الدورة التدريبية: الأمن السيبراني للمقاولات والهندسة: حماية التصاميم والبيانات الهندسية



16 - 20 نوفمبر 2026

مدريد

5900 € (للشخص الواحد)

Ref: #CYB1147_328340

مقدمة الدورة التدريبية / لمحة عامة:

في قطاعي المقاولات والهندسة، تُعد التصاميم الهندسية، البيانات الفنية، والبيانات التشغيلية للمشاريع أصولًا رقمية ذات قيمة استراتيجية عالية. إن أي اختراق أمني لهذه البيانات يمكن أن يؤدي إلى سرقة الملكية الفكرية، وتسرب أسرار تجارية، وتأخير في تسليم المشاريع، مما يسبب خسائر مالية فادحة وإضرارًا بالسمعة. مع تزايد الاعتماد على التقنيات الرقمية والنمذجة ثلاثية الأبعاد (BIM) والتحكم عن بُعد في المشاريع، أصبحت حماية البيانات الهندسية تحديًا بالغ الأهمية. تقدم هذه الدورة التدريبية المتخصصة للمهندسين، مديري المشاريع، ومتخصصي الأمن، المعرفة والمهارات اللازمة لتأمين البيانات الهندسية من التهديدات السيبرانية. سنتناول في هذه الدورة مفاهيم الأمن السيبراني المخصصة للقطاع، التهديدات الشائعة، واستراتيجيات الحماية. سيكتسب المشاركون القدرة على تحديد نقاط الضعف، تطبيق ضوابط أمنية قوية، ووضع سياسات متكاملة لحماية أصولهم الرقمية. تهدف الدورة إلى بناء كوادر متخصصة في الأمن الهندسي، مما يضمن أن المؤسسات في هذا القطاع تكون دائمًا في طليعة الدفاع. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور ويليام إم. بارون (William M. Baron)، المعروف بأعماله في أمن البنية التحتية الهندسية. يقدم BIG BEN Training Center هذه الدورة لتمكين قادة المقاولات من بناء بيئة عمل آمنة وموثوقة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المهندسون المعماريون والمدنيون.
- مديرو المشاريع الإنشائية.
- متخصصو أمن المعلومات.
- القيادات التقنية في شركات المقاولات.
- مهندسو النمذجة (BIM).
- المستشارون في الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- قطاع المقاولات والبناء.
- شركات الهندسة المعمارية والمدنية.
- الجهات الحكومية وما في حكمها المسؤولة عن المشاريع.
- قطاع البنية التحتية.
- شركات تطوير العقارات.

الأقسام المؤسسية المستهدفة:

إدارة المشاريع.
إدارة التصميم الهندسي.
إدارة تكنولوجيا المعلومات.
إدارة الأمن السيبراني.
الإدارة القانونية.

أهداف الدورة التدريبية:

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

- فهم التهديدات السيبرانية التي تواجه قطاع المقاولات.
- القدرة على تأمين التصاميم الهندسية والبيانات الحساسة.
- حماية الملكية الفكرية والأسرار التجارية.
- تطبيق ضوابط أمنية على أنظمة النمذجة (BIM) وCAD.
- وضع سياسات للتحكم في الوصول إلى البيانات الهندسية.
- الاستجابة للحوادث الأمنية في المشاريع.
- الامتثال للمعايير واللوائح الخاصة بالقطاع.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وتفاعلية، مصممة لتمكين المشاركين من فهم وتطبيق إجراءات الأمن السيبراني في بيئة العمل الهندسية. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لانتهاكات أمنية في مشاريع كبرى، وورش العمل التطبيقية، من ممارسة تأمين البيانات وتقييم المخاطر. تتضمن المنهجية مناقشات متعمقة حول الفرق بين أمن البيانات في المكاتب والمواقع، والتحديات الأمنية للتعاون مع المقاولين الفرعيين. سيتم التركيز على الجانب الاستباقي للأمن، وتشجيع المشاركين على التفكير في كيفية حماية أصولهم من التهديدات. يقدم BIG BEN Training Center هذه الدورة لتعزيز الوعي الأمني والخبرة لدى العاملين في هذا القطاع الحيوي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني في قطاع المقاولات والهندسة

- التهديدات السيبرانية التي تواجه المشاريع.
- أصول البيانات الهندسية وكيفية حمايتها.
- الفرق بين أمن المعلومات وأمن المشروع.
- الامتثال للوائح الأمنية.
- أهمية حماية الملكية الفكرية.
- بناء ثقافة أمنية في فرق العمل.
- الوعي بأدوات وتقنيات الهجوم.

الوحدة الثانية: تأمين التصاميم والبيانات الهندسية

- أمن أنظمة النمذجة (BIM) وCAD.
- تشفير البيانات أثناء النقل والتخزين.
- إدارة التحكم في الوصول إلى الملفات.
- أفضل الممارسات لحماية البيانات على السحابة.
- النسخ الاحتياطي والتعافي من الكوارث.
- حماية البيانات من التعديل غير المصرح به.
- أمن البرامج المستخدمة في التصميم.

الوحدة الثالثة: حماية الشبكات والأجهزة في المشاريع

- تأمين شبكات المواقع الإنشائية.
- حماية الأجهزة الطرفية (أجهزة الكمبيوتر، اللوحات الذكية).
- أمن الاتصالات اللاسلكية في الموقع.
- إدارة الثغرات الأمنية للأجهزة.
- تأمين أجهزة إنترنت الأشياء (IoT) في المشاريع.
- التحكم في وصول المقاولين الفرعيين للشبكة.
- مراقبة الشبكة وكشف الاختراقات.

الوحدة الرابعة: حوكمة الأمن وإدارة المخاطر

- وضع سياسات أمنية متكاملة للمشروع.
- إدارة المخاطر السيبرانية في مراحل المشروع.
- تقييم الموردين والمقاولين من ناحية الأمان.
- بناء خطة للاستجابة للحوادث الأمنية.
- التحقيق في الحوادث الأمنية في المشاريع.
- التدريب على الوعي الأمني للموظفين.
- التأمين ضد المخاطر السيبرانية.

الوحدة الخامسة: مستقبل الأمن في المقاولات والهندسة

- أمن الأتمتة والروبوتات في البناء.
- تأثير الذكاء الاصطناعي على الأمن.
- أمن البيانات في المشاريع الضخمة.
- استراتيجيات الأمن الاستباقي.
- دمج الأمن في تصميم المشروع.
- المرونة السيبرانية واستمرارية الأعمال.
- التطور المستقبلي لأمن البيانات الهندسية.

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 الاعتماد المتزايد على الرقمنة في قطاع المقاولات والهندسة، كيف يمكن للمؤسسات أن تبتكر إطار عمل أمني لا يقتصر على حماية التصاميم فحسب، بل يُنشئ نظامًا بيئيًا آمنًا للبيانات، ويضمن سلامة التعاون مع الشركاء، ويُمكّن المؤسسة من الاستجابة بفعالية للأزمات مع الحفاظ على التقدم المستمر في المشاريع؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص على الأمن السيبراني لقطاع المقاولات والهندسة، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية الفريدة في هذا المجال. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لتأمين التصاميم الهندسية، وحماية الملكية الفكرية، ووضع استراتيجيات متكاملة للبيانات الهندسية الحساسة. تقدم الدورة دراسات حالة واقعية لانتهاكات أمنية في مشاريع كبرى، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الترابط بين الجوانب الأمنية والإدارية للمشروع والاستراتيجيات الاستباقية للأمن، مما يضمن أن المشاركين سيخرجون بخبرة عملية قابلة للتطبيق. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في الأمن السيبراني قادرين على حماية مستقبل الصناعة.