الدورة التدريبية: أمن قواعد البيانات SQL NoSQL: حماية المعلومات الحساسة



15 - 19 نوفمبر 2026
الدوحة
5500 € (للشخص الواحد)
Ref: #CYB5803_397449

مقدمة الدورة التدريبية / لمحة عامة:

تُعد قواعد البيانات هي القلب النابض لأي مؤسسة حديثة، حيث تخزن المعلومات الحساسة بدءًا من بيانات العملاء وحتى السجلات المالية والتشغيلية. في ظل تزايد التهديدات السيبرانية، أصبح تأمين قواعد البيانات SQL وNoSQL أولوية قصوى لحماية هذه الأصول الحيوية من الاختراق والوصول غير المصرح به. تقدم هذه الدورة التدريبية المتخصصة لمديري قواعد البيانات، مطوري التطبيقات، ومتخصصي الأمن السيبراني، المعرفة والمهارات اللازمة لتأمين قواعد البيانات بفعالية. سنتناول في هذه الدورة مفاهيم أمن قواعد البيانات الأساسية، نقاط الضعف الشائعة، أفضل الممارسات لتأمين SQL وNoSQL، والامتثال للوائح حماية البيانات. سيكتسب المشاركون القدرة على تحديد المخاطر الأمنية، تطبيق ضوابط أمنية قوية، والاستجابة للحوادث التي تستهدف قواعد البيانات. تهدف الدورة إلى بناء كوادر متخصصة في أمن قواعد البيانات لضمان سرية وسلامة وتوافر المعلومات. يستند المحتوى إلى أحدث المعايير الصناعية وأفضل الممارسات في أمن قواعد البيانات، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور رون بافليك (Ron Pavlick)، المعروف بأعماله في أمن قواعد البيانات والتحليل الجنائي الرقمي. يقدم BIG BEN Training Center هذه الدورة لمساعدة المؤسسات على حماية بياناتها الأكثر قيمة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو قواعد البيانات (DBAs).
- مهندسو ومطورو البرمجيات.
- متخصصو الأمن السيبراني.
- مهندسو البيانات وعلماء البيانات.
- مدققو الأنظمة الأمنية.
- المسؤولون عن حماية البيانات والخصوصية.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- الرعاية الصحية.
- شركات تطوير البرمجيات.
- التجارة الإلكترونية.
- الاتصالات.
- الهيئات الحكومية وما في حكمها.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة الأمن السيبراني.
- أقسام تطوير التطبيقات.
- إدارة البيانات.
- إدارة المخاطر والامتثال.

أهداف الدورة التدريبية:

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

- فهم مبادئ أمن قواعد البيانات لكل من SQL وNoSQL.
- تحديد نقاط الضعف الشائعة في قواعد البيانات.
- القدرة على تطبيق ضوابط المصادقة والترخيص القوية.
- تأمين قواعد البيانات ضد هجمات الحقن (SQL Injection).
- تشفير البيانات الحساسة داخل قواعد البيانات.
- إدارة الثغرات الأمنية والتصحيحات.
- الاستجابة الفعالة للحوادث الأمنية التي تستهدف قواعد البيانات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية ومكثفة، مصممة لتمكين المشاركين من فهم وتطبيق إجراءات أمن قواعد البيانات في بيئات حقيقية. سيتمكن المتدربون من خلال ورش العمل العملية التي تتضمن اختبار اختراق قواعد البيانات، وتطبيق التشفير، وضبط أذونات الوصول، من اكتساب خبرة مباشرة في تأمين قواعد البيانات SQL وNoSQL. تتضمن المنهجية مناقشات متعمقة حول نقاط الضعف الفريدة لكل نوع من قواعد البيانات، وأفضل الممارسات لتأمينها. سيتم التركيز على التعامل مع البيانات الحساسة، والامتثال للوائح حماية البيانات. يقدم BIG BEN Training Center هذه الدورة لتزويد المشاركين بالمهارات اللازمة لحماية المعلومات الحساسة من الاختراق والسرقة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن قواعد البيانات ومفاهيمها

- مقدمة إلى أهمية أمن قواعد البيانات.
- الفرق بين قواعد بيانات SQL وNoSQL.
- مخاطر أمن قواعد البيانات الشائعة.
- مبادئ أمن قواعد البيانات (السرية، السلامة، التوافر).
- نقاط الضعف في تصميم قواعد البيانات.
- أمثلة على حوادث اختراق قواعد البيانات.
- التحديات الفريدة في تأمين NoSQL.

الوحدة الثانية: المصادقة والترخيص وأمن الوصول

- إدارة المستخدمين والأذونات في قواعد بيانات SQL.
- آليات المصادقة القوية (المصادقة متعددة العوامل).
- الترخيص (Authorization) والتحكم في الوصول الدقيق (Granular Access Control).
- أمن كلمات المرور وسياسات تعقيد كلمات المرور.
- إدارة الوصول المستندة إلى الدور (RBAC).
- أذونات الوصول في قواعد بيانات NoSQL.
- مراقبة الوصول إلى البيانات الحساسة.

الوحدة الثالثة: تأمين البيانات داخل قواعد البيانات

- تشفير البيانات المخزنة (Data-at-rest).
- التشفير الشفاف للبيانات (Transparent Data Encryption - TDE).
- التشفير على مستوى الأعمدة والصفوف.
- تقنيات إخفاء البيانات (Data Masking) والترميز (Tokenization).
- حماية البيانات الحساسة (Sensitive Data Protection).
- التشفير في قواعد بيانات NoSQL.
- إدارة المفاتيح التشفيرية لتشفير قواعد البيانات.

الوحدة الرابعة: حماية قواعد البيانات من الهجمات والتهديدات

- الحماية من هجمات حقن SQL (SQL Injection).
- التصحيح (Patching) وإدارة الثغرات الأمنية.
- مراجعة التكوينات الآمنة لقواعد البيانات.
- مراقبة نشاط قواعد البيانات (Database Activity Monitoring - DAM).
- الحماية من هجمات حجب الخدمة (DDoS).
- أمن النسخ الاحتياطية (Backup Security).
- التعامل مع هجمات Zero-day في قواعد البيانات.

الوحدة الخامسة: الامتثال، الاستجابة للحوادث، ومستقبل أمن قواعد البيانات

- الامتثال للوائح حماية البيانات (GDPR, HIPAA, PCI DSS).
- وضع خطة الاستجابة للحوادث الأمنية لقواعد البيانات.
- التحقيق الجنائي الرقمي في اختراقات قواعد البيانات.
- التعافي من الكوارث واستمرارية الأعمال.
- التدقيق الأمني الدوري لقواعد البيانات.
- أمن قواعد البيانات في السحابة.
- مستقبل أمن قواعد البيانات (الذكاء الاصطناعي في الأمن).

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 لأنواع قواعد البيانات (SQL وNoSQL) وظهور تحديات أمنية جديدة مع كل تقنية، كيف يمكن لمتخصصي الأمن ومديري قواعد البيانات أن يبتكرون استراتيجيات أمنية متكاملة لا تقتصر على حماية البيانات الحالية، بل تتوقع نقاط الضعف المستقبلية وتُنشئ بيئة بيانات مرنة وآمنة قادرة على التكيف مع التهديدات المتغيرة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على أمن قواعد البيانات لكل من SQL وNoSQL، مما يوفر محتوى مصممًا خصيصًا لحماية المعلومات الحساسة في مختلف البيئات. بدلاً من تناول أمن المعلومات بشكل عام، نغوص في التطبيق العملي لتأمين قواعد البيانات، بدءًا من المصادقة والترخيص وصولاً إلى التشفير المتقدم والاستجابة للحوادث. تقدم الدورة ورش عمل عملية تتضمن اختبارات اختراق محاكاة وتطبيق ضوابط أمنية حقيقية، مما يمنح المشاركين خبرة عملية مباشرة. نركز على التعامل مع التحديات الفريدة لكل نوع من قواعد البيانات، والامتثال للوائح حماية البيانات. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في أمن قواعد البيانات قادرين على حماية الأصول الرقمية الأكثر قيمة للمؤسسات.