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

يونيو - ٠٢ يوليو ٢٠٢٦ ٢٨

عمان

٤١٠٠ € (للشخص الواحد)

Ref: #HOS2556_73083

مقدمة الدورة التدريبية / لمحة عامة:

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

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- الصحية. مدراء تقنية المعلومات في المستشفيات والمراكز
- .(DPO مسؤولو الأمن السيبراني وحماية البيانات (CISO,
- 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.
- يتعاملون مع بيانات المرضى. جميع العاملين في مجال الرعاية الصحية الذين

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.
- صحية. البنوك والمؤسسات المالية التي تتعامل مع بيانات

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:

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

- فهم التهديدات السيبرانية الشائعة في القطاع الصحي.
- .(HIPAA تطبيق أطر عمل ومعايير حماية بيانات المرضى (مثل
- 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.
- البيانات. ضمان الامتثال للوائح المحلية والدولية لحماية
- إدارة الثغرات الأمنية واختبارات الاختراق.
- بناء دفاعات قوية ضد الهجمات السيبرانية.

منهجية الدورة التدريبية:

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

روادًا في حماية البيانات

خصوصية وسلامة معلومات المرضى. رين على بناء بيئات رقمية آمنة وموثوقة، وضمان

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الصحية. الوحدة الأولى: أساسيات الأمن السيبراني في الرعاية

- مقدمة في الأمن السيبراني ومفاهيمه الأساسية.
- الإلكترونية (.EHR) أهمية حماية بيانات المرضى (PHI) والمعلومات الصحية
- الصحي. التهديدات السيبرانية الشائعة التي تواجه القطاع
- مفهوم المخاطر السيبرانية وإدارتها.
- .CCPA) مقدمة لأطر العمل التنظيمية (مثلHIPAA، GDPR ،
- 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.
- .Identity and Access) إدارة الهوية والوصول Management - IAM).
- .Multi-Factor) المصادقة المتعددة العوامل 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.
- .(IDS/IPS) جدران الحماية (Firewalls) وأنظمة كشف/منع التطفل
- 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.
- الاستئصال، الاسترداد، الدروس المستفادة). خطوات الاستجابة للحوادث (التعرف، الاحتواء،
- التقارير عن الحوادث الأمنية.
- .(HIPAA Security Rule) الامتثال للوائح حماية البيانات
- 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.
- والهندسة الاجتماعية. أهمية الوعي بمخاطر التصيد الاحتيالي ((Phishing
- بناء ثقافة أمنية قوية داخل المؤسسة.
- التواصل الفعال حول قضايا الأمن السيبراني.
- تقييم مستوى الوعي الأمني.
- التعلم المستمر من التهديدات المتطورة.

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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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