الرقمية الدورة التدريبية: تأمين الاتصالات السحابية وحلول الحوسبة لبيئات العمل

اغسطس ٢٠٢٦ ٠٧ - ٠٣

جينف

(للشخص الواحد) ٦٢٠٠ €

Ref: #TEL8863_415426

مقدمة الدورة التدريبية / لمحة عامة:

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

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:

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

- 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:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الأمنية. الوحدة الأولى: أساسيات الحوسبة السحابية ومخاطرها

- 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.

السحابة. الوحدة الثانية: تأمين الهوية والوصول والبيانات في

- 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).

السحابية. الوحدة الرابعة: أمن التطبيقات والحاويات والخدمات

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

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

- 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:

التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة.

الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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