



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

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

القاهرة - \*

(للشخص الواحد) € ٤١٠٠

Ref: #AI9394\_559582



## 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، ومحلي حماية شاملة. يوفر الذكاء المستمر للتهديدات السيبرانية، لم تعد الأساليب تقنيات الذكاء الاصطناعي (AI) في ظل التطور Behavioral) وتحليل السلوك ((Anomaly Detection) الاصطناعي حلولاً مبتكرة لاكتشاف الشذوذ التقليدية كافية لتوفير وأكثر دقة. ستغطي الدورة ((Incident Response) والاستجابة للحوادث ((Threat Prediction) التهديدات (، 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 التسلسل ((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، 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 (Robert Graham) في اكتشافها حالة واقعية لهجمات سيبرانية وكيف يمكن للذكاء لمواجهة التهديدات المتزايدة. ستقدم الدورة دراسات العملية والتطبيقية والتصدي لها، مما يعزز فهم المشاركين للجوانب الاصطناعي أن يلعب دوراً حاسماً



## لأ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- متخصصي الأمن السيبراني.
- مطلبي الأمن.
- مهندسي SOC/NOCC.
- 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 المؤسسة 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



- السبراني، فهم العلاقة بين الذكاء الاصطناعي والأمن
- الاصطناعي معالجتها، تحديد أنواع التهديدات السبرانية التي يمكن للذكاء
- الخبيثة، تطبيق خوارزميات التعلم الآلي للكشف عن البرمجيات
- في الشبكات، استخدام الذكاء الاصطناعي لاكتشاف التسلسل السلوكي
- الذكاء الاصطناعي، تحليل البيانات الأمنية الضخمة باستخدام تقنيات
- المستقبلية، بناء نماذج تنبؤية للتهديدات السبرانية
- للحوادث الأمنية، فهم دور الذكاء الاصطناعي في تحسين الاستجابة
- السبراني، تقييم أدوات ومنصات الذكاء الاصطناعي في الأمن
- الذكاء الاصطناعي في الأمن، تحديد التحديات الأخلاقية والقانونية لتطبيق
- 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 حلولاً أمنية مبتكرة لمواجهة التحديات السيبرانية والتصدي في هذا المجال الحاسم والمتطوراً 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<sup>١</sup>.
- (Phishing, DoS) أنواع الهجمات السيبرانية الشائعة (Malware)<sup>١</sup>.
- مقدمة إلى الذكاء الاصطناعي والتعلم الآلي<sup>١</sup>.
- الحديثة<sup>١</sup> دور الذكاء الاصطناعي في تحديات الأمن السيبراني.
- البيانات الضخمة (Big Data) في الأمن السيبراني<sup>١</sup>.
- مبادئ حماية البيانات والخصوصية<sup>١</sup>.
- الذكاء الاصطناعي كأداة هجومية ودفاعية<sup>١</sup>.

## بالذكاء الاصطناعي<sup>١</sup>. الوحدة الثانية: اكتشاف البرمجيات الخبيثة وتحليلها

- (Worms) أنواع البرمجيات الخبيثة (Viruses, Ransomware)<sup>١</sup>.
- أساليب اكتشاف البرمجيات الخبيثة التقليدية<sup>١</sup>.
- الخبيثة<sup>١</sup> تطبيقات التعلم الآلي في الكشف عن البرمجيات.
- البرمجيات الخبيثة غير المعروفة<sup>١</sup> تحليل السلوك (Behavioral Analysis) لكشف.
- الملفات<sup>١</sup> استخدام التعلم العميق (Deep Learning) في تحليل.
- البرمجيات الخبيثة<sup>١</sup> جمع البيانات وتصنيفها لتدريب نماذج الكشف عن.
- البرمجيات الخبيثة<sup>١</sup> تحديات وتطورات الذكاء الاصطناعي في مكافحة.

## وتحليل الشبكات<sup>١</sup>. الوحدة الثالثة: الذكاء الاصطناعي في اكتشاف التسلسل

- (IPS) مقدمة إلى أنظمة كشف التسلسل (IDS) ومنع التسلسل.
- القائم على الشذوذ<sup>١</sup> الكشف عن التسلسل القائم على التوقيع مقابل الكشف.
- الشبكة<sup>١</sup> تطبيق التعلم الآلي لاكتشاف الشذوذ في حركة مرور.
- الذكاء الاصطناعي<sup>١</sup> تحليل سجلات الشبكة (Log Analysis) باستخدام.
- (Persistent Threats) تقنيات التعلم العميق للكشف عن التهديدات المتقدمة.
- نمذجة السلوك الطبيعي للشبكة<sup>١</sup>.
- الشبكات<sup>١</sup> الذكاء الاصطناعي لتحديد الثغرات الأمنية في.



## 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،
- الأمن، 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، راحة وأنشطة تفاعلية، 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 ودرج في عصرنا الرقمي. نغطي مجموعة واسعة من تطبيقات 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، ضرورة لأي محترف يسعى لتعزيز قدراته في مواجهة بفعالية في حماية الأصول الرقمية،