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

مايو ٢٠٢٦ ٠٧ - ٠٣

عمان

(للشخص الواحد) € ٤١٠٠

Ref: #AI9394_53126

## مقدمة الدورة التدريبية / لمحة عامة:

والوقاية منها، التدريبية المتخصصة حول الذكاء الاصطناعي في الأمن يقدم BIG BEN Training Center هذه الدورة الأمن، ومسؤولي تكنولوجيا وهي مصممة للمتخصصين في الأمن السيبراني، ومهندسي السيبراني - الكشف عن التهديدات في الدفاع ضد الهجمات السيبرانية باستخدام أحدث المعلومات، والباحثين الذين يسعون لتعزيز قدراتهم الشبكات، ومحللي حماية شاملة. يوفر الذكاء المستمر للتهديدات السيبرانية، لم تعد الأساليب تقنيات الذكاء الاصطناعي ( .(AIفي ظل التطور Behavioral، وتحليل السلوك ((Anomaly Detection الاصطناعي حلولاً مبتكرة لاكتشاف الشذوذ التقليدية كافية لتوفير وأكثر دقة. ستغطي الدورة (Incident Response، والاستجابة للحوادث ((Threat Predictionبالتهديدات ( ، والتنبؤ(Analysis في تحليل خوارزميات التعلم الآلي ((Machine Learning مفاهيم أساسيات الأمن السيبراني، وكيفية تطبيق بشكل أسرع والكشف عن البرمجيات الخبيثة (Malware) البيانات الأمنية الضخمة (Big Security Data)، والتعلم العميق (Deep Learning) توظيف أدوات سيتعلم .(Vulnerability Analysis، وتحليل الثغرات ((Intrusion Detection، واكتشاف التسلل ((Detection تمكين استباقية، وتحسين كفاءة العمليات الأمنية، وحماية وتقنيات الذكاء الاصطناعي لبناء أنظمة دفاعية المشاركون كيفية حلول أمنية ذكية المختصين من فهم إمكانات الذكاء الاصطناعي في مجال الأصول الرقمية للمؤسسات. تهدف الدورة إلى بيئة رقمية أكثر أماناً. الأمن السيبراني، وتصميم وتنفيذ

Robert Graham، (Robert ، وهو نستلهم في هذه الدورة من أعمال البروفيسور روبرت وفعالة، والمساهمة في بناء أهمية التطور المستمر في أدوات الأمن السيبراني خبير أمن سيبراني معروف ومؤلف، الذي يشدد على جراهام (Graham في اكتشافها حالة واقعية لـهجمات سيبرانية وكيف يمكن للذكاء لمواجهة التهديدات المتزايدة. ستقدم الدورة دراسات العملية والتطبيقية. والتصدي لها، مما يعزز فهم المشاركين للجوانب الاصطناعي أن يلعب دوراً حاسماً

## لـ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

## منهجية الدورة التدريبية:

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

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

## للذكاء الاصطناعي. الوحدة الأولى: أساسيات الأمن السيبراني ومقدمة

- 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**.

## للحوادث بالذكاء الاصطناعي. الوحدة الرابعة: التنبؤ بالتهديدات والاستجابة

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

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

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

## الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية.ا راحة وأنشطة تفاعلية،ا ليصل إجمالي

## سؤال للتأمل:

السيبراني لا ومرتكبي الهجمات السيبرانية، كيف يمكننا ضمان أن في ظل السباق المستمر بين مطوري الذكاء الاصطناعي

وتدقيقها، وبالتالي يزيد من يؤدي إلى خلق "صندوق أسود" يزيد من تعقيد الأنظمة استخدام الذكاء الاصطناعي في الدفاع

المخاطر بدلاً من تقليلها؟ الأمنية ويصعب فهمها

## ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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