التدريبية: الأمن السيبراني للقطاع التعليمي والجامعات الدورة

يوليو ٢٠٢٦ ٣١ - ٢٧

دوسلدورف

(للشخص الواحد) € ٤٢٠٠

Ref: #CYB6825_271347

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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.
- التعليم. الهيئات الحكومية وما في حكمها المسؤولة عن
- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: التحديات الأمنية في القطاع التعليمي

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

والشبكات الوحدة الثانية: تأمين البنية التحتية التعليمية

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

الوحدة الثالثة: حماية بيانات الطلاب والموظفين

- التعامل مع البيانات الشخصية للطلاب والموظفين.
- الامتثال لقوانين 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.

الرقمية الوحدة الرابعة: أمن التعليم عن بعد والمنصات

- 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.
- الطلابية. التعامل مع البرامج الضارة التي تستهدف الأجهزة
- بناء بيئة تعليمية افتراضية آمنة.

الأمن الوحدة الخامسة: الاستجابة للحوادث وبناء ثقافة

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

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 ٢٠٢٥- 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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

لمواجهة التحديات الأمن السيبراني للقطاع التعليمي والجامعات، مما تتميز هذه الدورة بتركيزها المتخصص والعميق على
السيبراني بشكل عام، نغوص في التطبيق العملي الأمنية الفريدة في هذا المجال. بدلاً من تناول يوفر محتوى مصممًا خصيصًا
المؤسسات التعليمية، وأمن التعليم عن بعد. تقدم الدورة دراسات حالة لـتأمين شبكات الجامعات، وحماية بيانات الطلاب، الأمن
أن نركز على الترابط بين الأنظمة المختلفة مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. واقعية لـهجمات سيبرانية على
هي برنامج تدريبي مكثف المشاركين سيخرجون بخبرة عملية قابلة للتطبيق. إنها والاستراتيجيات المتكاملة للأمن، مما يضمن
على حماية مستقبل التعليم. يهدف إلى بناء متخصصين في الأمن السيبراني قادرين ليست مجرد دورة نظرية، بل