الدورة التدريبية: تأمين البنية التحتية السحابية للشركات (AWS, Azure, Google Cloud)



18 - 22 اكتوبر 2026
المنامة
4400 € (للشخص الواحد)
Ref: #CYB4290_397277

مقدمة الدورة التدريبية / لمحة عامة:

في العصر الرقمي الحالي، أصبحت البنية التحتية السحابية العمود الفقري للعديد من الشركات، مما يجعل أمن السحابة أولوية قصوى لضمان حماية البيانات والأصول الرقمية. تركز هذه الدورة التدريبية المتخصصة على تزويد المهنيين بالمعرفة والمهارات اللازمة لتأمين بيئات السحابة عبر المنصات الرائدة مثل AWS وAzure وGoogle Cloud. سيتعلم المشاركون أفضل ممارسات أمن السحابة، وكيفية تكوين الإعدادات الأمنية، وإدارة الهوية والوصول (IAM)، وحماية الشبكات السحابية. سنغطي بالتفصيل مخاطر الأمن السيبراني في السحابة وكيفية التخفيف منها، بالإضافة إلى الامتثال للوائح الأمنية السحابية. تهدف الدورة إلى تمكين فرق تكنولوجيا المعلومات والأمن من بناء بنى تحتية سحابية آمنة ومرنة في مواجهة التهديدات السيبرانية المتزايدة. يستند المحتوى إلى أحدث المعايير الصناعية والممارسات الموصي بها، مع الاستفادة من خبرات خبراء مثل البروفيسور سكوت تشارني (Scott Charney)، الذي عمل في Microsoft وكان له دور كبير في أمن السحابة والبنى التحتية الحرجة. يقدم BIG BEN Training Center هذه الدورة لمساعدة الشركات على تحقيق أقصى استفادة من الخدمات السحابية مع الحفاظ على أعلى مستويات الأمن السيبراني.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو السحابة ومسؤولون الأنظمة السحابية.
- متخصصو الأمن السيبراني ومديرو أمن المعلومات.
- مهندسو DevOps ومطورو البرمجيات العاملون في بيئات سحابية.
- مدققو أمن المعلومات ومدققو الامتثال.
- مديرو البنية التحتية لتكنولوجيا المعلومات.
- أي مهني يعمل مع المنصات السحابية الرئيسية (AWS, Azure, Google Cloud).

القطاعات والصناعات المستهدفة:

- شركات التكنولوجيا وشركات تطوير البرمجيات.
- القطاع المالي والتأمين الذي يعتمد على السحابة لخدماته.
- قطاع الاتصالات والخدمات الرقمية.
- قطاع التجزئة والتجارة الإلكترونية.
- القطاع الحكومي والهيئات العامة وما في حكمها التي تنتقل إلى البيئات السحابية.
- الرعاية الصحية وشركات الأدوية التي تخزن بيانات حساسة في السحابة.

الأقسام المؤسسية المستهدفة:

- إدارة البنية التحتية لتكنولوجيا المعلومات.
- إدارة الأمن السيبراني وأمن المعلومات.
- أقسام DevOps وتطوير البرمجيات.
- إدارة المخاطر والامتثال.
- فريق عمليات تكنولوجيا المعلومات (IT Operations).

أهداف الدورة التدريبية:

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

- فهم نماذج المسؤولية المشتركة في أمن السحابة.
- تطبيق أفضل ممارسات أمن السحابة عبر AWS وAzure وGoogle Cloud.
- القدرة على تكوين وإدارة هويات المستخدمين والصلاحيات في السحابة (IAM).
- تأمين الشبكات الافتراضية ونقاط النهاية في البيئات السحابية.
- حماية البيانات المخزنة والمنقولة في السحابة.
- التعرف على أدوات وخدمات الأمن السحابي المتاحة.
- الامتثال للوائح الأمنية السحابية ومعايير الصناعة.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية شاملة تجمع بين المفاهيم النظرية المتقدمة والتطبيق العملي المكثف، مع التركيز على منصات السحابة الرئيسية (AWS, Azure, Google Cloud). سيتمكن المشاركون من خلال الجلسات التفاعلية والتمارين العملية من تطبيق مفاهيم الأمن السحابي مباشرة. تتضمن المنهجية دراسات حالة واقعية لأمن السحابة، مثل اختراقات السحابة الشهيرة وكيفية الوقاية منها. سيتم التركيز على تكوينات الأمان الموصي بها، وإدارة الثغرات الأمنية في البيئات السحابية، ومراقبة الأمن السحابي. يهدف BIG BEN Training Center إلى تزويد المشاركين بالمهارات اللازمة لتأمين البنية التحتية السحابية لشركاتهم بفعالية. يتم تشجيع النقاش وتبادل الخبرات بين المشاركين حول التحديات الأمنية المشتركة في السحابة وأفضل الحلول المتاحة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن السحابة ونماذجها

- مقدمة إلى الحوسبة السحابية وأنواع السحب.
- نموذج المسؤولية المشتركة في السحابة.
- مخاطر الأمن السيبراني في السحابة.
- أهمية تأمين البنية التحتية السحابية.
- مفاهيم الأمن الأساسية في بيئة السحابة.
- التحديات الأمنية لـ AWS Azureg Cloudg Google.
- استراتيجيات الانتقال الآمن إلى السحابة.

الوحدة الثانية: إدارة الهوية والوصول (IAM) في السحابة

- مفاهيم IAM في AWS IAM، Azure AD، Google Cloud IAM.
- إدارة المستخدمين والمجموعات والصلاحيات.
- تكوين مبدأ الامتياز الأقل.
- المصادقة متعددة العوامل (MFA) في السحابة.
- إدارة مفاتيح الوصول والأسرار في السحابة.
- أمن API والوصول البرمجي.
- مراجعة سجلات الوصول والتدقيق الأمني.

الوحدة الثالثة: أمن الشبكات والبيانات في البيئات السحابية

- تأمين الشبكات الافتراضية والشبكات الفرعية في السحابة.
- تكوين جدران الحماية (Security Groups, Network Security Groups).
- أمن الاتصال بين السحابة والبيئات المحلية.
- حماية البيانات المخزنة (Encryption at Rest) والمنقولة (Encryption in Transit).
- أمن قواعد البيانات السحابية.
- خدمات أمن البيانات في AWS, Azure, Google Cloud.
- أمن حاويات التخزين السحابي.

الوحدة الرابعة: حماية التطبيقات والامتثال في السحابة

- أمن التطبيقات السحابية وواجهات برمجة التطبيقات (APIs).
- تأمين بيئات DevOps وخطوط أنابيب CI/CD في السحابة.
- مراقبة الأمن السحابي واكتشاف التهديدات.
- الاستجابة للحوادث الأمنية في السحابة.
- الامتثال للوائح الأمنية السحابية (مثل HIPAA, GDPR).
- تقارير الامتثال والتدقيق السحابي.
- أمن الخدمات بلا خادم (Serverless Security).

الوحدة الخامسة: أدوات ومستقبل أمن السحابة

- أدوات الأمن السحابي المتقدمة في AWS Security Hub, Azure Security Center, Google Security Command Center.
- إدارة الثغرات الأمنية السحابية.
- أمن الذكاء الاصطناعي والتعلم الآلي في السحابة.
- أتمتة الأمن السحابي.
- الاتجاهات المستقبلية في أمن السحابة.
- التعاون مع مقدمي الخدمات السحابية بشأن الأمن.
- بناء إطار عمل أمني شامل للسحابة.

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 الاعتماد المتزايد على البنى التحتية السحابية المتعددة، كيف يمكن للشركات أن تبني استراتيجية أمن سحابي موحدة وفعالة تضمن حماية بياناتها عبر مختلف المنصات (AWS, Azure, Google Cloud)، مع الحفاظ على مرونة الابتكار وخفض التكاليف التشغيلية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والشامل على تأمين البنية التحتية السحابية عبر المنصات الثلاثة الرائدة: AWS Azureg وGoogle Cloudg. بدلاً من التركيز على منصة واحدة، نقدم رؤية متكاملة لأمن السحابة متعددة المنصات، مما يمنح المشاركين فهمًا أوسع وقدرة أكبر على التكيف. نغوص في أفضل الممارسات الأمنية لكل منصة، مع تسليط الضوء على أوجه التشابه والاختلاف في أدوات وخدمات الأمن. لا تقتصر الدورة على الجانب النظري، بل تقدم أمثلة عملية واقعية لتكوين الإعدادات الأمنية ومعالجة الثغرات. إنها ليست مجرد دورة لتعلم أدوات محددة، بل هي رحلة لفهم معمق لمبادئ الأمن السحابي، وكيفية تطبيقها بفعالية لضمان مرونة الشركات في البيئات السحابية المتطورة.