الدورة التدريبية: أمان البيانات في بيئات الحوسبة السحابية المختلطة ـ حماية الأصول الرقمية

#DM8153

الدورة التدريبية: أمان البيانات في بيئات الحوسبة السحابية المختلطة ـ حماية الأصول الرقمية

مقدمة الدورة التدريبية / لمحة عامة:

مع التوسع المتزايد لتبني الحوسبة السحابية، أصبحت المؤسسات تعتمد بشكل متزايد على البيئات السحابية المختلطة التي تجمع بين البنى التحتية السحابية العامة والخاصة، أو بين السحابة والمواقع المحلية. هذا النموذج، على الرغم من مرونته وفعاليته، يقدم تحديات فريدة ومعقدة في مجال أمان البيانات. تبرز الحاجة الملحة إلى فهم آليات حماية البيانات عبر هذه البيئات المتنوعة لضمان سرية، سلامة، وتوافر المعلومات الحساسة. تقدم هذه الدورة التدريبية من BIG BEN Training Center منهجاً شاملاً يغطي أفضل الممارسات والاستراتيجيات لتعزيز أمان البيانات في بيئات الحوسبة السحابية المختلطة. ستتناول الدورة المفاهيم الأساسية للأمن السحابي، تحديات الحماية، أدوات وتقنيات التشفير، إدارة الهوية والوصول، والامتثال للوائح والتشريعات. تستند الدورة إلى رؤى أكاديمية وعملية من خبراء مرموقين في الأمن السيبراني والبنية التحتية السحابية، مثل Bruce Schneier (بروس شناير)، وهو خبير أمان كمبيوتر وكاتب معروف بأعماله في التشفير وأمن الشبكات، مما يضمن محتوى غنياً بالمعرفة النظرية والتطبيقية. ستمكن هذه الدورة المتدربين من بناء إطارات أمنية قوية ومتكاملة، مما يعزز قدرتهم على حماية أصولهم الرقمية والتخفيف من المخاطر المحتملة في بيئات السحابة المختلطة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو أمن المعلومات.
- مديرو أمن البيانات.
- مهندسو السحابة.
- مديرو البنية التحتية لتكنولوجيا المعلومات.
- المتخصصون في الامتثال والتدقيق.
- مدققو الأمن السيبراني.
- صناع القرار في مجال تكنولوجيا المعلومات.

القطاعات والصناعات المستهدفة:

- الخدمات المصرفية والمالية.
- الرعاية الصحية.
- الحكومة والهيئات الحكومية وما في حكمها.
- التكنولوجيا والاتصالات.
- الخدمات السحابية.
- التعليم.
- التصنيع.

الأقسام المؤسسية المستهدفة:

- أمن المعلومات.
- تكنولوجيا المعلومات (IT).
- العمليات (Operations).
- المخاطر والامتثال.
- التدقيق الداخلي.
- البنية التحتية للشبكات.
- تطوير البرمجيات (DevSecOps).

أهداف الدورة التدريبية:

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

- فهم مبادئ وتحديات أمان البيانات في السحابة المختلطة.
- تحديد الفجوات الأمنية الشائعة في البيئات السحابية.
- تطبيق أفضل الممارسات لحماية البيانات في السحابة العامة والخاصة.
- استخدام تقنيات التشفير المتقدمة للبيانات.
- إدارة الهوية والوصول (IAM) بفعالية عبر السحابة.
- تأمين الشبكات في بيئات الحوسبة السحابية المختلطة.
- الامتثال للمعايير واللوائح الأمنية (GDPR، HIPAA).
- تطوير استراتيجيات الاستجابة للحوادث الأمنية.
- مراقبة التهديدات واكتشاف الانتهاكات الأمنية.
- بناء إطار عمل شامل لأمن السحابة المختلطة.

منهجية الدورة التدريبية:

تتبنى هذه الدورة التدريبية منهجية عملية وتفاعلية، مصممة لتمكين المشاركين من مواجهة تحديات أمان البيانات في بيئات الحوسبة السحابية المختلطة. يتم تقديم المحتوى من خلال مزيج من المحاضرات التفاعلية، التي تشرح المفاهيم المعقدة للأمن السحابي، وأفضل الممارسات، وأحدث التهديدات، وورش العمل التطبيقية المكثفة التي تتيح للمشاركين تطبيق استراتيجيات حماية البيانات عملياً. سيشارك المتدربون في دراسات حالة مستوحاة من سيناريوهات أمنية واقعية، مما يمكنهم من تحليل نقاط الضعف ووضع حلول دفاعية فعالة. يعزز العمل الجماعي مهارات التعاون وتبادل الخبرات في تصميم بنى أمنية مرنة وقوية، بينما تتيح الجلسات التفاعلية فرصة لطرح الأسئلة وتلقي تغذية راجعة من المدربين الخبراء. يحرص BIG BEN Training Center على توفير بيئة تعليمية غنية بالأمثلة والأدوات الحديثة، لضمان اكتساب المتدربين خبرة عملية مباشرة في تأمين بيئات السحابة المختلطة والامتثال للوائح. تهدف هذه المنهجية إلى تزويد المشاركين بالمهارات اللازمة ليصبحوا خبراء في أمن البيانات السحابية، قادرين على حماية الأصول الرقمية لمؤسساتهم بفعالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى الحوسبة السحابية المختلطة وأمن البيانات.

- مفاهيم الحوسبة السحابية (العامة، الخاصة، المختلطة).
- تحديات أمان البيانات في بيئات السحابة المختلطة.
- نموذج المسؤولية المشتركة في السحابة.
- المخاطر الأمنية الشائعة في السحابة المختلطة.
- المفاهيم الأساسية لأمن البيانات (السرية، السلامة، التوافر).
- الأطر والمعايير الأمنية (NIST، ISO 27001).
- الفرق بين أمن البيانات وأمن الشبكات في السحابة.

الوحدة الثانية: حماية البيانات في السحابة العامة.

- تأمين التخزين السحابي (Object Storage، Block Storage).
- استخدام تقنيات التشفير للبيانات في حالة السكون والحركة.
- إدارة مفاتيح التشفير (Key Management).
- أمان قواعد البيانات السحابية.
- تأمين حاويات التطبيقات والخدمات بدون خادم.
- التعامل مع مخاطر التكوين الخاطئ (Misconfiguration).
- أفضل الممارسات الأمنية لمقدمي الخدمات السحابية.

الوحدة الثالثة: أمن البنية التحتية السحابية المختلطة.

- تأمين الاتصال بين السحابة والمواقع المحلية (VPN، Direct Connect).
- جدران الحماية السحابية وقوائم التحكم في الوصول.
- إدارة الهوية والوصول (IAM) عبر البيئات المختلطة.
- التحكم في الوصول المستند إلى الدور (RBAC).
- المصادقة متعددة العوامل (MFA).
- تأمين الخوادم الافتراضية والحاويات.
- استراتيجيات تقسيم الشبكة (Network Segmentation).

الوحدة الرابعة: إدارة الامتثال، المراقبة، والاستجابة للحوادث.

- متطلبات الامتثال واللوائح (GDPR، HIPAA، PCI DSS).
- إدارة المخاطر والتهديدات.
- أدوات المراقبة والتسجيل (Logging and Monitoring).
- الكشف عن التهديدات والاستجابة لها (Incident Response).
- الطب الشرعي الرقمي في البيئات السحابية.
- التخطيط لاستمرارية الأعمال والتعافي من الكوارث.
- المراجعات الأمنية والتدقيق.

الوحدة الخامسة: استراتيجيات متقدمة لأمن البيانات السحابية.

- أمان البيانات الاصطناعية (Synthetic Data).
- أمان البيانات الضخمة في السحابة.
- التعلم الآلي في الكشف عن التهديدات.
- التحليلات الأمنية المتقدمة.
- DevSecOps في بيئات السحابة المختلطة.
- التحديات المستقبلية في أمن السحابة المختلطة.
- بناء خطة شاملة لأمن البيانات السحابية.

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 المشهد المتطور باستمرار لتهديدات الأمن السيبراني، كيف يمكن للمؤسسات التي تعتمد على الحوسبة السحابية المختلطة أن تضمن بقاء استراتيجياتها الأمنية مرنة وقادرة على التكيف، بحيث لا تقتصر على الاستجابة للتهديدات الحالية فحسب، بل تستبق التحديات المستقبلية لحماية بياناتها الحساسة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتركيزها المتخصص والعميق على تحديات وحلول أمان البيانات في بيئات الحوسبة السحابية المختلطة، مما يوفر للمشاركين فهماً استراتيجياً وعملياً لكيفية تأمين أصولهم الرقمية في هذه البنى التحتية المعقدة. يقدم BIG BEN Training Center محتوى متقدماً يغطي جوانب أمن البيانات من الألف إلى الياء، بدءاً من تقنيات التشفير وإدارة الهوية والوصول، وصولاً إلى الامتثال للوائح والاستجابة للحوادث الأمنية. تبرز الدورة بتوفيرها لدراسات حالة واقعية وتمارين تطبيقية، مما يتيح للمشاركين اكتساب خبرة مباشرة في تطبيق أفضل الممارسات في الأمن السحابي. هذا النهج المتكامل يضمن أن يكتسب المتدربون ليس فقط المعرفة العميقة، بل أيضاً الكفاءات العملية اللازمة ليصبحوا قادة في مجال أمن البيانات السحابية، قادرين على حماية مؤسساتهم من التهديدات المتزايدة في المشهد الرقمي.