الدورة التدريبية: التشفير المتقدم وأمن البيانات للأنظمة الحساسة



19 - 23 اكتوبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #CYB4540_327307

مقدمة الدورة التدريبية / لمحة عامة:

يمثل التشفير حجر الزاوية في أمن البيانات، وهو ضرورة لا غنى عنها لحماية المعلومات الحساسة في العصر الرقمي. مع تزايد التهديدات السيبرانية، أصبح الفهم العميق لمفاهيم التشفير المتقدمة ضروريًا للمؤسسات التي تتعامل مع بيانات سرية، سواء كانت مالية، طبية، أو حكومية. تقدم هذه الدورة التدريبية المتخصصة لمتخصصي الأمن السيبراني، المطورين، ومديري الأنظمة، الأدوات والمعرفة اللازمة لتأمين البيانات بشكل فعال باستخدام أحدث خوارزميات التشفير وبروتوكولات الأمان. سنتناول في هذه الدورة أساسيات التشفير، التشفير غير المتماثل، التوقيعات الرقمية، وإدارة المفاتيح التشفيرية. سيكتسب المشاركون القدرة على تطبيق حلول تشفير متقدمة، حماية البيانات أثناء النقل والتخزين، وضمان سرية وسلامة المعلومات. تهدف الدورة إلى بناء كوادر متخصصة في تأمين البيانات باستخدام التشفير. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور بروس شناير (Bruce Schneier)، المعروف بأعماله الرائدة في التشفير وأمن الكمبيوتر. يقدم BIG BEN Training Center هذه الدورة لتمكين المؤسسات من حماية أصولها الرقمية الأكثر حساسية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني.
- مهندسو الشبكات والأنظمة.
- مطورون وباحثون في مجال الأمن.
- مديرو أمن المعلومات.
- المهنيون العاملون في القطاعات الحيوية التي تتعامل مع بيانات حساسة.
- المسؤولون عن حماية البيانات والخصوصية.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- الرعاية الصحية والمستشفيات.
- الهيئات الحكومية والجهات الأمنية وما في حكمها.
- شركات تطوير البرمجيات.
- شركات الاتصالات.
- المؤسسات البحثية والعلمية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة تقنية المعلومات.
- أقسام تطوير البرمجيات.
- إدارة المخاطر والامتثال.
- إدارة العمليات (خاصة في الأنظمة التي تتعامل مع بيانات حساسة).

أهداف الدورة التدريبية:

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

- فهم عميق لمبادئ التشفير وأنواعه المختلفة.
- القدرة على تطبيق خوارزميات التشفير (AES, RSA) بشكل عملي.
- حماية البيانات أثناء النقل باستخدام بروتوكولات SSL/TLS.
- تأمين البيانات المخزنة باستخدام تقنيات التشفير.
- إنشاء وإدارة البنية التحتية للمفاتيح العامة (PKI).
- استخدام التوقيعات الرقمية والشهادات الرقمية لضمان الهوية.
- تصميم حلول أمنية شاملة للأنظمة الحساسة باستخدام التشفير.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية متقدمة وموجهة نحو التطبيق العملي، مصممة لتمكين المشاركين من فهم وتطبيق تقنيات التشفير المتقدمة. سيتمكن المتدربون من خلال ورش العمل العملية التي تتضمن تشفير ملفات، وإنشاء شهادات رقمية، وتأمين اتصالات الشبكة، من اكتساب خبرة مباشرة في أمن البيانات. تتضمن المنهجية مناقشات متعمقة حول نقاط القوة والضعف في خوارزميات التشفير المختلفة، وكيفية اختيار الحلول المناسبة لكل حالة استخدام. سيتم التركيز على الجانب العملي لإدارة المفاتيح التشفيرية، والتعامل مع التحديات التي يفرضها التشفير الكمومي. يقدم BIG BEN Training Center هذه الدورة لتمكين المشاركين من أن يصبحوا خبراء في حماية البيانات الحساسة باستخدام أقوى أدوات التشفير.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات التشفير وأمن البيانات

- مقدمة إلى مفاهيم التشفير والأمن السيبراني.
- التشفير المتماثل (Symmetric Encryption) وخوارزمياته (AES).
- التشفير غير المتماثل (Asymmetric Encryption) وخوارزمياته (RSA).
- دالات التجزئة (Hash Functions) وسلامة البيانات.
- مفاهيم المصادقة والسرية وسلامة البيانات.
- التشفير في سياق حماية البيانات الحساسة.
- أنواع الهجمات على أنظمة التشفير.

الوحدة الثانية: البنية التحتية للمفاتيح العامة (PKI)

- مقدمة إلى البنية التحتية للمفاتيح العامة (PKI).
- المكونات الأساسية لـ PKI (CA, RA, Certificates).
- إنشاء وإدارة الشهادات الرقمية.
- التوقيعات الرقمية والتأكد من هوية الأطراف.
- بروتوكولات SSL/TLS وتأمين الاتصالات عبر الإنترنت.
- تطبيق PKI في المؤسسات.
- التحديات في إدارة PKI.

الوحدة الثالثة: تأمين البيانات أثناء النقل والتخزين

- تشفير البيانات أثناء النقل (Data-in-transit).
- بروتوكولات VPN والشبكات الخاصة الافتراضية.
- تشفير البيانات المخزنة (Data-at-rest).
- تشفير الأقراص الصلبة وقواعد البيانات.
- التشفير في بيئة الحوسبة السحابية.
- أمن المفاتيح التشفيرية وأنظمة إدارة المفاتيح (KMS).
- التشفير المتقدم للبيانات الشخصية.

الوحدة الرابعة: خوارزميات التشفير المتقدمة وتطبيقاتها

- التشفير المنحني الإهليلجي (Elliptic Curve Cryptography).
- التشفير المتماثل المتقدم (Advanced Symmetric Encryption).
- التشفير على مستوى التطبيقات والبريد الإلكتروني.
- التشفير في أنظمة إنترنت الأشياء (IoT).
- مقدمة إلى التشفير ما بعد الكمومي (Post-Quantum Cryptography).
- استخدام التشفير في blockchain.
- التشفير والمخاطر المستقبلية.

الوحدة الخامسة: إدارة المفاتيح التشفيرية ووضع الاستراتيجيات

- أفضل الممارسات في إدارة المفاتيح التشفيرية.
- دورة حياة المفتاح التشفيري.
- مخاطر إدارة المفاتيح وكيفية التخفيف منها.
- تصميم سياسة تشفير شاملة للمؤسسة.
- الامتثال للوائح المتعلقة بحماية البيانات الحساسة.
- التدقيق الأمني لحلول التشفير.
- بناء استراتيجية أمن بيانات متكاملة.

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 التقدم المتسارع للحوسبة الكمومية، التي قد تهدد بعض خوارزميات التشفير الحالية، كيف يمكن للمؤسسات أن تبتكر استراتيجيات تشفير مرنة ومستقبلية لا تقتصر على حماية البيانات اليوم، بل تضمن سرية وسلامة المعلومات الحساسة في مواجهة التحديات التشفيرية القادمة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتعمق والعملي على التشفير المتقدم وأمن البيانات، مما يوفر للمشاركين فهمًا شاملاً لكيفية حماية المعلومات الحساسة بفعالية. بدلاً من مجرد سرد المفاهيم النظرية، نغوص في التطبيق العملي لخوارزميات التشفير، وبناء وإدارة البنية التحتية للمفاتيح العامة (PKI)، وتأمين البيانات في جميع حالاتها (نقل، تخزين، استخدام). تقدم الدورة ورش عمل عملية تتضمن تشفير الأنظمة وإنشاء الشهادات الرقمية، مما يمنح المشاركين خبرة عملية مباشرة. نركز على الجانب الاستراتيجي لإدارة المفاتيح التشفيرية، والتعامل مع التحديات المستقبلية مثل الحوسبة الكمومية. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في أمن البيانات قادرين على تصميم وتنفيذ حلول تشفير قوية لحماية أصول المؤسسات الأكثر حساسية.