ذكاء الأعمال الدورة التدريبية: الأمن السيبراني وحماية البيانات في مشاريع

يونيو ٢٠٢٦ ١٢ - ٠٨

الدار البيضاء

(للشخص الواحد) € ٤١٠٠

Ref: #BUI7826_579731

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

- 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:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

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

- 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 ـ مشاريع ذكاء الأعمال.
- تأثير اللوائح على جمع البيانات واستخدامها.
- أفضل الممارسات ـ 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.

الأعمال الوحدة الخامسة: مستقبل أمن البيانات في ذكاء

- 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:

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:

الرؤى، حجم البيانات، كيف يمكن للمؤسسات تحقيق التوازن بين في ظل التطور المتسارع للتهديدات السيبرانية وتزايد

عملائها؟ وبين ضمان أقصى درجات الأمن والخصوصية لـ معلومات الحاجة الماسة لـ تحليل البيانات واستخلاص

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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