الدورة التدريبية: الأمن السيبراني في أنظمة الطيران وحماية البيانات الجوية الحساسة



19 - 23 اكتوبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #AVI7364_423641

مقدمة الدورة التدريبية / لمحة عامة:

مع تزايد الاعتماد على الأنظمة الرقمية والشبكات في قطاع الطيران، أصبح الأمن السيبراني يمثل تحديًا حاسمًا لضمان سلامة العمليات الجوية وحماية البيانات الحساسة. يدرك BIG BEN Training Center هذه الأهمية، ولذلك يقدم هذه الدورة التدريبية المتخصصة التي تركز على الجوانب الأكثر حيوية في الأمن السيبراني للطيران. صممت الدورة لتزويد المهنيين بالمعرفة والأدوات اللازمة لتأمين الأنظمة الحيوية، من أنظمة الملاحة والتحكم الجوي إلى بيانات الركاب والمعلومات التشغيلية. نعتمد في هذه الدورة على أحدث المعايير الدولية والممارسات الأكاديمية، مثل تلك التي قدمها البروفيسور ألبرت جيرتز (Albert Görtz) في أبحاثه عن أمن أنظمة الطيران. سيتعلم المشاركون كيفية تحليل التهديدات السيبرانية، وتطوير استراتيجيات دفاعية فعالة، وتطبيق بروتوكولات حماية البيانات. تهدف الدورة إلى إعداد محترفين قادرين على حماية المؤسسات من الهجمات السيبرانية، والامتثال للوائح التنظيمية، والمساهمة في بناء بيئة طيران أكثر أمانًا ومرونة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء الأمن السيبراني وتكنولوجيا المعلومات.
- المهندسون في قطاع الطيران.
- المسؤولون عن الأمن والجودة والامتثال.
- المتخصصون في شبكات وأنظمة الطيران.
- المطورون والمهندسون في مجال البرمجيات.
- مدراء العمليات والتشغيل.
- أخصائيو تحليل البيانات.
- الموظفون في هيئات الطيران المدني.

القطاعات والصناعات المستهدفة:

- شركات الطيران التجارية.
- المطارات وشركات الخدمات الأرضية.
- شركات تصنيع الطائرات والمكونات.
- شركات صيانة وإصلاح الطائرات (MROs).
- هيئات الطيران المدني الحكومية وما في حكمها.
- شركات تكنولوجيا الطيران.
- شركات الدفاع والأمن.
- شركات الشحن الجوي.

الأقسام المؤسسية المستهدفة:

- الأمن السيبراني.
- تكنولوجيا المعلومات.
- العمليات التشغيلية.
- الهندسة والصيانة.
- السلامة والجودة.
- التخطيط الاستراتيجي.
- إدارة المخاطر.
- الامتثال والتدقيق.

أهداف الدورة التدريبية:

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

- فهم التهديدات السيبرانية وتأثيرها على أنظمة الطيران.
- تطوير استراتيجيات وسياسات الأمن السيبراني.
- تأمين البنية التحتية لتكنولوجيا المعلومات والأنظمة التشغيلية.
- حماية البيانات الجوية الحساسة وبيانات الركاب.
- تطبيق معايير الامتثال الدولية للأمن السيبراني في الطيران.
- التعامل مع الحوادث السيبرانية والاستجابة لها بفعالية.
- تحليل الثغرات الأمنية في أنظمة الطائرات والشبكات الأرضية.
- بناء ثقافة أمن سيبراني قوية داخل المؤسسة.

منهجية الدورة التدريبية:

يتبع BIG BEN Training Center منهجية تدريبية تجمع بين النظرية المتقدمة والتطبيق العملي، مصممة خصيصًا لتلبية الاحتياجات المتزايدة للأمن السيبراني في قطاع الطيران. تعتمد الدورة على مزيج من المحاضرات التفاعلية التي يقدمها مدربون متخصصون، وورش العمل العملية التي تركز على تحليل المخاطر وتطبيق الحلول الدفاعية. يتم إثراء المحتوى النظري بدراسات حالة واقعية لهجمات سيبرانية سابقة في القطاع، مما يتيح للمشاركين فهم التحديات وكيفية التعامل معها. كما تتضمن الدورة تمارين محاكاة لاختبار قدرات المشاركين على الاستجابة للحوادث السيبرانية، وتحديد نقاط الضعف في الأنظمة. يتم تشجيع العمل الجماعي ومناقشة أفضل الممارسات، بالإضافة إلى جلسات تغذية راجعة فردية لضمان فهم عميق للمفاهيم. هذه المنهجية الشاملة تضمن أن يخرج المشاركون ليس فقط بمعرفة نظرية، بل بمهارات عملية تمكنهم من حماية مؤسساتهم بفعالية في عالم يزداد فيه التهديد السيبراني.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني في الطيران.

- مقدمة في الأمن السيبراني للطيران.
- أنواع التهديدات السيبرانية.
- أنظمة الطيران الحيوية ونقاط الضعف.
- اللوائح والمعايير الدولية للأمن السيبراني (EASA, ICAO).
- مبادئ حماية البيانات.
- بنية أنظمة الاتصالات الجوية.
- دور العنصر البشري في الأمن.

الوحدة الثانية: تأمين أنظمة الطائرات والملاحة.

- هندسة الأمن السيبراني للطائرات.
- حماية أنظمة الملاحة والتحكم.
- تأمين أنظمة الترفيه على متن الطائرة.
- التهديدات على أنظمة الطيران المتصلة.
- أمن برمجيات الطائرات.
- التشفير والتحقق.
- التعامل مع تحديثات النظام.

الوحدة الثالثة: حماية البنية التحتية الأرضية والبيانات.

- تأمين شبكات المطارات.
- حماية أنظمة المراقبة الجوية.
- أمن أنظمة إدارة الأمتعة.
- حماية بيانات الركاب والمعلومات التشغيلية.
- سياسات الوصول والتحكم.
- التقييم المستمر للثغرات الأمنية.
- الحماية من البرامج الضارة.

الوحدة الرابعة: إدارة الحوادث السيبرانية والاستجابة لها.

- تخطيط الاستجابة للحوادث السيبرانية.
- التحقيق في الحوادث السيبرانية.
- التعافي من الهجمات.
- التواصل خلال الأزمات.
- التحليل الجنائي الرقمي.
- التعاون مع الجهات التنظيمية.
- الاستفادة من الدروس المستفادة.

الوحدة الخامسة: مستقبل الأمن السيبراني في الطيران.

- الذكاء الاصطناعي في الدفاع السيبراني.
- أمن الحوسبة السحابية.
- تقنية البلوك تشين.
- التهديدات السيبرانية الناشئة.
- الأمن السيبراني في الطائرات المسيرة.
- التدريب المستمر للموظفين.
- الابتكار في حلول الأمن.

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 الأنظمة المتصلة في الطائرات، كيف يمكننا تحقيق التوازن الأمثل بين الابتكار التكنولوجي وضمان أعلى مستويات الأمن السيبراني لمنع الهجمات المحتملة على أنظمة التحكم الحرجة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

ما يميز هذه الدورة هو تركيزها المتخصص والدقيق على الأمن السيبراني في قطاع الطيران، والذي يعد مجالًا فريدًا بمتطلباته الخاصة. نحن لا نقدم مفاهيم عامة للأمن السيبراني، بل نغوص في التفاصيل الدقيقة المتعلقة بأنظمة الطائرات والمطارات، ونظم الملاحة والاتصالات. على عكس الدورات التي قد تكتفي بالشرح النظري، نقدم أمثلة واقعية ودراسات حالة من حوادث سيبرانية سابقة، مما يساعد المشاركين على فهم حجم التحدي وأهمية الحلول الدفاعية. يركز المحتوى على الجمع بين الجوانب التقنية والإدارية، مما يمكن المشاركين من تطوير استراتيجيات شاملة لحماية مؤسساتهم. كما نعتمد على خبرات أكاديمية ومهنية في المجال، مما يضمن أن المحتوى حديث وموثوق ويتماشى مع أحدث التهديدات والتقنيات. هذا المزيج الفريد من المحتوى المتخصص والتطبيق العملي والخبرة الميدانية يجعل هذه الدورة تجربة تعليمية لا مثيل لها، تمكن المشاركين من قيادة جهود الأمن السيبراني بفعالية في عالم الطيران المتغير.