الدورة التدريبية: تأمين الاتصالات السحابية وحلول الحوسبة لبيئات العمل الرقمية



23 - 27 نوفمبر 2026
شرم الشيخ
4100 € (للشخص الواحد)
Ref: #TEL8863_428439

مقدمة الدورة التدريبية / لمحة عامة:

أصبح الانتقال إلى الخدمات السحابية (Cloud Services) حتمية للمؤسسات الحديثة التي تسعى لتحقيق المرونة، وكفاءة التكلفة، والابتكار. ومع هذا التحول، تبرز تحديات أمنية معقدة تتطلب فهمًا عميقًا لتأمين البيانات والاتصالات في البيئات السحابية. إن ضمان سرية وسلامة وتوافر المعلومات في السحابة لم يعد مجرد خيار، بل هو ضرورة قصوى للحفاظ على العمليات التشغيلية والثقة الرقمية. تقدم هذه الدورة التدريبية من BIG BEN Training Center فهمًا شاملاً للمفاهيم الأساسية والتقنيات المتقدمة في تأمين الاتصالات السحابية وحلول الحوسبة. سنتناول في هذه الدورة نماذج الخدمات السحابية (IaaS, PaaS, SaaS)، والمسؤولية المشتركة للأمن، وتشفير البيانات في السحابة، وإدارة الهوية والوصول (IAM). سيتعرف المشاركون على أحدث التهديدات الأمنية السحابية، وكيفية تنفيذ أفضل الممارسات الأمنية، والامتثال للمعايير التنظيمية. كما ستسلط الدورة الضوء على أهمية الأمن السيبراني في حماية البنية التحتية السحابية، والتطبيقات السحابية، والبيانات المخزنة. تستند محاور الدورة إلى أحدث المعايير الصناعية والأبحاث الأكاديمية في هذا المجال، مستلهمة من رؤى أكاديميين وخبراء مثل Thomas Erl في كتابه Cloud Computing: Concepts, Technology & Architecture، والذي يُعد مرجعًا في هندسة الحوسبة السحابية وأمنها. هذه الدورة هي بوابتك نحو إتقان تأمين الاتصالات السحابية وحلول الحوسبة، مما يمكنك من بناء بيئات سحابية آمنة وموثوقة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو أمن المعلومات.
- مدراء تقنية المعلومات.
- مهندسو الشبكات السحابية.
- مطورو التطبيقات السحابية.
- مدراء الامتثال والمخاطر.
- المحللون الأمنيون.
- المدققون الأمنيون.
- المتخصصون في أمن البيانات.
- مسؤولو البنية التحتية.

القطاعات والصناعات المستهدفة:

- شركات الخدمات السحابية (Cloud Providers).
- المؤسسات المالية والبنوك.
- قطاع الرعاية الصحية.
- الجهات الحكومية والوزارات.
- شركات تطوير البرمجيات.
- شركات الأمن السيبراني.
- قطاع التجزئة والتجارة الإلكترونية.
- شركات الاتصالات ومزودو الخدمة.
- الشركات التي تستخدم الحوسبة السحابية.

الأقسام المؤسسية المستهدفة:

- قسم أمن المعلومات.
- إدارة تقنية المعلومات (IT).
- قسم البنية التحتية السحابية.
- إدارة المخاطر والامتثال.
- قسم تطوير البرمجيات.
- إدارة العمليات (Ops).
- قسم الدعم الفني.
- إدارة العقود والمشتريات (لخدمات السحابة).
- قسم الحوكمة المؤسسية.

أهداف الدورة التدريبية:

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

- فهم نماذج الحوسبة السحابية وتصنيفاتها.
- تحديد المخاطر الأمنية الشائعة في السحابة.
- تطبيق مبادئ الأمن السيبراني على البيئات السحابية.
- إدارة الهوية والوصول (IAM) في السحابة.
- تنفيذ تقنيات التشفير لحماية البيانات.
- تأمين الشبكات السحابية والاتصالات.
- التعامل مع الامتثال التنظيمي والأطر الأمنية.
- اختيار أفضل حلول الأمن السحابي.
- الاستجابة للحوادث الأمنية في السحابة.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية عملية ومكثفة، مصممة لتزويد المشاركين بالمهارات اللازمة لتأمين الاتصالات السحابية وحلول الحوسبة بفعالية. ستبدأ الدورة بشرح نظري للمفاهيم الأساسية للحوسبة السحابية ومبادئ الأمن السيبراني، مدعومة بدراسات حالة واقعية لأمثلة على خروقات أمنية سحابية وكيفية تجنبها. سيشارك المتدربون في ورش عمل تطبيقية وجلسات تدريب عملية، حيث سيتعلمون كيفية تكوين إعدادات الأمان السحابي، وإدارة الهويات والوصول، وتنفيذ سياسات التشفير، وتأمين الاتصالات بين الخدمات السحابية. سيتم التركيز على التمارين العملية التي تحاكي سيناريوهات الهجمات الحقيقية، مما يتيح للمشاركين اكتساب خبرة مباشرة في التعامل مع مختلف تحديات الأمن السحابي. يقدم المدربون الخبراء في BIG BEN Training Center، الذين يمتلكون خبرة عملية واسعة في الأمن السيبراني السحابي، تغذية راجعة فورية ومخصصة. تهدف هذه المنهجية إلى بناء قدرات المتدربين على تحليل الثغرات الأمنية في البيئات السحابية، وتطبيق أفضل الممارسات لحماية البيانات والاتصالات، وضمان الامتثال للمعايير الأمنية، مما يمكنك من العمل بفعالية في بيئات الحوسبة السحابية المعقدة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الحوسبة السحابية ومخاطرها الأمنية.

- مقدمة إلى الحوسبة السحابية (تعريف، نماذج).
- نماذج الخدمة السحابية (IaaS, PaaS, SaaS).
- مفهوم المسؤولية المشتركة في الأمن السحابي.
- المخاطر الأمنية الشائعة في البيئات السحابية.
- أبرز الثغرات الأمنية السحابية.
- التحديات الفريدة لتأمين الاتصالات السحابية.
- أهمية الحوكمة في الأمن السحابي.

الوحدة الثانية: تأمين الهوية والوصول والبيانات في السحابة.

- إدارة الهوية والوصول (IAM) في البيئات السحابية.
- المصادقة متعددة العوامل (MFA).
- التحكم في الوصول المستند إلى الدور (RBAC).
- تشفير البيانات في حالة السكون (Data at Rest).
- تشفير البيانات أثناء النقل (Data in Transit).
- إدارة مفاتيح التشفير.
- حماية البيانات الحساسة في التخزين السحابي.

الوحدة الثالثة: أمن الشبكات والاتصالات السحابية.

- عزل الشبكة (Network Isolation).
- جدران الحماية السحابية (Cloud Firewalls).
- الشبكات الافتراضية الخاصة (VPNs).
- تأمين واجهات برمجة التطبيقات (APIs).
- أمن الاتصالات بين الخدمات السحابية.
- نظم كشف ومنع التطفل (IDS/IPS) في السحابة.
- إدارة حركة المرور (Traffic Management).

الوحدة الرابعة: أمن التطبيقات والحاويات والخدمات السحابية.

- أمن التطبيقات في السحابة.
- تأمين الحاويات (Containers) Kubernetesg.
- أمن وظائف بلا خادم (Serverless Functions).
- التهديدات المتقدمة (Advanced Threats) للهجمات.
- مراقبة سجلات الأمان (Security Logs).
- الاستجابة للحوادث الأمنية في السحابة.
- اختبار الاختراق (Penetration Testing) للتطبيقات السحابية.

الوحدة الخامسة: الامتثال، الحوكمة، وأفضل ممارسات الأمن السحابي.

- معايير الأمن السحابي (CSA, NIST).
- الامتثال للوائح (GDPR, HIPAA, PCI DSS).
- إدارة المخاطر السحابية.
- أفضل الممارسات لتأمين البيئات السحابية.
- تخطيط التعافي من الكوارث (DRP) في السحابة.
- تقييم مزودي الخدمات السحابية.
- مستقبل الأمن السحابي والتهديدات الناشئة.

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 التوسع اللامحدود للحوسبة السحابية واعتماد المؤسسات المتزايد عليها، ومع التطور المستمر لتهديدات الأمن السيبراني التي تستهدف هذه البيئات، كيف يمكن لمتخصصي الأمن تطوير استراتيجيات دفاعية استباقية لا تكتفي بردع الهجمات الحالية، بل تتنبأ بالتهديدات المستقبلية، وتضمن استمرارية الأعمال وحماية البيانات الحساسة في عالم رقمي سريع التغير؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها تركيزًا عميقًا وعمليًا على تأمين الاتصالات السحابية وحلول الحوسبة، مما يجعلها مختلفة بشكل جوهري عن الدورات العامة في الأمن السيبراني. بخلاف الدورات التي تتناول الأمن بشكل سطحي، تُسلط هذه الدورة الضوء على التحديات الأمنية الفريدة للبيئات السحابية، وتُقدم حلولًا تطبيقية ومتقدمة. يقدم BIG BEN Training Center هذه الدورة بمنهجية تدريبية تجمع بين المعرفة التقنية المتخصصة ودراسات الحالة الواقعية لسيناريوهات الاختراق، وتدريبات عملية مكثفة على أدوات ومنصات الأمن السحابي. سيتم تزويد المشاركين بالمهارات اللازمة لتقييم المخاطر الأمنية، وتصميم بنى تحتية سحابية آمنة، والاستجابة الفعالة للحوادث، مما يمكنك من حماية الأصول الرقمية لمؤسستك في السحابة. هذه الدورة هي الخيار الأمثل للمهنيين الذين يسعون للتميز في أمن الحوسبة السحابية.