الدورة التدريبية: تحليل البيانات لتقييم المخاطر السيبرانية وحماية الأنظمة



26 - 30 اكتوبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #DM6951_348638

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التهديدات السيبرانية المتزايدة والمتطورة، أصبحت القدرة على تحليل البيانات بفعالية لتقييم المخاطر السيبرانية وحماية الأصول الرقمية أمراً حيوياً للمؤسسات من جميع الأحجام والقطاعات. لم يعد الأمن السيبراني مجرد مسألة دفاعية، بل هو جانب استراتيجي يعتمد على البيانات للتنبؤ بالتهديدات، اكتشاف الاختراقات، والاستجابة للحوادث بفعالية. بدون تحليل بيانات قوي، قد تظل المؤسسات عرضة للهجمات السيبرانية المدمرة التي يمكن أن تؤدي إلى خسائر مالية فادحة، الإضرار بالسمعة، وتسرب البيانات الحساسة. تهدف هذه الدورة التدريبية من BIG BEN Training Center إلى تزويد المهنيين بالمعرفة والمهارات اللازمة لتسخير قوة تحليل البيانات لتقييم المخاطر السيبرانية، وتحديد نقاط الضعف، وتحسين الدفاعات الأمنية. ستتناول الدورة المفاهيم الأساسية لأمن المعلومات، أنواع البيانات الأمنية، أدوات وتقنيات جمع البيانات الأمنية وتحليلها، كيفية استخدام التحليلات الإحصائية والتعلم الآلي لاكتشاف الشذوذ والتنبؤ بالهجمات، وإدارة الاستجابة للحوادث بناءً على البيانات. تستند الدورة إلى رؤى أكاديمية وعملية من خبراء مرموقين في الأمن السيبراني وتحليل البيانات، مثل Bruce Schneier (بروس شناير)، وهو خبير عالمي مشهور في الأمن السيبراني والتشفير يركز على أهمية تحليل البيانات لفهم المخاطر الأمنية واتخاذ قرارات استراتيجية، مما يضمن محتوى غنياً بالمعرفة النظرية والتطبيقية. ستمكن هذه الدورة المتدربين من بناء دفاعات سيبرانية قوية ومرنة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- محللو الأمن السيبراني.
- مهندسو الأمن السيبراني.
- محللو المخاطر الأمنية.
- مديرو أمن المعلومات (CISO).
- مديرو تكنولوجيا المعلومات.
- مدققو الأمن.
- محللو العمليات الأمنية (SOC Analysts).
- أي مهني يعمل في مجال أمن المعلومات.

القطاعات والصناعات المستهدفة:

- الخدمات المالية.
- التكنولوجيا والبرمجيات.
- الحكومة والدفاع.
- الرعاية الصحية.
- الاتصالات.
- التصنيع.
- الطاقة والمرافق.
- القطاع الحكومي وما في حكمه.

الأقسام المؤسسية المستهدفة:

- الأمن السيبراني.
- تكنولوجيا المعلومات.
- إدارة المخاطر.
- الامتثال.
- العمليات الأمنية.
- التحقيقات الرقمية.
- حوكمة تكنولوجيا المعلومات.
- الاستجابة للحوادث.

أهداف الدورة التدريبية:

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

- فهم العلاقة بين تحليل البيانات وتقييم المخاطر السيبرانية.
- تحديد أنواع البيانات الأمنية ومصادرها.
- جمع وتنظيف وإعداد البيانات الأمنية للتحليل.
- تطبيق تقنيات التحليل الإحصائي لكشف الشذوذ.
- استخدام أدوات تحليل البيانات لتحليل السجلات الأمنية.
- بناء نماذج تنبؤية للهجمات السيبرانية.
- تطبيق التعلم الآلي لاكتشاف التهديدات.
- تقييم نقاط الضعف والثغرات الأمنية بناءً على البيانات.
- تطوير تقارير المخاطر السيبرانية ولوحات المعلومات.
- اتخاذ قرارات مستنيرة لتعزيز الأمن السيبراني.

منهجية الدورة التدريبية:

تتبنى هذه الدورة التدريبية منهجية عملية وتطبيقية، مصممة لتمكين المشاركين من تحليل البيانات بفعالية لتقييم المخاطر السيبرانية. يتم تقديم المحتوى من خلال مزيج من المحاضرات التفاعلية، التي تشرح المفاهيم الأساسية لأمن البيانات، المخاطر السيبرانية، والتحليلات الأمنية، وورش العمل التطبيقية المكثفة التي تتيح للمشاركين العمل مباشرة على سيناريوهات بيانات أمنية حقيقية. سيقوم المتدربون بجمع السجلات الأمنية من أنظمة مختلفة، وتنظيفها، وتحليلها باستخدام أدوات شائعة، وتحديد الأنماط المشبوهة، وتطبيق خوارزميات التعلم الآلي لكشف الاختراقات، وإنشاء تقارير مخاطر واضحة. يعزز العمل الجماعي مهارات التعاون وتبادل الخبرات في معالجة تحديات المخاطر السيبرانية الواقعية، بينما تتيح الجلسات التفاعلية فرصة لطرح الأسئلة وتلقي تغذية راجعة من المدربين الخبراء. يحرص BIG BEN Training Center على توفير بيئة تعليمية غنية بالأمثلة ودراسات الحالة من حوادث أمنية حقيقية، لضمان اكتساب المتدربين خبرة عملية مباشرة في تسخير البيانات لتعزيز الدفاعات السيبرانية لمؤسساتهم.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات المخاطر السيبرانية والبيانات الأمنية.

- مقدمة إلى المخاطر السيبرانية وأنواعها.
- إطار عمل الأمن السيبراني (NIST, ISO 27001).
- مفهوم البيانات الأمنية ومصادرها (سجلات النظام، الشبكة، التطبيقات).
- تأثير البيانات على تقييم المخاطر والاستجابة للحوادث.
- نماذج التهديد ونقاط الضعف.
- أهمية جودة البيانات الأمنية.
- أمثلة على الهجمات السيبرانية وكيفية تحليل بياناتها.

الوحدة الثانية: جمع وتجهيز البيانات للتحليل الأمني.

- تقنيات جمع البيانات الأمنية (SIEM, EDR, IDS/IPS).
- تنظيف البيانات الأمنية وتوحيدها.
- إثراء البيانات الأمنية (Threat Intelligence).
- نمذجة البيانات للتحليل الأمني.
- التعامل مع البيانات الضخمة الأمنية.
- أدوات إدارة السجلات (Log Management Tools).
- تحديات خصوصية البيانات وأمنها.

الوحدة الثالثة: التحليل الإحصائي واكتشاف الشذوذ في البيانات الأمنية.

- مقدمة إلى التحليل الإحصائي في الأمن السيبراني.
- مقاييس الاتجاه المركزي والتشتت للبيانات الأمنية.
- تحديد القيم الشاذة (Anomalies) والأنماط غير الطبيعية.
- استخدام الرسوم البيانية لتصور البيانات الأمنية.
- تطبيق الاختبارات الإحصائية لكشف التهديدات.
- تحليل الاتجاهات والتنبؤ بالهجمات.
- ورشة عمل: اكتشاف الشذوذ في سجلات الشبكة.

الوحدة الرابعة: التعلم الآلي والذكاء الاصطناعي للأمن السيبراني.

- مقدمة إلى التعلم الآلي (Machine Learning) في الأمن السيبراني.
- أنواع خوارزميات التعلم الآلي (تصنيف، تجميع، انحدار).
- تطبيق التعلم الآلي لكشف البرامج الضارة (Malware Detection).
- كشف الاختراقات (Intrusion Detection) باستخدام الذكاء الاصطناعي.
- تحليل السلوك (Behavioral Analytics) لكشف التهديدات الداخلية.
- بناء نماذج التعلم الآلي للأمن.
- التعامل مع تحديات النماذج الزائفة (False Positives/Negatives).

الوحدة الخامسة: إدارة المخاطر السيبرانية والتوجهات المستقبلية.

- بناء تقارير المخاطر السيبرانية ولوحات المعلومات.
- تقييم المخاطر وتصنيفها بناءً على البيانات.
- استراتيجيات التخفيف من المخاطر.
- الاستجابة للحوادث (Incident Response) المدفوعة بالبيانات.
- دور التحقيقات الرقمية (Digital Forensics).
- الاتجاهات المستقبلية في التهديدات السيبرانية والتحليلات الأمنية.
- بناء برنامج أمن سيبراني قائم على البيانات.

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 عالم تتسارع فيه وتيرة التهديدات السيبرانية وتتزايد فيه أحجام البيانات الأمنية، كيف يمكن للمؤسسات أن تتحول من مجرد الاستجابة للهجمات إلى بناء دفاعات استباقية تستند إلى التحليلات العميقة للبيانات، مما يمكنها من التنبؤ بالمخاطر، اكتشاف الشذوذ، والاستجابة بذكاء للحوادث، وبالتالي تحقيق مستوى غير مسبوق من المرونة السيبرانية وحماية الأصول الأكثر قيمة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتركيزها العملي والشامل على تحليل البيانات لتقييم المخاطر السيبرانية، مما يوفر للمشاركين فهماً عميقاً لكيفية تسخير قوة البيانات لتعزيز الدفاعات الأمنية. يقدم BIG BEN Training Center محتوى متقدماً يغطي جميع جوانب الأمن السيبراني المدفوع بالبيانات، من جمع البيانات الأمنية وإعدادها إلى تطبيق التحليلات الإحصائية والتعلم الآلي لاكتشاف التهديدات والتنبؤ بالهجمات، مع التركيز على الأمثلة العملية ودراسات الحالة من حوادث أمنية حقيقية. تبرز الدورة بتوفيرها لورش عمل تطبيقية مكثفة تتيح للمشاركين تحليل سجلات أمنية، وتحديد الأنماط المشبوهة، وتطبيق خوارزميات التعلم الآلي لكشف الاختراقات، مما يضمن اكتسابهم خبرة مباشرة في تطبيق المفاهيم النظرية. هذا النهج المتكامل يضمن أن يكتسب المتدربون ليس فقط المعرفة العميقة، بل أيضاً الكفاءات العملية اللازمة ليصبحوا قادة في الأمن السيبراني، قادرين على بناء دفاعات قوية ومرنة لمؤسساتهم.