الدورة التدريبية: الأمن السيبراني وحماية البيانات في مشاريع ذكاء الأعمال



21 - 25 ديسمبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #BUI7826_424867

مقدمة الدورة التدريبية / لمحة عامة:

يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة في الأمن السيبراني وحماية البيانات في مشاريع ذكاء الأعمال. في عصر البيانات الضخمة والتحليلات المتقدمة، أصبحت حماية المعلومات الحساسة أمرًا بالغ الأهمية لـ الاستمرارية التشغيلية والسمعة المؤسسية. مع تزايد التهديدات السيبرانية والمتطلبات التنظيمية المتعلقة بـ خصوصية البيانات، لم يعد كافيًا مجرد جمع وتحليل البيانات، بل يجب ضمان أمنها وسلامتها في جميع مراحل دورة حياتها. ستركز هذه الدورة على تزويد المشاركين بـ المهارات والمعرفة اللازمة لـ تحديد المخاطر الأمنية، وتطبيق أفضل ممارسات الحماية، والامتثال للوائح حماية البيانات (مثل GDPR وCCPA) ضمن مشاريع ذكاء الأعمال. تستند الدورة إلى أحدث الأطر والمعايير العالمية في الأمن السيبراني وحوكمة البيانات، مستلهمة من أعمال خبراء مثل البروفيسور ويليام إدوارد ديمينغ (W. Edwards Deming)، الذي أسس مفاهيم إدارة الجودة الشاملة التي يمكن تطبيقها على أمن البيانات. تهدف هذه الدورة إلى تمكين المختصين من بناء حلول ذكاء أعمال آمنة، مما يحمي الأصول المعلوماتية ويدعم اتخاذ القرارات بثقة ومسؤولية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء مشاريع ذكاء الأعمال.
- محللو البيانات.
- مهندسو البيانات.
- مدراء أمن المعلومات.
- متخصصو الامتثال والتدقيق.
- مدراء تقنية المعلومات.
- مدراء المنتجات الذين يتعاملون مع البيانات.
- أي شخص مسؤول عن التعامل مع البيانات الحساسة.

القطاعات والصناعات المستهدفة:

- الخدمات المالية.
- الرعاية الصحية.
- الاتصالات.
- الجهات الحكومية وما في حكمها.
- التكنولوجيا.
- التجزئة والتجارة الإلكترونية.
- الطاقة.
- الاستشارات الأمنية.

الأقسام المؤسسية المستهدفة:

- ذكاء الأعمال.
- أمن المعلومات.
- تقنية المعلومات.
- الامتثال والتدقيق.
- القسم القانوني.
- إدارة المخاطر.
- العمليات.
- إدارة المشاريع.

أهداف الدورة التدريبية:

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

- فهم التهديدات السيبرانية لـ بيئات ذكاء الأعمال.
- تطبيق مبادئ حماية البيانات والخصوصية.
- تحديد الثغرات الأمنية في نظم البيانات.
- تطوير استراتيجيات أمنية لـ مشاريع ذكاء الأعمال.
- الامتثال للوائح حماية البيانات العالمية والمحلية.
- إدارة الوصول وصلاحيات المستخدمين.
- تأمين البنية التحتية لـ ذكاء الأعمال.
- الاستجابة للحوادث الأمنية المتعلقة بالبيانات.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية تجمع بين المفاهيم النظرية المتقدمة والتطبيقات العملية المكثفة، لتمكين المشاركين من تأمين مشاريع ذكاء الأعمال بفعالية. تبدأ الدورة بـ محاضرات تفاعلية تستعرض أهمية الأمن السيبراني وحماية البيانات في سياق التحليلات. سيتم التركيز على ورش العمل العملية، حيث يقوم المتدربون بـ تحليل سيناريوهات أمنية واقعية، وتطبيق أدوات وتقنيات الحماية، وتقييم المخاطر المحتملة في نظم البيانات. تتضمن الدورة دراسات حالة مفصلة لـ انتهاكات البيانات وكيف يمكن لـ الاستراتيجيات الأمنية السليمة أن تمنعها. بالإضافة إلى ذلك، سيتم تشجيع المناقشات الجماعية لـ تبادل الخبرات حول أفضل الممارسات الأمنية، وجلسات التغذية الراجعة لـ تطوير فهم شامل للموضوع. تهدف هذه المنهجية إلى تزويد المشاركين بـ الخبرات العملية والرؤى الاستراتيجية اللازمة لـ بناء حلول ذكاء أعمال آمنة وموثوقة، مما يحمي الأصول المعلوماتية للمؤسسة ويعزز الثقة في البيانات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني وحماية البيانات في سياق ذكاء الأعمال

- مقدمة إلى الأمن السيبراني وأهميته.
- مفاهيم حماية البيانات والخصوصية.
- التهديدات السيبرانية الشائعة على نظم البيانات.
- مبادئ أمن المعلومات (السرية، التكامل، التوافر).
- مخاطر البيانات في مشاريع ذكاء الأعمال.
- أهمية حوكمة البيانات.
- الفرق بين الأمن السيبراني وأمن البيانات.

الوحدة الثانية: لوائح حماية البيانات والامتثال

- مقدمة إلى اللوائح العالمية لحماية البيانات (GDPR، CCPA).
- متطلبات الامتثال لـ مشاريع ذكاء الأعمال.
- تأثير اللوائح على جمع البيانات واستخدامها.
- أفضل الممارسات لـ ضمان الامتثال.
- تحديد البيانات الحساسة وإدارتها.
- دور مسؤول حماية البيانات (DPO).
- دراسة حالة عن الامتثال للوائح.

الوحدة الثالثة: تأمين بنية البيانات التحتية

- تأمين قواعد البيانات ومستودعات البيانات.
- حماية البيانات أثناء النقل وفي وضع السكون.
- إدارة الوصول والتحكم في الصلاحيات.
- تشفير البيانات وإخفاء الهوية.
- تأمين منصات الحوسبة السحابية لـ ذكاء الأعمال.
- مراقبة الأمن واكتشاف التهديدات.
- أدوات وتقنيات لـ تأمين البيانات.

الوحدة الرابعة: إدارة المخاطر والاستجابة للحوادث

- تحديد المخاطر الأمنية وتقييمها.
- وضع خطط الاستجابة للحوادث الأمنية.
- استعادة البيانات بعد الحوادث.
- التحقيق في الحوادث الأمنية.
- بناء فريق استجابة للحوادث.
- اختبار الاختراق والتقييم الأمني.
- التوعية الأمنية وتدريب الموظفين.

الوحدة الخامسة: مستقبل أمن البيانات في ذكاء الأعمال

- الذكاء الاصطناعي والأمن السيبراني.
- تأمين البيانات الضخمة وإنترنت الأشياء (IoT).
- التشفير الكمي وتحدياته.
- أخلاقيات استخدام البيانات والخصوصية.
- التهديدات الناشئة والتصدي لها.
- بناء ثقافة أمنية في المؤسسة.
- التوجهات المستقبلية في حماية 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 ظل التطور المتسارع للتهديدات السيبرانية وتزايد حجم البيانات، كيف يمكن للمؤسسات تحقيق التوازن بين الحاجة الماسة لـ تحليل البيانات واستخلاص الرؤى، وبين ضمان أقصى درجات الأمن والخصوصية لـ معلومات عملائها؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المزدوج على الأمن السيبراني وحماية البيانات، مع تطبيق خاص على مشاريع ذكاء الأعمال، مما يوفر رؤى شاملة وحلولاً عملية لا تتوفر في الدورات المنفصلة. نحن لا نكتفي بتقديم المفاهيم العامة، بل نغوص في التحديات الأمنية المحددة التي تواجه فرق ذكاء الأعمال، ونقدم استراتيجيات فعالة لـ تأمين البيانات من المصدر وحتى العرض. ما يميزنا هو دمج أحدث لوائح حماية البيانات مع أفضل الممارسات الأمنية، مما يضمن أن يمتلك المشاركون المعرفة اللازمة لـ الامتثال وبناء نظم بيانات موثوقة. يتميز المحتوى الأكاديمي للدورة بتعمقه في تقنيات التشفير، وإدارة الوصول، والاستجابة للحوادث، مما يضمن أن يكتسب المتدربون مهارات عملية لـ حماية الأصول المعلوماتية الأكثر قيمة. هذه الدورة ليست مجرد تدريب، بل هي استثمار استراتيجي في مرونة المؤسسة وسمعتها، وتمكينها من الاستفادة من البيانات بأمان وثقة.