الدورة التدريبية: إدارة الأمن السيبراني وحماية بيانات المرضى في المنشآت الصحية لتأمين المعلومات

#HOS2556

الدورة التدريبية: إدارة الأمن السيبراني وحماية بيانات المرضى في المنشآت الصحية لتأمين المعلومات

مقدمة الدورة التدريبية / لمحة عامة:

تُعد إدارة الأمن السيبراني وحماية بيانات المرضى في المنشآت الصحية تحديًا حاسمًا في العصر الرقمي، حيث أصبحت المعلومات الصحية الإلكترونية هدفًا متزايدًا للهجمات السيبرانية. إن حماية سرية وسلامة وتوفر بيانات المرضى ليست مجرد مسألة امتثال للوائح، بل هي ضرورة أخلاقية وتشغيلية لضمان ثقة المرضى واستمرارية الخدمات الصحية. يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة لتزويد المشاركين بالمعرفة والمهارات اللازمة لتصميم وتطبيق استراتيجيات أمن سيبراني قوية تحمي المعلومات الصحية الحساسة "من الألف الى الياء". تتناول الدورة مفاهيم مثل تهديدات الأمن السيبراني الشائعة، أطر عمل حماية البيانات (مثل HIPAA وGDPR)، تقنيات التشفير، إدارة الهوية والوصول، الاستجابة للحوادث، والتدريب على الوعي الأمني. نستلهم في هذه الدورة من رواد الفكر في الأمن السيبراني، مثل البروفيسور William Stallings، الذي يُعد مؤلفاً للعديد من الكتب المرجعية في أمن الشبكات وأنظمة التشغيل، ومنها "Cryptography and Network Security: Principles and Practice"، والذي يسلط الضوء على أهمية الحماية الشاملة للأنظمة والبيانات. سيتعلم المشاركون كيفية تقييم المخاطر، تطبيق أفضل الممارسات الأمنية، تطوير خطط للاستجابة السريعة للحوادث، وبناء ثقافة أمنية داخل مؤسساتهم، كل ذلك بهدف نهائي يتمثل في بناء دفاعات قوية ضد التهديدات السيبرانية وضمان خصوصية وسلامة بيانات المرضى.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء تقنية المعلومات في المستشفيات والمراكز الصحية.
- مسؤولو الأمن السيبراني وحماية البيانات (CISO, DPO).
- أخصائيو أمن الشبكات والأنظمة.
- المدققون الداخليون والخارجيون في القطاع الصحي.
- مدراء الامتثال والشؤون القانونية.
- القيادات الإدارية والطبية المعنية بأمن المعلومات.
- مسؤولو إدارة المخاطر.
- محللو الأمن السيبراني.
- المطورون العاملون على أنظمة الرعاية الصحية.
- جميع العاملين في مجال الرعاية الصحية الذين يتعاملون مع بيانات المرضى.

القطاعات والصناعات المستهدفة:

- المستشفيات العامة والخاصة.
- العيادات والمراكز الطبية المتخصصة.
- شركات تطوير البرمجيات والأنظمة الصحية.
- شركات التأمين الصحي.
- هيئات الصحة الحكومية والتنظيمية.
- مراكز البحوث الطبية الحيوية.
- المختبرات الطبية ومراكز الأشعة.
- شركات الأدوية.
- شركات الاستشارات في الأمن السيبراني.
- البنوك والمؤسسات المالية التي تتعامل مع بيانات صحية.

الأقسام المؤسسية المستهدفة:

- تقنية المعلومات.
- الأمن السيبراني.
- إدارة المخاطر.
- الامتثال والشؤون القانونية.

- إدارة السجلات الطبية.
- إدارة العمليات.
- التدريب والتطوير.
- الإدارة العليا.
- المراجعة الداخلية.
- البحث والتطوير.

أهداف الدورة التدريبية:

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

- فهم التهديدات السيبرانية الشائعة في القطاع الصحي.
- تطبيق أطر عمل ومعايير حماية بيانات المرضى (مثل HIPAA).
- تصميم وتنفيذ سياسات وإجراءات الأمن السيبراني.
- استخدام تقنيات التشفير وإدارة الهوية والوصول.
- تحديد وتقييم المخاطر الأمنية في الأنظمة الصحية.
- تطوير خطط فعالة للاستجابة للحوادث الأمنية.
- تعزيز الوعي الأمني لدى الموظفين في المنشأة الصحية.
- ضمان الامتثال للوائح المحلية والدولية لحماية البيانات.
- إدارة الثغرات الأمنية واختبارات الاختراق.
- بناء دفاعات قوية ضد الهجمات السيبرانية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تجمع بين المعرفة النظرية والتدريب العملي لضمان اكتساب المشاركين فهماً عميقاً ومهارات قابلة للتنفيذ في إدارة الأمن السيبراني وحماية بيانات المرضى في المنشآت الصحية. تبدأ الدورة بتقديم نظرة شاملة على المشهد الحالي للتهديدات السيبرانية التي تواجه القطاع الصحي، مع استعراض أهمية حماية بيانات المرضى الحساسة. يتم التركيز بشكل كبير على دراسات الحالة الواقعية لحوادث أمنية كبرى وكيفية التعامل معها، مما يتيح للمشاركين تحليل الاستجابات الفعالة والدروس المستفادة. تتضمن الدورة ورش عمل تفاعلية مكثفة وتمارين محاكاة، حيث يتم تدريب المشاركين على تقييم المخاطر، تطبيق ضوابط أمنية، تطوير خطط الاستجابة للحوادث، وإجراء تقييمات للثغرات. كما يتم تشجيع العمل الجماعي وتبادل الخبرات بين المشاركين، مما يثري النقاش ويوفر منظورات متنوعة لتحديات الأمن السيبراني. يقدم مدربو BIG BEN Training Center ذوو الخبرة الواسعة في مجال الأمن السيبراني والرعاية الصحية تغذية راجعة مستمرة ومباشرة، لضمان استيعاب المفاهيم وتطبيقها الصحيح. تهدف المنهجية إلى تمكين المشاركين من أن يصبحوا روادًا في حماية البيانات الصحية، قا
رين على بناء بيئات رقمية آمنة وموثوقة، وضمان خصوصية وسلامة معلومات المرضى.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني في الرعاية الصحية.

- مقدمة في الأمن السيبراني ومفاهيمه الأساسية.
- أهمية حماية بيانات المرضى (PHI) والمعلومات الصحية الإلكترونية (EHR).
- التهديدات السيبرانية الشائعة التي تواجه القطاع الصحي.
- مفهوم المخاطر السيبرانية وإدارتها.
- مقدمة لأطر العمل التنظيمية (مثل HIPAA، GDPR، CCPA).
- دور التكنولوجيا في حماية البيانات.
- أخلاقيات الأمن السيبراني في الرعاية الصحية.

الوحدة الثانية: حماية البيانات والتحكم في الوصول.

- مبادئ حماية البيانات (السرية، السلامة، التوفر).
- تقنيات التشفير المستخدمة لحماية البيانات.
- إدارة الهوية والوصول (Identity and Access Management – IAM).

- المصادقة المتعددة العوامل (Multi-Factor Authentication – MFA).
- التحكم في الوصول المادي والمنطقي.
- سياسات وإجراءات كلمة المرور القوية.
- التعامل الآمن مع البيانات الحساسة.

الوحدة الثالثة: أمن الشبكات والأنظمة.

- أساسيات أمن الشبكات في المنشآت الصحية.
- جدران الحماية (Firewalls) وأنظمة كشف/منع التطفل (IDS/IPS).
- أمن الأجهزة الطرفية (Endpoint Security).
- إدارة الثغرات الأمنية (Vulnerability Management).
- أمن الخوادم وقواعد البيانات.
- النسخ الاحتياطي للبيانات واستعادة الكوارث.
- مفاهيم أمن السحابة في الرعاية الصحية.

الوحدة الرابعة: الاستجابة للحوادث والامتثال.

- تخطيط الاستجابة للحوادث السيبرانية.
- خطوات الاستجابة للحوادث (التعرف، الاحتواء، الاستئصال، الاسترداد، الدروس المستفادة).
- التقارير عن الحوادث الأمنية.
- الامتثال للوائح حماية البيانات (HIPAA Security Rule).
- إجراءات التدقيق الأمني والتقييمات.
- العقوبات المترتبة على انتهاكات البيانات.
- بناء فريق استجابة للحوادث.

الوحدة الخامسة: ثقافة الأمن السيبراني والقيادة.

- دور القيادة في تعزيز الأمن السيبراني.
- برامج التدريب والتوعية للموظفين.
- أهمية الوعي بمخاطر التصيد الاحتيالي (Phishing) والهندسة الاجتماعية.
- بناء ثقافة أمنية قوية داخل المؤسسة.
- التواصل الفعال حول قضايا الأمن السيبراني.
- تقييم مستوى الوعي الأمني.
- التعلم المستمر من التهديدات المتطورة.

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 عصر يزداد فيه الاعتماد على التكنولوجيا الرقمية في الرعاية الصحية، وكثرة الهجمات السيبرانية المعقدة، كيف يمكن للمنشآت الصحية أن تحقق التوازن بين توفير الوصول السريع والفعال للمعلومات الضرورية للرعاية، وبين تطبيق أقصى درجات الأمن السيبراني لحماية بيانات المرضى الحساسة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على إدارة الأمن السيبراني وحماية بيانات المرضى في المنشآت الصحية، مما يجعلها مختلفة عن الدورات العامة في الأمن السيبراني. نحن نقدم للمشاركين نهجًا شموليًا يجمع بين الأطر النظرية المتقدمة وأفضل الممارسات التطبيقية المخصصة لتحديات بيئة الرعاية الصحية. يتميز المحتوى بتقديم دراسات حالة واقعية لحوادث أمنية في القطاع الصحي، مما يتيح للمشاركين تطبيق المفاهيم المكتسبة مباشرة على سياقاتهم. نركز على تزويد المتدربين بمهارات عملية لتقييم المخاطر، تطبيق الضوابط الأمنية، الاستجابة للحوادث، وضمان الامتثال للوائح، بالإضافة إلى استراتيجيات لبناء ثقافة أمنية قوية. الدورة مصممة لتمكين المهنيين من حماية الأصول الرقمية للمؤسسات الصحية، مما يساهم في بناء أنظمة رعاية صحية آمنة وموثوقة، وتحقيق أعلى مستويات خصوصية بيانات المرضى.