com

اكتشاف التهديدات والاستجابة لها باستخدام الذكاء الاصطناعي

المرجع: 336968_3255274 **التاريخ:** 17 – 21 مايو 2027 **المكان:** باريس (فرنسا) **الرسوم:** GBP 5900

مقدمة

في ظل تسارع التطورات الرقمية وتزايد الهجمات السيبرانية المعقدة، أصبحت الحلول التقليدية غير كافية لمواجهة التهديدات الحديثة. هنا يأتي دور الذكاء الاصطناعي في اكتشاف التهديدات والاستجابة لها كأحد أكثر الابتكارات تأثيرًا في مجال الأمن السيبراني.

يتيح الذكاء الاصطناعي للمؤسسات الانتقال من النهج التفاعلي إلى النهج الاستباقي، من خلال التنبؤ بالهجمات وتحليل السلوكيات غير المعتادة والاستجابة لها في الوقت الفعلي.

تهدف هذه الدورة إلى تزويد المشاركين بفهم شامل لكيفية توظيف تقنيات الذكاء الاصطناعي في تعزيز قدرات الاكتشاف والاستجابة الأمنية، وبناء أنظمة أكثر مرونة واستدامة قادرة على مواجهة التحديات الرقمية المتصاعدة.

أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم المفاهيم الأساسية لتطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني.
- تحليل القيود في أنظمة الكشف التقليدية وكيف يعالجها الذكاء الاصطناعي.
- تطبيق خوارزميات التعلم الآلي لاكتشاف التهديدات وتحليل السلوكيات.
- دمج نماذج الذكاء الاصطناعي في أنظمة إدارة الأحداث والمعلومات الأمنية.
- تصميم استراتيجيات استجابة مؤتمتة للتعامل مع الهجمات الإلكترونية.
- دراسة الجوانب الأخلاقية والحوكمة في استخدام الذكاء الاصطناعي الأمني.
- تطوير قدرات التحليل واتخاذ القرار باستخدام بيانات التهديدات الذكية.

محاور الدورة

اليوم الأول: مقدمة في الذكاء الاصطناعي للأمن السيبراني

- دور الذكاء الاصطناعي في تطوير منظومات الأمن الحديثة.
- التعلم الآلي والتعلم العميق في كشف التهديدات.
- مقارنة بين الأنظمة التقليدية والأنظمة القائمة على الذكاء الاصطناعي.
- أهمية البيانات في بناء أنظمة كشف فعالة.
- التحديات التقنية في دمج الذكاء الاصطناعي مع الأنظمة القائمة.

اليوم الثاني: نماذج التعلم الآلي لكشف التهديدات

- أنواع نماذج التعلم الآلي: الموجّه وغير الموجّه والتعزيز.
- تدريب النماذج على اكتشاف السلوكيات الخبيثة والأنشطة غير الطبيعية.
- تقليل الأخطاء الإيجابية وتحسين دقة الاكتشاف.
- اختيار الخصائص المناسبة لبيانات الأمن السيبراني.
- دراسة حالات ناجحة لاستخدام الذكاء الاصطناعي في الحماية المؤسسية.

اليوم الثالث: المراقبة والتحليل في الوقت الفعلي

- استخدام التحليلات الضخمة للمراقبة المستمرة للتهديدات.
- دمج مصادر البيانات المختلفة للكشف المبكر عن المخاطر.
- تطبيق الذكاء الاصطناعي في أنظمة الكشف والمنع من التسلل.
- تحليل السلوك الداخلي لاكتشاف التهديدات من داخل المؤسسة.
- تفسير وتحليل النتائج الصادرة عن النماذج الذكية.

اليوم الرابع: الاستجابة المؤتمتة للحوادث الأمنية

- بناء إجراءات استجابة تلقائية ومعايير التعامل مع الحوادث.
- تكامل الذكاء الاصطناعي مع أنظمة حماية نقاط النهاية.
- تطوير استراتيجيات دفاعية تعتمد على التنبؤ بالهجمات المستقبلية.
- تقليل زمن الاكتشاف وزمن الاستجابة للحوادث الأمنية.
- تحسين التنسيق بين الذكاء الاصطناعي والفرق البشرية في الاستجابة.

اليوم الخامس: استراتيجية التطبيق والتقييم

- وضع خارطة طريق لتطبيق الذكاء الاصطناعي في البنية الأمنية.
- تقييم الجاهزية المؤسسية والبنية التحتية التقنية.
- إدارة الجوانب الأخلاقية وحوكمة الخوارزميات والبيانات.
- قياس العائد الاستثماري في الأنظمة الذكية للأمن السيبراني.
- المشروع الختامي: تصميم نموذج أمني متكامل يعتمد على الذكاء الاصطناعي.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة عميقة حول دور الذكاء الاصطناعي في تطوير الأمن السيبراني.
- تعلم كيفية بناء أنظمة ذكية قادرة على التنبؤ بالتهديدات.
- تعزيز القدرة على الاستجابة للحوادث بسرعة وكفاءة.
- تطوير استراتيجيات استباقية تقلل المخاطر التشغيلية.
- تحسين دقة الكشف وتقليل معدلات الإنذارات الخاطئة.
- فهم المخاطر الأخلاقية والتنظيمية المرتبطة بتطبيق الذكاء الاصطناعي.
- استخدام التحليلات التنبؤية لاتخاذ قرارات أمنية أكثر دقة.
- بناء مرونة مؤسسية قادرة على مواجهة التهديدات الرقمية المستقبلية.

الخاتمة

يمثل الذكاء الاصطناعي في اكتشاف التهديدات والاستجابة لها نقلة نوعية في مفهوم الأمن السيبراني، إذ يتيح للمؤسسات الانتقال من الدفاع التفاعلي إلى الدفاع الذكي القائم على التحليل والتنبؤ.

من خلال هذه الدورة، يكتسب المشاركون الأدوات والاستراتيجيات العملية لتطبيق الذكاء الاصطناعي بفعالية داخل أنظمتهم الأمنية، مما يسهم في تعزيز الحماية، تقليل المخاطر، وتحقيق استقرار رقمي مستدام.

في عالم تتحول فيه التهديدات باستمرار، يصبح الاستثمار في الذكاء الاصطناعي الأمني ضرورة استراتيجية لضمان استمرارية الأعمال وحماية الأصول الرقمية على المدى الطويل.