الدورة التدريبية: بناء خطط أمن سيبراني استراتيجية متكاملة لحماية المؤسسات من التهديدات الحديثة

#PLA8402

الدورة التدريبية: بناء خطط أمن سيبراني استراتيجية متكاملة لحماية المؤسسات من التهديدات الحديثة

مقدمة الدورة التدريبية / لمحة عامة:

تقدم هذه الدورة إطارًا متكاملًا لتصميم خطط أمن سيبراني استباقية تحمي أصول المؤسسات الرقمية الحيوية. في ظل تطور التهديدات الإلكترونية مثل برامج الفدية والهجمات الموجهة، يصبح التخطيط الاستراتيجي ضرورة حتمية لضمان استمرارية الأعمال. خلال 25 ساعة تدريبية، ستستكشف منهجيات عالمية كإطار NIST ونماذج حوكمةISO 27001 ، مع دراسة حالات واقعية لانتهاكات البيانات. يدمج المحتوى رؤى الخبير بروس شناير Bruce Schneier في تحليل التهديدات المعقدة. يقدمBIG BEN Training Centerهذه الدورة عبر جلسات تفاعلية تمزج بين المحاكاة والتخطيط العملي، مما يمكن المشاركين من تطوير استراتيجيات قابلة للتنفيذ فورًا.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو أمن المعلوماتCISOs .
- مسؤولو إدارة المخاطر المؤسسية.
- قادة فرق الاستجابة للحوادث السيبرانية.
- مدراء تكنولوجيا المعلومات في القطاع العام والخاص.
- مسؤولو التوافق التنظيمي.
- استشاريو الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- الرعاية الصحية والمستشفيات.
- شركات الطاقة والبنية التحتية الحيوية.
- الهيئات الحكومية والوزارات.
- مقدمي الخدمات السحابية.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- قسم الجودة والتوافق.
- فرق الاستمرارية التشغيلية.
- الإدارة التنفيذية العليا.
- إدارة التخطيط الاستراتيجي.

أهداف الدورة التدريبية:

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

- تحليل نضج الأمن السيبراني الحالي باستخدام نموذجCMMC .
- تحديد الأصول الرقمية الحرجة وتقييم تعرضها للتهديدات.
- صياغة سياسات أمنية متوافقة مع PCI DSS وISO 27001.
- تصميم خطة استجابة فعالة لحوادث الأمن السيبراني.
- قياس العائد الاستثماري لاستراتيجيات الأمن السيبراني.

منهجية الدورة التدريبية:

تعتمد الدورة على منهجية قائمة على التطبيق العملي، حيث يشارك المتدربون في ورش عمل لتحليل ثغرات أمنية حقيقية وتصميم خطط حماية متعددة الطبقات. تشمل الجلسات محاكاة هجمات إلكترونية لتطوير مهارات الاستجابة السريعة، مع مناقشات جماعية لتقييم حلول إدارة المخاطر في قطاعات مختلفة. يقدم المدربون تغذية راجعة فورية على نماذج التخطيط المقدمة من المشاركين، مدعومة بدراسات حالة من قطاعات الصحة والمالية. يستخدم BIG BEN Training Center تقنيات تفاعلية كالتصويت المباشر لحل المعضلات الأمنية، مما يعزز اكتساب المهارات القابلة للتطبيق في بيئات العمل.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات التخطيط الاستراتيجي للأمن السيبراني

- مفاهيم الأصول الرقمية وتصنيفها حسب الأهمية.
- تحليل بيئة التهديدات السيبرانية الحديثة.
- الإطار القانوني والتنظيمي المحلي والدولي.
- معايير التوافق الإلزامية في القطاعات الحيوية.
- أدوات تقييم نضج الأمن السيبراني.
- دراسة حالة: انهيار البنية التحتية بسبب هجوم إلكتروني.

الوحدة الثانية: منهجيات تصميم استراتيجيات الحماية

- تطبيق إطار NIST CSF في التخطيط.
- دمج متطلبات ISO 27001 مع أهداف الأعمال.
- خرائط التهديدات السيبرانيةThreat Intelligence .
- تحديد مؤشرات الأداء الرئيسية KPIs للأمن.
- نمذجة مخاطر الهجمات على سلاسل التوريد.
- ورشة عمل: تطوير إطار حوكمة لأمن المعلومات.

الوحدة الثالثة: إدارة المخاطر والاستجابة للحوادث

- آليات كشف الثغرات الأمنية الاستباقية.
- تصنيف الحوادث حسب خطورتها.
- تصميم خطط استمرارية الأعمالBCP .
- نموذج محاكاة إدارة أزمة اختراق البيانات.
- تنسيق فرق الاستجابة مع الإدارات الداعمة.
- تحليل أدوات احتواء الهجمات الإلكترونية.

الوحدة الرابعة: التوافق التنظيمي وقياس الفعالية

- متطلبات PCI DSS للجهات المالية.
- معايير HIPAA في قطاع الرعاية الصحية.
- إجراءات التدقيق الداخلي للتخطيط الأمني.
- تقييم العائد الاستثماري لتدابير الحماية.
- تقارير الأداء لمجالس الإدارة.
- دراسة حالة: غرامات عدم التوافق التنظيمي.

الوحدة الخامسة: التكامل والتحسين المستمر

- دمج الأمن السيبراني في التحول الرقمي.
- آليات تحديث الخطط وفق تطور التهديدات.
- التدريب المستمر للكوادر على المهارات الجديدة.
- توثيق الدروس المستفادة من الحوادث.

- نموذج التخطيط النهائي الشامل.
- عرض مشاريع المشاركين وتقييمها.

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:

كيف يمكن موازنة تكلفة تطبيق معايير الأمن السيبراني الصارمة مع محدودية ميزانيات المؤسسات الناشئة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تركز هذه الدورة على الجانب الاستراتيجي التشغيلي بدلاً من الأدوات التقنية، من خلال تمكين المشاركين من تحويل المفاهيم النظرية إلى خطط عمل قابلة للقياس. باستخدام منهجية "التعلم بالمشكلات"، يحلل المتدربون ثغرات أمنية حقيقية في قطاعاتهم ويصممون حلولاً مخصصة أثناء الجلسات، بدعم من خبراء .BIG BEN Training Center تم تطوير المحتوى بناءً على تحديات تواجهها المؤسسات في البيئة العربية، مثل متطلبات التوافق مع الأنظمة المحلية وأزمات نقص الكوادر المؤهلة. كما تتضمن الدورة أحدث التحديثات في معايير NIST الخاصة بإدارة مخاطر سلسلة التوريد، مما يوفر رؤية استباقية غير متوفرة في البرامج التقليدية.