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

يونيو ٢٠٢٦ ٢٦ - ٢٢

شرم الشيخ

(للشخص الواحد) € ٤١٠٠

Ref: #PLA8402_540069

مقدمة الدورة التدريبية / لمحة عامة:

الإلكترونية مثل سيبراني استباقية تحمي أصول المؤسسات الرقمية تقدم هذه الدورة إطارًا متكاملا لتصميم خطط أمن ضرورة حتمية لضمان استمرارية الأعمال. برامج الفدية والهجمات الموجهة، يصبح التخطيط الحيوية. في ظل تطور التهديدات المحتوى كإطار NIST ونماذج حوكمة ISO ٢٧٠٠١، مع دراسة خلال ٢٥ ساعة تدريبية، ستستكشف منهجيات عالمية الاستراتيجي يقدم BIG BEN Training Center رؤى الخبير بروس شناير Bruce Schneier في تحليل حالات واقعية لانتهاكات البيانات. يدمج والتخطيط العملي، مما يمكن المشاركين من تطوير هذه الدورة عبر جلسات تفاعلية تمزج بين المحاكاة التهديدات المعقدة. استراتيجيات قابلة للتنفيذ فورًا.

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو أمن المعلومات.CISOs
- 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:

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

- CMMC. تحليل نضج الأمن السيبراني الحالي باستخدام نموذج
- للتهديدات. تحديد الأصول الرقمية الحرجة وتقييم تعرضها
- ٢٧٠٠١. صياغة سياسات أمنية متوافقة مع PCI DSS وISO
- تصميم خطة استجابة فعالة لحوادث الأمن السيبراني.
- السيبراني. قياس العائد الاستثماري لاستراتيجيات الأمن

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

السيبراني الوحدة الأولى: أساسيات التخطيط الاستراتيجي للأمن

- 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.
- إلكتروني. دراسة حالة: انهيار البنية التحتية بسبب هجوم

الوحدة الثانية: منهجيات تصميم استراتيجيات الحماية.

- تطبيق إطار NIST CSF في التخطيط.
- دمج متطلبات ISO ٢٧٠٠١ مع أهداف الأعمال.
- خرائط التهديدات السيبرانية Threat 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 الأعمال BCP.
- 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:

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 ٢٠-٢٥ 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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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