الدورة التدريبية: الأمن السيبراني للقطاع التعليمي والجامعات

#CYB6825

الدورة التدريبية: الأمن السيبراني للقطاع التعليمي والجامعات

مقدمة الدورة التدريبية / لمحة عامة:

يُعد القطاع التعليمي والجامعات بيئة فريدة من نوعها، تجمع بين الأبحاث الحساسة، البيانات الشخصية للطلاب والموظفين، وأنظمة الحرم الجامعي المترابطة. هذا المزيج يجعلها هدفًا جذابًا للتهديدات السيبرانية، مثل هجمات الفدية وسرقة البيانات الأكاديمية. إن أي اختراق أمني في هذا القطاع قد يهدد سمعة المؤسسة، ويعرض البيانات للخطر، ويعطل العملية التعليمية بأكملها. تقدم هذه الدورة التدريبية المتخصصة لمتخصصي تكنولوجيا المعلومات، مديري الأنظمة، والقيادات الأكاديمية، المعرفة والمهارات اللازمة لحماية البنية التحتية التعليمية من الهجمات الرقمية. سنتناول في هذه الدورة مفاهيم الأمن السيبراني في التعليم، تأمين شبكات الجامعات، وحماية بيانات الطلاب. سيكتسب المشاركون القدرة على تحديد المخاطر الأمنية، تطبيق ضوابط أمنية فعالة، والاستجابة للحوادث التي تستهدف المؤسسات التعليمية. تهدف الدورة إلى بناء كوادر متخصصة في الأمن السيبراني الأكاديمي. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور سكوت أ. جونز (Scott A. Jones)، المعروف بأعماله في السياسات الأمنية في التعليم. يقدم BIG BEN Training Center هذه الدورة لتعزيز مرونة المؤسسات التعليمية واستدامتها في العصر الرقمي.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو تكنولوجيا المعلومات في الجامعات والمدارس.
- متخصصو الأمن السيبراني في القطاع التعليمي.
- القيادات الأكاديمية ومسؤولو اتخاذ القرار.
- مسؤولو حماية البيانات والخصوصية.
- مهندسو الشبكات والأنظمة.
- الموظفون الإداريون في أقسام القبول والتسجيل.

القطاعات والصناعات المستهدفة:

- الجامعات والمؤسسات التعليمية العليا.
- المدارس الحكومية والخاصة.
- الهيئات الحكومية وما في حكمها المسؤولة عن التعليم.
- مراكز الأبحاث.
- شركات تكنولوجيا التعليم (EdTech).

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة الأمن السيبراني.
- إدارة القبول والتسجيل.
- إدارة الشؤون المالية.
- إدارة البحث العلمي.

أهداف الدورة التدريبية:

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

- فهم التحديات الأمنية الفريدة للقطاع التعليمي والجامعات.
- القدرة على تأمين شبكات الجامعات وأنظمة الإدارة الأكاديمية.
- حماية بيانات الطلاب والمعلومات الشخصية.
- التعامل مع هجمات الفدية والبرامج الضارة.
- تطبيق أفضل الممارسات لـأمن التعليم عن بعد.
- تطوير خطط الاستجابة للحوادث في البيئة التعليمية.
- الامتثال للوائح والتشريعات الخاصة بحماية البيانات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية تفاعلية وعملية، مصممة لتمكين المشاركين من مواجهة التحديات الأمنية المعقدة في القطاع التعليمي. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لـهجمات سيبرانية على الجامعات، وورش العمل التطبيقية، من فهم كيفية تطبيق ضوابط الأمن على أنظمة إدارة التعلم (LMS) وأنظمة السجلات الطلابية. تتضمن المنهجية مناقشات متعمقة حول الفرق بين أمن البيانات الأكاديمية وأمن البيانات التقليدية، وأفضل الممارسات لـتأمين البحث العلمي. سيتم التركيز على تحليل المخاطر وبناء دفاعات قوية ضد التهديدات الموجهة. يقدم BIG BEN Training Center هذه الدورة لتعزيز الخبرة الأمنية لدى العاملين في القطاع التعليمي وضمان استمرارية العملية التعليمية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: التحديات الأمنية في القطاع التعليمي

- مقدمة إلى الأمن السيبراني للجامعات والمدارس.
- التهديدات السيبرانية التي تستهدف المؤسسات التعليمية.
- نقاط الضعف في أنظمة إدارة التعلم (LMS) والسجلات الطلابية.
- أمن البيانات الأكاديمية والخصوصية.
- هجمات الفدية والبرامج الضارة.
- التوعية الأمنية للطلاب والموظفين.
- الامتثال للوائح التعليمية الخاصة بالأمن.

الوحدة الثانية: تأمين البنية التحتية التعليمية والشبكات

- تقييم المخاطر الأمنية لشبكات الجامعات.
- تأمين شبكات Wi-Fi للحرم الجامعي.
- أمن أنظمة الإدارة الأكاديمية وأنظمة المعلومات.
- التحكم في الوصول إلى أنظمة الموظفين والطلاب.
- حماية قواعد البيانات التي تحتوي على بيانات الطلاب.
- فصل الشبكات لتأمين أقسام البحث.
- التدقيق الأمني للبنية التحتية الرقمية.

الوحدة الثالثة: حماية بيانات الطلاب والموظفين

- التعامل مع البيانات الشخصية للطلاب والموظفين.
- الامتثال لـقوانين حماية البيانات (مثل FERPA).
- تشفير البيانات أثناء النقل والتخزين.
- أمن الأجهزة الشخصية المستخدمة في التعليم.
- الخصوصية على الإنترنت في البيئة التعليمية.
- إدارة هويات المستخدمين والصلاحيات.
- التوعية بأهمية الخصوصية.

الوحدة الرابعة: أمن التعليم عن بعد والمنصات الرقمية

- التحديات الأمنية للتعليم عن بعد.
- تأمين منصات التعليم عبر الإنترنت (Zoom, Teams).
- أمن الاتصالات أثناء المحاضرات الافتراضية.
- حماية المحتوى التعليمي من القرصنة.
- المصادقة الآمنة للطلاب.
- التعامل مع البرامج الضارة التي تستهدف الأجهزة الطلابية.
- بناء بيئة تعليمية افتراضية آمنة.

الوحدة الخامسة: الاستجابة للحوادث وبناء ثقافة الأمن

- وضع خطة للاستجابة للحوادث الأمنية.
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التعافي من حوادث الفدية.
- التدريب على الأمن السيبراني لجميع الأطراف المعنية.
- بناء ثقافة أمنية قوية في المؤسسة التعليمية.
- التواصل مع الجهات الأمنية في حالة الحوادث.
- المرونة السيبرانية واستمرارية الأعمال الأكاديمية.

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 التوسع المستمر للتعلم عن بعد والمنصات الرقمية، كيف يمكن للمؤسسات التعليمية أن تبتكر استراتيجيات أمنية لا تقتصر على حماية البنية التحتية فحسب، بل تُدمج الوعي الأمني كجزء لا يتجزأ من المناهج الدراسية، وتُنشئ مجتمعًا أكاديميًا مرنًا قادرًا على التصدي للتهديدات السيبرانية وحماية المعرفة والبيانات؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على الأمن السيبراني للقطاع التعليمي والجامعات، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية الفريدة في هذا المجال. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لـتأمين شبكات الجامعات، وحماية بيانات الطلاب، وأمن التعليم عن بعد. تقدم الدورة دراسات حالة واقعية لـهجمات سيبرانية على المؤسسات التعليمية، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الترابط بين الأنظمة المختلفة والاستراتيجيات المتكاملة 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 التعليم.