الدورة التدريبية: تأمين التجارة الإلكترونية وحماية المعاملات الرقمية المتقدمة

#SM1436

الدورة التدريبية: تأمين التجارة الإلكترونية وحماية المعاملات الرقمية المتقدمة

مقدمة الدورة التدريبية / لمحة عامة:

يشهد قطاع التجارة الإلكترونية نموًا هائلاً، مما يجعله هدفًا رئيسيًا للمخاطر الأمنية المتزايدة التي تهدد ثقة المستهلكين وسمعة الشركات. تهدف هذه الدورة التدريبية المتخصصة، التي يقدمها BIG BEN Training Center، إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتأمين منصات التجارة الإلكترونية وحماية المعاملات عبر الإنترنت. ستغطي الدورة كافة الجوانب المتعلقة بأمن التجارة الإلكترونية، بدءًا من البنية التحتية للمواقع والشبكات، وصولًا إلى حماية بيانات الدفع والمعلومات الشخصية للعملاء. سيتعلم المشاركون كيفية تحديد الثغرات الأمنية، وتطبيق أفضل الممارسات في التشفير، وإدارة الهوية والوصول، والاستجابة للحوادث الأمنية. تستند هذه الدورة إلى أحدث المعايير الدولية وأطر العمل الأمنية، مستلهمة من أعمال أكاديميين بارزين مثل البروفيسور William Stallings (ويليام ستالينغز)، الذي يعد من أبرز المؤلفين في مجال أمن الشبكات والبيانات، والذي أسهمت مؤلفاته في إرساء أسس فهم أمن المعلومات. تهدف الدورة إلى تمكين المهنيين من بناء بيئات تجارة إلكترونية آمنة وموثوقة، تعزز ثقة العملاء وتحمي الأصول الرقمية، مما يضمن استمرارية الأعمال وازدهارها في ظل التحديات الأمنية المستمرة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء أمن المعلومات والأمن السيبراني في شركات التجارة الإلكترونية.
- مطورون ومصممو مواقع التجارة الإلكترونية.
- متخصصو الأمن السيبراني ومحللو التهديدات.
- مدراء تكنولوجيا المعلومات في الشركات الرقمية.
- مسؤولو الامتثال والمخاطر.
- رواد الأعمال وأصحاب المتاجر الإلكترونية.
- متخصصو التسويق الرقمي الذين يتعاملون مع بيانات العملاء.
- فرق الدعم الفني والعمليات.

القطاعات والصناعات المستهدفة:

- شركات التجارة الإلكترونية ومتاجر التجزئة عبر الإنترنت.
- المؤسسات المالية والبنوك.
- شركات تطوير الويب والتطبيقات.
- شركات الدفع الإلكتروني.
- شركات الاستضافة والخدمات السحابية.
- شركات التسويق الرقمي.
- الجهات الحكومية المنظمة لقطاع التجارة الإلكترونية.
- شركات اللوجستيات والشحن المتعاملة مع البيانات.

الأقسام المؤسسية المستهدفة:

- قسم أمن المعلومات.
- قسم تكنولوجيا المعلومات.
- قسم تطوير الويب والتطبيقات.
- قسم العمليات والتشغيل.
- القسم القانوني والامتثال.
- قسم التسويق الرقمي.
- إدارة المخاطر.
- القيادة التنفيذية.

أهداف الدورة التدريبية:

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

- فهم التهديدات الأمنية الشائعة التي تواجه التجارة الإلكترونية.
- تطبيق أفضل الممارسات لتأمين منصات ومواقع التجارة الإلكترونية.
- حماية بيانات الدفع والمعلومات الشخصية للعملاء.
- تحديد وتقييم الثغرات الأمنية في تطبيقات الويب.
- تصميم وتنفيذ استراتيجيات قوية للتشفير والمصادقة.
- التعامل مع حوادث اختراق البيانات والاستجابة لها بفعالية.
- ضمان الامتثال للمعايير الدولية لأمن بطاقات الدفع (PCI DSS).
- بناء ثقة العملاء من خلال تعزيز الأمن السيبراني.
- فهم تحديات أمن سلسلة التوريد الرقمية.
- تأمين واجهات برمجة التطبيقات (APIs) المستخدمة في التجارة الإلكترونية.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية تجمع بين الجانب النظري والتطبيق العملي، لضمان فهم شامل وقدرة على تطبيق المعرفة في مجال أمن التجارة الإلكترونية. ستتضمن الدورة محاضرات تفاعلية تستعرض أحدث التهديدات والحلول الأمنية، تليها ورش عمل تطبيقية تتيح للمشاركين ممارسة الأدوات والتقنيات اللازمة لتأمين المنصات الرقمية. سيتم تحليل دراسات حالة واقعية لهجمات سيبرانية شهيرة على منصات التجارة الإلكترونية، وكيفية التعامل معها والتخفيف من آثارها. كما سيتم التركيز على التحديات الأمنية الخاصة ببيئات التجارة الإلكترونية، مثل تأمين بوابات الدفع، وحماية بيانات العملاء، ومنع الاحتيال. سيتم تشجيع المشاركين على تبادل الخبرات والتجارب، مما يعزز من فهمهم المشترك للموضوع. تهدف هذه المنهجية إلى تزويد المتدربين بمهارات عملية تمكنهم من بناء وصيانة بيئات تجارة إلكترونية آمنة وموثوقة، مما يحمي أعمالهم وعملائهم.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى أمن التجارة الإلكترونية والمخاطر

- مفهوم التجارة الإلكترونية وتحدياتها الأمنية.
- التهديدات الشائعة التي تواجه منصات التجارة الإلكترونية.
- أنواع الهجمات السيبرانية على مواقع الويب.
- أهمية حماية بيانات الدفع والمعلومات الشخصية.
- الاحتيال عبر الإنترنت وكيفية منعه.
- الأطر القانونية والتنظيمية لأمن التجارة الإلكترونية.
- بناء الثقة مع العملاء.

الوحدة الثانية: تأمين منصات التجارة الإلكترونية وتطبيقات الويب

- نقاط الضعف في تطبيقات الويب (OWASP Top 10).
- أمن قاعدة البيانات وحماية المعلومات الحساسة.
- تأمين واجهات برمجة التطبيقات (APIs).
- حماية الخوادم والبنية التحتية.
- نظم إدارة المحتوى (CMS) وأمنها.
- إدارة الثغرات الأمنية والتصحيحات.
- المراقبة المستمرة وكشف التسلل.

الوحدة الثالثة: حماية المعاملات والدفع الإلكتروني

- معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS).
- تقنيات التشفير المستخدمة في المعاملات.
- أمن بوابات الدفع وأنظمة معالجة الدفع.
- المصادقة متعددة العوامل (MFA).
- منع الاحتيال في البطاقات الائتمانية.
- الترميز (Tokenization) وإخفاء البيانات.
- المراجعة الأمنية للمعاملات.

الوحدة الرابعة: إدارة الهوية والوصول وحماية العملاء

- إدارة الهوية والوصول (IAM) في التجارة الإلكترونية.
- أمن حسابات المستخدمين وحمايتها.
- سياسات كلمات المرور القوية.
- التعامل مع حسابات المستخدمين المخترقة.
- خصوصية البيانات الشخصية للعملاء.
- حقوق المستهلك وحماية معلوماته.
- الامتثال لقوانين حماية البيانات.

الوحدة الخامسة: الاستجابة للحوادث الأمنية وتعزيز المرونة

- تطوير خطط الاستجابة للحوادث الأمنية.
- التحقيق في خروقات البيانات.
- التعافي من الكوارث واستمرارية الأعمال.
- التدريب والوعي الأمني للموظفين.
- التعاون مع الجهات الأمنية الخارجية.
- التحسين المستمر لبرامج الأمن.
- أحدث الاتجاهات في أمن التجارة الإلكترونية.

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 التطور المتسارع لتقنيات التجارة الإلكترونية وتزايد حجم المعاملات عبر الإنترنت، كيف يمكن للمؤسسات تحقيق التوازن الدقيق بين توفير تجربة مستخدم سلسة وجذابة وبين تطبيق أعلى معايير الأمن السيبراني لحماية البيانات الحساسة وثقة العملاء من التهديدات المتطورة باستمرار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بمنهجها الشامل والعميق الذي يركز بشكل خاص على التحديات الأمنية المعقدة في قطاع التجارة الإلكترونية، مما يميزها عن الدورات العامة في الأمن السيبراني. يقدم BIG BEN Training Center محتوى أكاديميًا متطورًا، مبنيًا على أحدث المعايير وأفضل الممارسات العالمية في حماية المعاملات الرقمية، بما في ذلك التركيز على الامتثال لمعيار PCI DSS. ما يجعل هذه الدورة فريدة هو تركيزها على الرؤى العملية والأمثلة المستقاة من سيناريوهات الاختراقات الحقيقية التي تعرضت لها منصات التجارة الإلكترونية، مما يمكن المشاركين من تحليل المشكلات وتطبيق حلول فعالة ومبتكرة. بدلاً من مجرد سرد الأدوات التقنية، توفر الدورة فهمًا عميقًا لكيفية بناء بنية تحتية آمنة، وحماية بيانات الدفع، وتعزيز ثقة العملاء، مما يضمن أن يكون المتدربون مجهزين لمواجهة التهديدات المتطورة وحماية أصول شركاتهم الرقمية بفعالية.