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

يونيو ٢٠٢٦ ٠٥ - ٠١

كيب تاون - *

(للشخص الواحد) ٦٠٠٠ €

Ref: #AVI7364_574362

مقدمة الدورة التدريبية / لمحة عامة:

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

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:

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

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

منهجية الدورة التدريبية:

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

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.
- .(ICAO اللوائح والمعايير الدولية للأمن السيبراني (EASA,
- 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.

والبيانات. الوحدة الثالثة: حماية البنية التحتية الأرضية

- 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.

والاستجابة لها. الوحدة الرابعة: إدارة الحوادث السيبرانية

- 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:

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:

أعلى مستويات الأمن الطائرات، كيف يمكننا تحقيق التوازن الأمثل بين في ظل الاعتماد المتزايد على الأنظمة المتصلة في

الحرجة؟ السيبراني لمنع الهجمات المحتملة على أنظمة التحكم الابتكار التكنولوجي وضمان

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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