الدورة التدريبية: الأمن السيبراني للمقاولات

حماية التصاميم والبيانات الهندسية

والهندسة:

Ref: #CYB1147

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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.
- المشاريع الجهات الحكومية وما في حكمها المسؤولة عن
- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

المقاولات والهندسة الوحدة الأولى: أساسيات الأمن السيبراني في قطاع

- 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) و CAD.
- 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.
- الذكية). حماية الأجهزة الطرفية (أجهزة الكمبيوتر، اللوحات
- 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 لـأمن البيانات الهندسية.

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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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