# التدريبية: التشفير المتقدم وأمن البيانات

# للأنظمة الحساسة الدورة

يونيو - ٠٢ يوليو ٢٠٢٦ ٢٨

عمان

(للشخص الواحد) € ٤١٠٠

Ref: #CYB4540_59238

## مقدمة الدورة التدريبية / لمحة عامة:

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

## لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- متخصصو الأمن السيبراني.
- مهندسو الشبكات والأنظمة.
- مطورون وباحثون في مجال الأمن.
- مديرو أمن المعلومات.
- مع بيانات حساسة. المهنيون العاملون في القطاعات الحيوية التي تتعامل
- 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.
- بيانات حساسة). إدارة العمليات (خاصة في الأنظمة التي تتعامل مع

## أهداف الدورة التدريبية:

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

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

## منهجية الدورة التدريبية:

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

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

### الوحدة الأولى: أساسيات التشفير وأمن البيانات

- مقدمة إلى مفاهيم التشفير والأمن السيبراني.
- وخوارزمياته (AES). التشفير المتماثل (Symmetric Encryption)
- وخوارزمياته (RSA). التشفير غير المتماثل (Asymmetric Encryption)
- 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.
- الإنترنت. بروتوكولات SSL/TLS وتأمين الاتصالات عبر
- تطبيق PKI في المؤسسات.
- التحديات في إدارة PKI.

## والتخزين الوحدة الثالثة: تأمين البيانات أثناء النقل

- 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.

## وتطبيقاتها الوحدة الرابعة: خوارزميات التشفير المتقدمة

- 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.

## الاستراتيجيات الوحدة الخامسة: إدارة المفاتيح التشفيرية ووضع

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

## 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 ٢٠-٢٥ 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:

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

## ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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