الدورة التدريبية: أمن التجارة الإلكترونية وحماية بيانات العملاء عبر الإنترنت

#CYB2009

الدورة التدريبية: أمن التجارة الإلكترونية وحماية بيانات العملاء عبر الإنترنت

مقدمة الدورة التدريبية / لمحة عامة:

مع النمو الهائل للتجارة الإلكترونية، أصبح أمن بيانات العملاء وحماية المعاملات عبر الإنترنت أمرًا حيويًا لـنجاح الأعمال التجارية وبناء ثقة المستهلك. تتعرض المنصات الإلكترونية باستمرار للتهديدات السيبرانية التي تستهدف المعلومات الحساسة وعمليات الدفع. تقدم هذه الدورة التدريبية الشاملة لأصحاب الأعمال، مطوري الويب، مديري الأمن، وأي شخص معني بحماية المتاجر الإلكترونية، المعرفة والمهارات اللازمة لـتأمين منصات التجارة الإلكترونية وضمان خصوصية بيانات العملاء. سنتناول في هذه الدورة مفاهيم أمن التجارة الإلكترونية الأساسية، تقنيات التشفير، أمن بوابات الدفع، والامتثال للوائح حماية البيانات. سيكتسب المشاركون القدرة على تحديد نقاط الضعف، تطبيق ضوابط أمنية فعالة، والاستجابة للحوادث الأمنية التي قد تؤثر على سمعة الأعمال وثقة العملاء. تهدف الدورة إلى تمكين الشركات من توفير تجربة تسوق آمنة وموثوقة. يستند المحتوى إلى أحدث المعايير الصناعية وأفضل الممارسات في أمن الويب والتجارة الإلكترونية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور باري شرينر (Gary McGraw)، المعروف بأعماله في أمن تطبيقات الويب والهندسة الأمنية. يقدم BIG BEN Training Center هذه الدورة لمساعدة الشركات على بناء منصات تجارة إلكترونية حصينة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- أصحاب المتاجر الإلكترونية ومديرو التجارة الإلكترونية.
- مطورو ومصممو مواقع التجارة الإلكترونية.
- متخصصو الأمن السيبراني وأمن تطبيقات الويب.
- مديرو تكنولوجيا المعلومات.
- المسؤولون عن حماية البيانات والخصوصية.
- المسؤولون عن إدارة المخاطر في الشركات الرقمية.

القطاعات والصناعات المستهدفة:

- شركات التجارة الإلكترونية والبيع بالتجزئة عبر الإنترنت.
- القطاع المصرفي والمالي (خاصة بوابات الدفع).
- شركات تطوير الويب والتطبيقات.
- المؤسسات التي تقدم خدمات عبر الإنترنت.
- قطاع التكنولوجيا المالية (FinTech).
- الجهات الحكومية وما في حكمها، المعنية بـتنظيم التجارة الإلكترونية.

الأقسام المؤسسية المستهدفة:

- إدارة التجارة الإلكترونية.
- إدارة تقنية المعلومات وتطوير الويب.
- إدارة الأمن السيبراني.
- إدارة التسويق الرقمي (لجانب الثقة والأمان).
- القسم القانوني (لجانب الامتثال).

أهداف الدورة التدريبية:

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

- فهم تحديات أمن التجارة الإلكترونية وتهديداتها الرئيسية.
- القدرة على تأمين مواقع الويب وتطبيقات التجارة الإلكترونية.
- حماية بيانات العملاء الشخصية والمالية.
- تأمين بوابات الدفع الإلكتروني ومنع الاحتيال.
- الامتثال للوائح حماية البيانات (مثل GDPR, CCPA).
- الاستجابة الفعالة للحوادث الأمنية في بيئة التجارة الإلكترونية.
- بناء ثقة العملاء من خلال تعزيز الأمن السيبراني.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وشاملة، تركز على تزويد المشاركين بالخبرة المباشرة في تأمين منصات التجارة الإلكترونية وحماية بيانات العملاء. سيتمكن المتدربون من خلال ورش العمل التطبيقية ودراسات الحالة الواقعية لـاختراقات المتاجر الإلكترونية، من فهم كيفية تطبيق إجراءات الأمن السيبراني على مواقع الويب وتطبيقات الدفع. تتضمن المنهجية مناقشات متعمقة حول أفضل الممارسات في أمن الويب، وكيفية التعامل مع الثغرات الشائعة مثل هجمات SQL Injection وXSS. سيتم التركيز على أمن الطبقات المختلفة في منصة التجارة الإلكترونية، من الخادم وحتى واجهة المستخدم. يقدم BIG BEN Training Center هذه الدورة لتمكين الشركات من بناء بيئة تجارة إلكترونية آمنة وموثوقة لملايين المستخدمين.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن التجارة الإلكترونية والتهديدات

- مقدمة إلى عالم التجارة الإلكترونية وأهمية أمنها.
- أنواع التهديدات السيبرانية التي تستهدف المتاجر الإلكترونية.
- مفاهيم أمن الويب الأساسية (OWASP Top 10).
- حماية البيانات الشخصية للعملاء (PII).
- الاحتيال الإلكتروني وطرق الوقاية منه.
- أمن منصات التجارة الإلكترونية الشائعة (مثل Magento, Shopify).
- بناء نموذج تهديد لمتجر إلكتروني.

الوحدة الثانية: تأمين تطبيقات الويب وقواعد البيانات

- تأمين تطبيقات الويب ضد هجمات الحقن (SQL Injection, Command Injection).
- الحماية من هجمات البرمجة عبر المواقع (XSS) وتزوير الطلبات عبر المواقع (CSRF).
- إدارة الجلسات الآمنة والمصادقة والتفويض.
- تأمين قواعد البيانات التي تحتوي على بيانات العملاء.
- التشفير للبيانات أثناء النقل والتخزين.
- مراجعة الكود البرمجي من منظور أمني.
- تطبيق مبادئ التطوير الآمن (Secure Development Lifecycle).

الوحدة الثالثة: أمن بوابات الدفع والمعاملات المالية

- مقدمة إلى بوابات الدفع الإلكتروني وآليات عملها.
- معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS).
- تأمين المعاملات المالية وتقنيات التشفير (SSL/TLS).
- كشف الاحتيال في المدفوعات وأنظمة منع الاحتيال.
- أمن معلومات بطاقات الائتمان.
- التعامل مع عمليات استرداد المدفوعات (Chargebacks).
- أمن الدفع عبر الأجهزة المحمولة.

الوحدة الرابعة: حماية بيانات العملاء والامتثال للخصوصية

- لوائح حماية البيانات العالمية (GDPR, CCPA) وتأثيرها على التجارة الإلكترونية.
- تصميم سياسات خصوصية شفافة وفعالة.
- موافقات المستخدمين على جمع واستخدام البيانات.
- إدارة حقوق الأفراد المتعلقة ببياناتهم.
- أمن تخزين البيانات وفترات الاحتفاظ بها.
- عمليات التدقيق للامتثال للوائح الخصوصية.
- إدارة خروقات البيانات والإبلاغ عنها.

الوحدة الخامسة: الاستجابة للحوادث وبناء الثقة في التجارة الإلكترونية

- وضع خطة الاستجابة للحوادث الأمنية للمتاجر الإلكترونية.
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التحقيق في الحوادث الأمنية لمنصات التجارة الإلكترونية.
- التعافي من الهجمات واستعادة الخدمات.
- بناء ثقة العملاء من خلال الشفافية الأمنية.
- شهادات الأمن (مثل SSL/TLS) وأهميتها.
- مستقبل 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 لـتقنيات التجارة الإلكترونية وظهور أساليب جديدة للاحتيال السيبراني، كيف يمكن للمتاجر الإلكترونية أن تبتكر استراتيجيات أمنية لا تكتفي بصد التهديدات المعروفة، بل تتوقع التحديات المستقبلية وتُنشئ تجربة تسوق رقمية موثوقة تضع حماية بيانات العملاء في صلب أولوياتها؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والعميق على أمن التجارة الإلكترونية وحماية بيانات العملاء، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية في هذا القطاع الحيوي. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لـأمن تطبيقات الويب، تأمين بوابات الدفع، والامتثال للوائح حماية البيانات مثل GDPR. تقدم الدورة دراسات حالة واقعية لـاختراقات المتاجر الإلكترونية، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على بناء ثقة العملاء من خلال ممارسات أمنية شفافة وفعالة. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في أمن التجارة الإلكترونية قادرين على حماية الأصول الرقمية للشركات وضمان تجربة تسوق آمنة للمستهلكين.