الدورة التدريبية: تأمين بيئات العمل عن بعد والعمل الهجين للشركات



19 - 23 اكتوبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #CYB8633_421613

مقدمة الدورة التدريبية / لمحة عامة:

أحدثت بيئات العمل عن بعد والعمل الهجين تحولًا جذريًا في طريقة عمل الشركات، مقدمة مرونة أكبر وزيادة في الإنتاجية. ومع ذلك، فإن هذا التغيير قد أزال الحدود التقليدية لأمن الشبكات، مما خلق ثغرات أمنية جديدة وزاد من المخاطر السيبرانية. إن حماية البيانات والأنظمة في بيئة موزعة أصبح تحديًا معقدًا يتطلب استراتيجيات أمنية مُحكمة. إن أي هجوم سيبراني يستهدف موظفًا يعمل عن بُعد يمكن أن يكون نقطة دخول إلى شبكة المؤسسة بأكملها. تقدم هذه الدورة التدريبية المتخصصة لمديري تكنولوجيا المعلومات، متخصصي الأمن، ومديري الموارد البشرية، المعرفة والمهارات اللازمة لتأمين بيئات العمل الهجين. سنتناول في هذه الدورة مفاهيم الأمن السيبراني المخصصة للعمل عن بعد، التهديدات الشائعة، واستراتيجيات الحماية. سيكتسب المشاركون القدرة على تحديد نقاط الضعف، تطبيق ضوابط أمنية قوية، ووضع سياسات متكاملة لضمان أمان البيانات والأنظمة. تهدف الدورة إلى بناء كوادر متخصصة في أمن العمل عن بعد، مما يضمن أن المؤسسات تكون دائمًا في طليعة الدفاع. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور ديفيد إس. فيربر (David S. Ferber)، المعروف بأعماله في أمن الشبكات المنزلية. يقدم BIG BEN Training Center هذه الدورة لتمكين قادة الأعمال من بناء بيئة عمل آمنة ومرنة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو تقنية المعلومات.
- متخصصو الأمن السيبراني.
- مديرو الموارد البشرية.
- مديرو الأقسام وفرق العمل.
- المحللون الأمنيون.
- القيادات التقنية.

القطاعات والصناعات المستهدفة:

- شركات التكنولوجيا.
- الجهات الحكومية وما في حكمها.
- القطاع المالي والمصرفي.
- الرعاية الصحية.
- الشركات التي تعتمد على العمل الهجين.

الأقسام المؤسسية المستهدفة:

- إدارة تكنولوجيا المعلومات.
- إدارة الأمن السيبراني.
- إدارة الموارد البشرية.
- إدارة العمليات التشغيلية.
- إدارة المخاطر.

أهداف الدورة التدريبية:

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

- فهم المخاطر الأمنية المرتبطة ببيئات العمل الهجين.
- القدرة على تأمين الأجهزة الشخصية وشبكات Wi-Fi المنزلية.
- حماية البيانات الحساسة عند الوصول إليها عن بعد.
- تطبيق سياسات التحكم في الوصول والمصادقة المتعددة العوامل.
- وضع خطط للاستجابة للحوادث في بيئات العمل الموزعة.
- تدريب الموظفين على أفضل ممارسات الأمن السيبراني.
- الامتثال للوائح الأمنية الدولية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وتفاعلية، مصممة لتمكين المشاركين من فهم وتطبيق إجراءات الأمن السيبراني في بيئات العمل الهجين. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لاختراقات أمنية ناتجة عن العمل عن بعد، وورش العمل التطبيقية، من ممارسة تأمين الأجهزة وتحليل المخاطر. تتضمن المنهجية مناقشات متعمقة حول الفرق بين أمن المكتب وأمن المنزل، وأفضل الممارسات لتأمين الوصول عن بعد. سيتم التركيز على الجانب الاستباقي للأمن، وتشجيع المشاركين على التفكير في كيفية حماية أصولهم من التهديدات. يقدم BIG BEN Training Center هذه الدورة لتعزيز الوعي الأمني والخبرة لدى العاملين في بيئة العمل الهجين.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: فهم المخاطر الأمنية للعمل الهجين

- مقدمة إلى بيئات العمل عن بعد والهجين.
- المخاطر الأمنية الجديدة.
- التهديدات التي تستهدف الموظفين عن بعد (Phishing).
- أهمية حماية البيانات خارج المكتب.
- الفرق بين أمن المكتب والمنزل.
- مسؤولية الموظف والمؤسسة.
- بناء ثقافة أمنية قوية.

الوحدة الثانية: تأمين الأجهزة والشبكات

- تأمين الأجهزة الشخصية (Laptops, Mobile Devices).
- أفضل الممارسات لتأمين شبكات Wi-Fi المنزلية.
- استخدام الشبكات الخاصة الافتراضية (VPN).
- المصادقة المتعددة العوامل (MFA).
- إدارة الثغرات الأمنية للأجهزة.
- تشفير البيانات على الأجهزة.
- التحكم في الوصول إلى الأنظمة.

الوحدة الثالثة: حماية البيانات والتطبيقات

- أمن الحوسبة السحابية في بيئات العمل الهجين.
- تأمين التطبيقات والبرامج المستخدمة.
- حماية البيانات الحساسة من التسرب.
- سياسات النسخ الاحتياطي والتعافي.
- إدارة الهوية والوصول.
- أمن البريد الإلكتروني.
- أمن الاجتماعات الافتراضية.

الوحدة الرابعة: حوكمة الأمن والامتثال

- وضع سياسات أمنية للعمل الهجين.
- التدريب على الوعي الأمني للموظفين.
- الامتثال للوائح الأمنية (GDPR).
- إدارة المخاطر الأمنية في بيئة العمل الموزعة.
- الاستجابة للحوادث الأمنية عن بعد.
- التواصل الفعال خلال الأزمات.
- قياس أداء برنامج الأمن.

الوحدة الخامسة: مستقبل الأمن في العمل الهجين

- استراتيجيات الأمن الاستباقي (Zero Trust).
- أمن الأتمتة والذكاء الاصطناعي.
- تطور التهديدات في بيئات العمل الجديدة.
- المرونة السيبرانية واستمرارية الأعمال.
- أمن البيانات في بيئة العمل المستقبلية.
- التكامل بين الأمن والأعمال.
- التطور المستقبلي للعمل الهجين.

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 المستمر للعمل الهجين، كيف يمكن للمؤسسات أن تبتكر إطار عمل أمني لا يقتصر على حماية الأجهزة فحسب، بل يُنشئ نظامًا بيئيًا آمنًا للبيانات، ويضمن سلامة التعاون بين الموظفين، ويُمكّن المؤسسة من الاستجابة بفعالية للأزمات مع الحفاظ على المرونة والإنتاجية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص على تأمين بيئات العمل عن بعد والهجين، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية الفريدة في هذا المجال. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لتأمين الأجهزة الشخصية، وحماية البيانات عن بعد، ووضع استراتيجيات متكاملة لضمان أمان الموظفين. تقدم الدورة دراسات حالة واقعية لاختراقات أمنية ناتجة عن بيئات العمل الهجين، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الترابط بين الجوانب الأمنية والإدارية والاستراتيجيات الاستباقية للأمن، مما يضمن أن المشاركين سيخرجون بخبرة عملية قابلة للتطبيق. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في الأمن السيبراني قادرين على حماية مستقبل العمل.