# للشركات الدورة التدريبية: تأمين بيئات العمل عن بعد والعمل الهجين

يوليو ٢٠٢٦ ٣٠ - ٢٦

المنامة

٤٧٠٠ € (للشخص الواحد)

Ref: #CYB8633_60656

## مقدمة الدورة التدريبية / لمحة عامة:

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

## لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

## منهجية الدورة التدريبية:

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

## 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:

يُنشئ نظامًا بيئيًا آمنًا للمؤسسات أن تبتكر إطار عمل أمني لا يقتصر على في ظل التوسع المستمر للعمل الهجين، كيف يمكن

ويُمكّن المؤسسة من الاستجابة بفعالية للأزمات مع للبيانات، ويضمن سلامة التعاون بين الموظفين، حماية الأجهزة فحسب، بل

الحفاظ على المرونة والإنتاجية؟

## ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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