الدورة التدريبية: أمن الأنظمة السحابية والبيئات الهجينة المتقدمة



14 - 18 ديسمبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #SM6286_340593

مقدمة الدورة التدريبية / لمحة عامة:

مع التوسع الهائل في الاعتماد على الحوسبة السحابية والبيئات الهجينة، أصبح أمن الأنظمة السحابية والبيئات الهجينة المتقدمة من أهم التحديات التي تواجه المؤسسات في جميع القطاعات. تتطلب حماية البيانات والتطبيقات في هذه البيئات فهمًا عميقًا للبنى التحتية السحابية، ونقاط الضعف المحتملة، وأفضل الممارسات لتأمينها. هذه الدورة التدريبية الشاملة مصممة لتزويد متخصصي الأمن السيبراني وتقنية المعلومات بالمعرفة والمهارات المتقدمة اللازمة لتصميم، وتنفيذ، وإدارة حلول أمنية قوية للأنظمة السحابية والبيئات الهجينة. سنتعمق في استراتيجيات أمن السحابة، إدارة الهوية والوصول، تشفير البيانات، ومراقبة التهديدات في السحابة. تستند الدورة إلى أعمال خبراء أكاديميين بارزين في مجال أمن الحوسبة السحابية، مثل البروفيسور Indrakshi Ray، التي تُعرف بأبحاثها في أمن البيانات والخصوصية في السحابة. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من حماية أصولهم في السحابة، وتقليل المخاطر، وضمان الامتثال للمعايير الأمنية العالمية. سيركز التدريب على الجوانب التطبيقية والعملية، مع تقديم دراسات حالة واقعية وتمارين محاكاة، لمساعدة المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم المعقدة، وتعزيز قدراتهم على مواجهة التحديات الأمنية بفعالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الأمن السحابي.
- مهندسو DevOps/SecOps.
- مديرو الأمن السيبراني.
- مسؤولو أمن المعلومات.
- مهندسو الشبكات والسحابة.
- المطورون العاملون على تطبيقات سحابية.
- مدققو الأمن.

القطاعات والصناعات المستهدفة:

- شركات تقنية المعلومات والبرمجيات.
- مزودو الخدمات السحابية.
- القطاع المالي والمصرفي.
- الحكومة والقطاع العام.
- التجارة الإلكترونية والتجزئة.
- الرعاية الصحية.
- الشركات الكبرى متعددة الجنسيات.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة تقنية المعلومات.
- إدارة البنية التحتية.
- فرق تطوير البرمجيات.
- إدارة المخاطر والامتثال.
- العمليات السحابية.
- الاستراتيجية الرقمية.

أهداف الدورة التدريبية:

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

- فهم نماذج النشر السحابي وأنواع الخدمات (IaaS, PaaS, SaaS).
- تطبيق مبادئ الأمن السحابي وإدارة المخاطر.
- تأمين الهوية والوصول في البيئات السحابية.
- حماية البيانات في السحابة (التشفير، DLP).
- مراقبة التهديدات والاستجابة للحوادث في البيئات السحابية.
- تكوين أمن الشبكات السحابية وجدران الحماية.
- إدارة الامتثال والمتطلبات التنظيمية لأمن السحابة.
- تأمين البيئات الهجينة (Hybrid Clouds) بشكل فعال.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وعملية مكثفة، تهدف إلى تزويد المشاركين بفهم عميق ومهارات تطبيقية في مجال أمن الأنظمة السحابية والبيئات الهجينة المتقدمة. تبدأ المنهجية بمحاضرات متعمقة يقدمها خبراء متخصصون في أمن السحابة، يليها جلسات نقاش حيوية لتبادل الخبرات والتحديات التي يواجهها المشاركون في بيئات عملهم. تركز الدورة بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل سيناريوهات اختراق سحابي، وتقييم الثغرات في بيئات هجينة، وتطوير استراتيجيات للحماية والاستجابة. تتضمن المنهجية ورش عمل تطبيقية ومختبرات افتراضية، تتيح للمتدربين تكوين سياسات أمنية في منصات سحابية رائدة (مثل AWS، Azure، GCP)، وإدارة الهوية والوصول، وتطبيق حلول التشفير. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات حل المشكلات تحت الضغط. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة لحماية أصولهم في السحابة وضمان أمان ومرونة البيئات الهجينة المعقدة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن الحوسبة السحابية والبيئات الهجينة

- مقدمة إلى نماذج الحوسبة السحابية وأنواع الخدمات (IaaS, PaaS, SaaS).
- مفاهيم الأمن في السحابة والنموذج المسؤولية المشتركة.
- التهديدات الأمنية الشائعة في البيئات السحابية والهجينة.
- تصميم بنية أمنية سحابية قوية.
- أهمية أمن البيئات الهجينة (On-Premise + Cloud).
- المعايير وأطر العمل لأمن السحابة (CSA CCM، NIST CSF).
- الفرق بين أمن السحابة وأمن مركز البيانات التقليدي.

الوحدة الثانية: إدارة الهوية والوصول وحماية البيانات في السحابة

- إدارة الهوية والوصول (IAM) في البيئات السحابية.
- مبادئ الامتياز الأقل (Least Privilege).
- التحقق متعدد العوامل (MFA) وتأمينه في السحابة.
- حماية البيانات في حالة السكون وأثناء النقل (Data at Rest/in Transit).
- تقنيات التشفير المتقدمة في السحابة.
- منع فقدان البيانات (DLP) في البيئات السحابية.
- إدارة المفاتيح وتخزين الأسرار (Key Management).

الوحدة الثالثة: أمن الشبكات السحابية والبنية التحتية كخدمة (IaaS)

- تأمين الشبكات الافتراضية الخاصة بالسحابة (VPCs).
- جدران الحماية السحابية وقوائم التحكم في الوصول (ACLs).
- أمن الحوسبة عديمة الخادم (Serverless Security).
- تأمين حاويات (Containers) وأوركسترا الحاويات (Kubernetes).
- إدارة الثغرات الأمنية في البنية التحتية السحابية.
- أمن واجهات برمجة التطبيقات (APIs) في السحابة.
- أمن التكوين (Configuration Security) في السحابة.

الوحدة الرابعة: أمن المنصات كخدمة (PaaS) والبرمجيات كخدمة (SaaS)

- تأمين خدمات PaaS (مثل قواعد البيانات المدارة، منصات التطوير).
- مراجعة أمن التطبيقات المبنية على PaaS.
- تقييم الأمن لموردي SaaS.
- إدارة المخاطر في تطبيقات SaaS.
- أمن البرمجيات كخدمة (Software-as-a-Service Security).
- التكامل الآمن بين الخدمات السحابية المختلفة.
- التعامل مع التهديدات الموجهة لتطبيقات SaaS.

الوحدة الخامسة: مراقبة الأمن، الاستجابة للحوادث، والامتثال السحابي

- مراقبة السجلات (Logging) والتدقيق (Auditing) في السحابة.
- أدوات وأنظمة إدارة معلومات وأحداث الأمن (SIEM) السحابية.
- الاستجابة للحوادث الأمنية في البيئات السحابية.
- خطط التعافي من الكوارث في السحابة.
- الامتثال للمتطلبات التنظيمية في السحابة (GDPR، HIPAA، ISO 27017).
- تقييم المخاطر المستمر لأمن السحابة.
- أتمتة الأمن السحابي (Cloud Security Automation).

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 لخدمات الحوسبة السحابية والتهديدات السيبرانية، كيف يمكن للمؤسسات أن تضمن أقصى درجات الأمان والامتثال مع الحفاظ على مرونة التوسع والابتكار في بيئاتها السحابية والهجينة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتقدم والشمولي على أمن الأنظمة السحابية والبيئات الهجينة المتقدمة، وهو ما يميزها عن الدورات التي تغطي جانبًا واحدًا فقط من أمن السحابة. نحن لا نكتفي بتقديم المفاهيم النظرية، بل نغوص في التطبيقات العملية من خلال ورش عمل مكثفة وتمارين مختبرية على منصات سحابية حقيقية، مما يمنح المشاركين خبرة مباشرة لا تقدر بثمن. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث التهديدات والحلول الأمنية في هذا المجال الحيوي والمتغير باستمرار. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء قادرين على تصميم، وتنفيذ، وإدارة استراتيجيات أمنية قوية للبيئات السحابية والهجينة، مما يعزز مرونة المؤسسات وقدرتها على مواجهة التحديات السيبرانية بفعالية استثنائية.