الدورة التدريبية: الذكاء الاصطناعي في الأمن السيبراني ـ الكشف عن التهديدات والوقاية منها

#AI9394

الدورة التدريبية: الذكاء الاصطناعي في الأمن السيبراني ـ الكشف عن التهديدات والوقاية منها

مقدمة الدورة التدريبية / لمحة عامة:

يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة حول الذكاء الاصطناعي في الأمن السيبراني ـ الكشف عن التهديدات والوقاية منها، وهي مصممة للمتخصصين في الأمن السيبراني، ومهندسي الشبكات، ومحللي الأمن، ومسؤولي تكنولوجيا المعلومات، والباحثين الذين يسعون لـتعزيز قدراتهم في الدفاع ضد الهجمات السيبرانية باستخدام أحدث تقنيات الذكاء الاصطناعي (AI). في ظل التطور المستمر للتهديدات السيبرانية، لم تعد الأساليب التقليدية كافية لتوفير حماية شاملة. يوفر الذكاء الاصطناعي حلولاً مبتكرة لـاكتشاف الشذوذ (Anomaly Detection)، وتحليل السلوك (Behavioral Analysis)، والتنبؤ بالتهديدات (Threat Prediction)، والاستجابة للحوادث (Incident Response) بشكل أسرع وأكثر دقة. ستغطي الدورة مفاهيم أساسيات الأمن السيبراني، وكيفية تطبيق خوارزميات التعلم الآلي (Machine Learning) والتعلم العميق (Deep Learning) في تحليل البيانات الأمنية الضخمة (Big Security Data)، والكشف عن البرمجيات الخبيثة (Malware Detection)، واكتشاف التسلل (Intrusion Detection)، وتحليل الثغرات (Vulnerability Analysis). سيتعلم المشاركون كيفية توظيف أدوات وتقنيات الذكاء الاصطناعي لـبناء أنظمة دفاعية استباقية، وتحسين كفاءة العمليات الأمنية، وحماية الأصول الرقمية للمؤسسات. تهدف الدورة إلى تمكين المختصين من فهم إمكانات الذكاء الاصطناعي في مجال الأمن السيبراني، وتصميم وتنفيذ حلول أمنية ذكية وفعالة، والمساهمة في بناء بيئة رقمية أكثر أماناً. نستلهم في هذه الدورة من أعمال البروفيسور روبرت جراهام (Robert Graham)، Robert Graham، وهو خبير أمن سيبراني معروف ومؤلف، الذي يشدد على أهمية التطور المستمر في أدوات الأمن السيبراني لمواجهة التهديدات المتزايدة. ستقدم الدورة دراسات حالة واقعية لـهجمات سيبرانية وكيف يمكن للذكاء الاصطناعي أن يلعب دوراً حاسماً في اكتشافها والتصدي لها، مما يعزز فهم المشاركين للجوانب العملية والتطبيقية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصي الأمن السيبراني.
- محللي الأمن.
- مهندسي SOC/NOC.
- مسؤولي تكنولوجيا المعلومات.
- مهندسي الشبكات.
- مديري الأمن.
- المدققين الأمنيين.
- المطورين المهتمين بالأمن.
- الباحثين في الأمن السيبراني.
- أخصائيو الاستجابة للحوادث.

القطاعات والصناعات المستهدفة:

- تكنولوجيا المعلومات والاتصالات.
- الخدمات المالية والبنوك.
- القطاع الحكومي والدفاع.
- الرعاية الصحية.
- التعليم العالي.
- الطاقة والمرافق.
- التصنيع.
- التجارة الإلكترونية.
- شركات الأمن السيبراني.
- البحث والتطوير.

الأقسام المؤسسية المستهدفة:

- قسم الأمن السيبراني.
- قسم تكنولوجيا المعلومات.
- قسم إدارة المخاطر.
- قسم الامتثال.
- قسم تحليل البيانات.
- فريق الاستجابة للحوادث الأمنية.
- قسم البنية التحتية للشبكات.
- قسم البحث والتطوير.
- وحدات العمليات الأمنية (SOC).
- قسم تطوير البرمجيات (منظور الأمن).

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم العلاقة بين الذكاء الاصطناعي والأمن السيبراني.
- تحديد أنواع التهديدات السيبرانية التي يمكن للذكاء الاصطناعي معالجتها.
- تطبيق خوارزميات التعلم الآلي للكشف عن البرمجيات الخبيثة.
- استخدام الذكاء الاصطناعي لـاكتشاف التسلل السلوكي في الشبكات.
- تحليل البيانات الأمنية الضخمة باستخدام تقنيات الذكاء الاصطناعي.
- بناء نماذج تنبؤية للتهديدات السيبرانية المستقبلية.
- فهم دور الذكاء الاصطناعي في تحسين الاستجابة للحوادث الأمنية.
- تقييم أدوات ومنصات الذكاء الاصطناعي في الأمن السيبراني.
- تحديد التحديات الأخلاقية والقانونية لـتطبيق الذكاء الاصطناعي في الأمن.
- تصميم استراتيجيات أمنية متكاملة تعتمد على الذكاء الاصطناعي.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة على منهجية تدريبية تجمع بين المعرفة النظرية والتطبيق العملي، بهدف تزويد المشاركين بـالمهارات اللازمة لتوظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني. تشمل المنهجية محاضرات تفاعلية حول المفاهيم الأساسية للأمن السيبراني ومبادئ الذكاء الاصطناعي، تليها ورش عمل تطبيقية مكثفة. سيقوم المشاركون بـاستكشاف مجموعات بيانات أمنية حقيقية، وبناء وتدريب نماذج تعلم آلي لاكتشاف التهديدات، ومحاكاة سيناريوهات هجوم ودفاع باستخدام أدوات الذكاء الاصطناعي. سيتم التركيز على دراسات حالة واقعية لـهجمات سيبرانية معاصرة وكيف يمكن لـتقنيات الذكاء الاصطناعي أن تلعب دوراً حاسماً في اكتشافها والتصدي لها. تتضمن الدورة جلسات عمل جماعي لـتطوير حلول أمنية مبتكرة لمواجهة التحديات السيبرانية المتزايدة. يتلقى المشاركون تغذية راجعة مفصلة ومنتظمة من المدربين الخبراء لضمان تطوير مهاراتهم في هذا المجال الحاسم والمتطور.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني ومقدمة للذكاء الاصطناعي.

- مقدمة إلى الأمن السيبراني: المفاهيم والتهديدات.
- أنواع الهجمات السيبرانية الشائعة (Malware, Phishing, DoS).
- مقدمة إلى الذكاء الاصطناعي والتعلم الآلي.
- دور الذكاء الاصطناعي في تحديات الأمن السيبراني الحديثة.
- البيانات الضخمة (Big Data) في الأمن السيبراني.
- مبادئ حماية البيانات والخصوصية.
- الذكاء الاصطناعي كأداة هجومية ودفاعية.

الوحدة الثانية: اكتشاف البرمجيات الخبيثة وتحليلها بالذكاء الاصطناعي.

- أنواع البرمجيات الخبيثة (Viruses, Ransomware, Worms).
- أساليب اكتشاف البرمجيات الخبيثة التقليدية.
- تطبيقات التعلم الآلي في الكشف عن البرمجيات الخبيثة.
- تحليل السلوك (Behavioral Analysis) لكشف البرمجيات الخبيثة غير المعروفة.
- استخدام التعلم العميق (Deep Learning) في تحليل الملفات.
- جمع البيانات وتصنيفها لتدريب نماذج الكشف عن البرمجيات الخبيثة.
- تحديات وتطورات الذكاء الاصطناعي في مكافحة البرمجيات الخبيثة.

الوحدة الثالثة: الذكاء الاصطناعي في اكتشاف التسلل وتحليل الشبكات.

- مقدمة إلى أنظمة كشف التسلل (IDS) ومنع التسلل (IPS).
- الكشف عن التسلل القائم على التوقيع مقابل الكشف القائم على الشذوذ.
- تطبيق التعلم الآلي لاكتشاف الشذوذ في حركة مرور الشبكة.
- تحليل سجلات الشبكة (Log Analysis) باستخدام الذكاء الاصطناعي.
- تقنيات التعلم العميق للكشف عن التهديدات المتقدمة Persistent Threats).
- نمذجة السلوك الطبيعي للشبكة.
- الذكاء الاصطناعي لتحديد الثغرات الأمنية في الشبكات**.

الوحدة الرابعة: التنبؤ بالتهديدات والاستجابة للحوادث بالذكاء الاصطناعي.

- الذكاء الاصطناعي للتنبؤ بالتهديدات السيبرانية المستقبلية.
- الاستخبارات التهديدية (Threat Intelligence) المدعومة بالذكاء الاصطناعي.
- أتمتة الاستجابة للحوادث (Incident Response Automation) بالذكاء الاصطناعي.
- التحقيق الجنائي الرقمي (Digital Forensics) المدعم بالذكاء الاصطناعي.
- دور الذكاء الاصطناعي في إدارة الضعف (Vulnerability Management).
- الأمن الاستباقي (Proactive Security) باستخدام الذكاء الاصطناعي.
- دمج الذكاء الاصطناعي في مركز العمليات الأمنية (SOC).

الوحدة الخامسة: التحديات، الأخلاقيات، ومستقبل الذكاء الاصطناعي في الأمن السيبراني.

- التحديات التقنية في تطبيق الذكاء الاصطناعي على نطاق واسع.
- الهجمات العدائية على نماذج الذكاء الاصطناعي.
- أخلاقيات استخدام الذكاء الاصطناعي في المراقبة الأمنية.
- الخصوصية والشفافية في أنظمة الأمن المدعومة بالذكاء الاصطناعي.
- الامتثال القانوني والتنظيمي (GDPR, CCPA) في الأمن السيبراني.
- التطورات المستقبلية في الذكاء الاصطناعي والأمن السيبراني.
- الذكاء الاصطناعي كعامل تمكين (Enabler) للمجرمين السيبرانيين.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

في ظل السباق المستمر بين مطوري الذكاء الاصطناعي ومرتكبي الهجمات السيبرانية، كيف يمكننا ضمان أن استخدام الذكاء الاصطناعي في الدفاع السيبراني لا يؤدي إلى خلق "صندوق أسود" يزيد من تعقيد الأنظمة الأمنية ويصعب فهمها وتدقيقها، وبالتالي يزيد من المخاطر بدلاً من تقليلها؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتقديمها نهجاً شاملاً وتطبيقياً لتوظيف الذكاء الاصطناعي في الأمن السيبراني، وهو مجال حيوي وحرج في عصرنا الرقمي. ما يميزنا هو التركيز على الاستراتيجيات المتقدمة للكشف عن التهديدات والوقاية منها** باستخدام أحدث تقنيات الذكاء الاصطناعي والتعلم الآلي والتعلم العميق. نغطي مجموعة واسعة من تطبيقات الذكاء الاصطناعي في الأمن، من اكتشاف البرمجيات الخبيثة وتحليل الشبكات إلى التنبؤ بالتهديدات وأتمتة الاستجابة للحوادث. الدورة تركز على تزويد المشاركين بالمهارات اللازمة لبناء دفاعات سيبرانية قوية وذكية، وتحليل البيانات الأمنية بكفاءة، والمساهمة بفعالية في حماية الأصول الرقمية، مما يجعلها ضرورية لأي محترف يسعى لتعزيز قدراته في مواجهة التحديات السيبرانية المتزايدة.