الدورة التدريبية: أمن المعلومات المتقدم في بيئات الحوسبة السحابية



28 ديسمبر 2026 - 01 يناير 2027
شرم الشيخ
4100 € (للشخص الواحد)
Ref: #IT7247_432292

مقدمة الدورة التدريبية / لمحة عامة:

أصبحت الحوسبة السحابية جزءًا لا يتجزأ من البنية التحتية لمعظم المؤسسات، لما تقدمه من مرونة، كفاءة، وقدرة على التوسع. ومع هذا الاعتماد المتزايد، تتصاعد كذلك المخاطر والتحديات الأمنية المرتبطة بتخزين البيانات ومعالجتها في البيئات السحابية. إن حماية المعلومات الحساسة وضمان الامتثال للمعايير التنظيمية يُعد أمرًا بالغ الأهمية لنجاح أي استراتيجية سحابية. تقدم هذه الدورة التدريبية من BIG BEN Training Center فهمًا شاملًا لمفاهيم أمن المعلومات في الحوسبة السحابية، بدءًا من نماذج الخدمة السحابية المختلفة (IaaS, PaaS, SaaS) ونماذج النشر (عامة، خاصة، هجينة)، وصولًا إلى التهديدات الأمنية الشائعة والاستراتيجيات المتقدمة للحماية. سيتعلم المشاركون كيفية تأمين البنية التحتية السحابية، وحماية البيانات، وإدارة الهوية والوصول، بالإضافة إلى فهم المتطلبات التنظيمية والامتثال للمعايير الأمنية السحابية. تركز الدورة على الجوانب النظرية والتطبيقية، مستلهمة من أفكار خبراء الأمن السيبراني مثل البروفيسور ويليام ستالينغز (William Stallings)، المعروف بأعماله الأكاديمية في أمن الشبكات وأنظمة الكمبيوتر، مما يضمن تزويد المتدربين بمعرفة عميقة ومحدثة. يهدف BIG BEN Training Center إلى تمكين المتدربين من تصميم وتطبيق استراتيجيات أمن سحابي فعالة تحمي أصولهم الرقمية في العصر السحابي.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الأمن السحابي.
- مديرو أمن المعلومات.
- متخصصو الأمن السيبراني.
- مهندسو الشبكات والبنية التحتية.
- مدققو الأنظمة السحابية.
- مديرو تقنية المعلومات.
- مطورو التطبيقات السحابية.

القطاعات والصناعات المستهدفة:

- الشركات التي تستخدم أو تخطط للانتقال إلى الحوسبة السحابية.
- مزودو الخدمات السحابية.
- القطاع المالي والمصرفي.
- قطاع التكنولوجيا والاتصالات.
- القطاع الحكومي.
- قطاع الرعاية الصحية.
- شركات تطوير البرمجيات.

الأقسام المؤسسية المستهدفة:

- أقسام الأمن السيبراني.
- إدارات تكنولوجيا المعلومات.
- أقسام البنية التحتية السحابية.
- أقسام الامتثال والمخاطر.
- أقسام تطوير التطبيقات.
- إدارات التدقيق الداخلي.

أهداف الدورة التدريبية:

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

- فهم تحديات أمن المعلومات في بيئات الحوسبة السحابية.
- تحديد التهديدات الأمنية الشائعة ونقاط الضعف في السحابة.
- تطبيق مبادئ أمن البيانات والخصوصية في البيئات السحابية.
- إدارة الهوية والوصول (IAM) في السحابة بفعالية.
- تأمين البنية التحتية كخدمة (IaaS) والمنصات كخدمة (PaaS).
- حماية التطبيقات والبيانات في البرمجيات كخدمة (SaaS).
- الامتثال للمعايير واللوائح الأمنية السحابية (مثل ISO 27017, CSA STAR).
- تصميم وتنفيذ استراتيجيات أمن سحابي قوية.
- الاستجابة للحوادث الأمنية في البيئات السحابية.

منهجية الدورة التدريبية:

يقدم BIG BEN Training Center هذه الدورة التدريبية بمنهجية شاملة وتفاعلية، تجمع بين المعرفة النظرية المتعمقة لأمن المعلومات في الحوسبة السحابية والتطبيقات العملية المكثفة. تعتمد المنهجية على محاضرات تُعزز بدراسات حالة واقعية تُحلل سيناريوهات أمنية معقدة وتُقدم حلولًا مبتكرة في البيئات السحابية المختلفة. تُشجع ورش العمل الجماعية المتدربين على تصميم بنى أمنية سحابية، وتكوين أدوات أمنية، ومحاكاة الاستجابة للحوادث، مما يعزز الفهم العملي وتبادل الخبرات. تُعد الجلسات التفاعلية جزءًا أساسيًا من المنهجية، حيث تتيح طرح الأسئلة، والمناقشات المفتوحة، وتلقي التغذية الراجعة الفورية من المدربين الخبراء. يتم استخدام بيئات سحابية افتراضية وأدوات أمن سحابية متخصصة، مما يُمكّن المتدربين من ممارسة التقنيات وتطوير قدراتهم في بيئة آمنة ومتحكم بها. يهدف هذا النهج إلى تزويد المتدربين بالمهارات اللازمة لمواجهة تحديات الأمن السحابي بفعالية، وحماية أصول مؤسساتهم الرقمية، وضمان الامتثال للمعايير العالمية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الحوسبة السحابية ومخاطرها الأمنية.

- مقدمة إلى الحوسبة السحابية ونماذج الخدمة (IaaS, PaaS, SaaS).
- نماذج النشر السحابي (عامة، خاصة، هجينة، مجتمعية).
- نموذج المسؤولية المشتركة (Shared Responsibility Model).
- أهم التهديدات الأمنية في البيئات السحابية.
- نقاط الضعف الشائعة في البنى التحتية السحابية.
- التحديات الأمنية الفريدة للحوسبة السحابية.
- المفاهيم الأساسية لأمن المعلومات في السحابة.

الوحدة الثانية: تأمين البنية التحتية كخدمة (IaaS).

- أمن الشبكات السحابية (Virtual Networks, Security Groups).
- تأمين الحوسبة السحابية (Virtual Machines, Containers).
- أمن التخزين السحابي (Object Storage, Block Storage).
- إدارة الهوية والوصول (IAM) في IaaS.
- أمن الخوادم الافتراضية.
- إدارة الثغرات الأمنية في IaaS.
- المراقبة والتسجيل في بيئات IaaS.

الوحدة الثالثة: أمن المنصات (PaaS) والبرمجيات (SaaS) كخدمة.

- تأمين المنصات كخدمة (PaaS Security).
- حماية التطبيقات على PaaS.
- أمن قواعد البيانات كخدمة (DBaaS).
- التهديدات الأمنية لتطبيقات SaaS.
- أمن بيانات المستخدم في SaaS.
- تقييم واعتماد مزودي SaaS.
- أفضل الممارسات لتكوين PaaS وSaaS بأمان.

الوحدة الرابعة: حوكمة الأمن السحابي والامتثال.

- معايير الأمن السحابي (ISO 27017, CSA STAR).
- لوائح حماية البيانات (GDPR, CCPA).
- أطر عمل الحوكمة السحابية والمخاطر والامتثال (GRC).
- إدارة المخاطر في البيئات السحابية.
- إجراء عمليات التدقيق الأمني السحابي.
- وضع سياسات أمن سحابي فعالة.
- الاستجابة للحوادث الأمنية في السحابة.

الوحدة الخامسة: التشفير وأمن البيانات والاتجاهات المستقبلية.

- تشفير البيانات في حالة السكون وأثناء النقل.
- إدارة مفاتيح التشفير (Key Management).
- أمن البيانات الحساسة في السحابة.
- التعلم الآلي والذكاء الاصطناعي في أمن السحابة.
- أمن الحوسبة الخالية من الخوادم (Serverless Security).
- أمن الحوسبة المتطورة (Edge Computing Security).
- مستقبل أمن المعلومات في الحوسبة 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:

كيف يمكن للمؤسسات التي تعتمد على نماذج نشر سحابية متعددة (Multi-cloud) إدارة التعقيدات الأمنية الناتجة عن اختلاف الضوابط والسياسات بين المزودين المختلفين، مع ضمان مستوى عالٍ من الحماية والامتثال؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها لنهج متكامل وعملي في مجال أمن المعلومات في الحوسبة السحابية، مما يجعلها مختلفة عن الدورات التي قد تركز على جانب واحد فقط من جوانب الأمن السحابي. يلتزم BIG BEN Training Center بتزويد المتدربين بمعرفة عميقة وشاملة تغطي كافة نماذج الخدمة والنشر، مع التركيز على التحديات الأمنية الفعلية والحلول العملية. يتميز التدريب بدمج دراسات حالة واقعية وتمارين تطبيقية تُمكن المتدربين من التعامل مع سيناريوهات أمنية معقدة في بيئات سحابية حقيقية، مما يعزز من قدرتهم على تطبيق المفاهيم النظرية بفعالية. كما تتناول الدورة أحدث الاتجاهات والتقنيات في أمن السحابة، مثل التعلم الآلي وأمن الحوسبة الخالية من الخوادم، مما يُعد المشاركين للمستقبل. هذا المزيج الفريد من العمق النظري، والتطبيق العملي، والرؤية المستقبلية، يُمكّن خريجي هذه الدورة من أن يصبحوا خبراء في تأمين البيئات السحابية، قادرين على حماية الأصول الرقمية لمؤسساتهم بفعالية وثقة.