التدريبية: إدارة مخاطر الأمن السيبراني:

التقييم، التحليل، والمعالجة الشاملة الدورة

يونيو ٢٠٢٦ ٠٥ - ٠١

أمستردام - *

(للشخص الواحد) € ٥٧٠٠

Ref: #SM5748_325971

مقدمة الدورة التدريبية / لمحة عامة:

للمؤسسات التي تسعى مخاطر الأمن السيبراني: التقييم، التحليل، في ظل المشهد الرقمي المتغير باستمرار، أصبحت إدارة المتعمقة مصممة لتزويد المشاركين لحماية أصولها وبياناتها الحساسة. هذه الدورة والمعالجة الشاملة ضرورة حتمية المنهجيات والأطر تحليل، ومعالجة المخاطر السيبرانية بشكل استباقي بالمعرفة والمهارات المتقدمة لتحديد، تقييم، التدريبية السيبرانية يتوافق مع أهداف الأعمال العالمية، سيتعلم المتدربون كيفية بناء برنامج شامل وفعال. من خلال التركيز على أحدث Carl ، الذي أعمال خبراء رواد في مجال إدارة المخاطر، مثل ويقلل من التعرض للتهديدات. تستند الدورة إلى لإدارة المخاطر الدورة BIG BEN Training Center يقدم رؤى قيمة حول التخطيط للمخاطر وإدارتها. يقدم الدكتور Carl Pritchard Pritchard للمؤسسة. المخاطر، وتنفيذ ضوابط أمنية فعالة، واتخاذ قرارات المهنيين من تطوير استراتيجيات قوية لإدارة بهدف تمكين هذه المشاركين على تطبيق المفاهيم سنركز على الجوانب العملية، مع تقديم أمثلة واقعية مستنيرة لحماية البنية التحتية الرقمية السيبراني. النظرية في بيئات عملهم لتعزيز مرونة الأمن ودراسات حالة تساعد

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو المخاطر الأمنية.
- محللو الأمن السيبراني.
- مديرو أمن المعلومات.
- مسؤولو الامتثال.
- مدققو أمن المعلومات.
- مهندسو الأمن.
- القادة وصناع القرار في تقنية المعلومات.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الرعاية الصحية.
- الحكومة والدفاع.
- قطاع الطاقة والمرافق.
- شركات الاتصالات.
- الشركات التكنولوجية.
- الاستشارات الأمنية.
- الشركات الصناعية الكبرى.

الأقسام المؤسسية المستهدفة:

- إدارة المخاطر.
- إدارة أمن المعلومات.
- إدارة تقنية المعلومات.
- قسم التدقيق الداخلي.
- قسم الامتثال.
- الإدارة العليا.
- إدارة العمليات.

أهداف الدورة التدريبية:

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

- تحديد المخاطر السيبرانية المحتملة وتقييمها بدقة.
- تحليل تأثير المخاطر على العمليات التجارية والأصول.
- تطوير استراتيجيات فعالة لمعالجة المخاطر (القبول، التجنب، التخفيف، النقل).
- تنفيذ ضوابط أمنية لتقليل التعرض للمخاطر.
- مراقبة وتقييم المخاطر بشكل مستمر.
- بناء إطار عمل شامل لإدارة المخاطر السيبرانية.
- التعامل مع المخاطر الناشئة والتهديدات المتطورة.
- إعداد تقارير المخاطر وتقديم التوصيات للإدارة.

منهجية الدورة التدريبية:

الأمن السيبراني: تهدف إلى تزويد المشاركين بفهم عميق ومهارات تتبنى هذه الدورة التدريبية منهجية تفاعلية وعملية متعمقة يقدمها خبراء متخصصون في إدارة التقييم، التحليل، والمعالجة الشاملة. تبدأ الدورة تطبيقية في مجال إدارة مخاطر المشاركون لتبادل الأفكار والتحديات. يتم التركيز بشكل مكثف المخاطر السيبرانية، تليها مناقشات جماعية بناءة بمحاضرات واقتراح استراتيجيات معالجة. بتحليل سيناريوهات مخاطر سيبرانية معقدة، وتحديد على دراسات الحالة الواقعية، حيث يقوم BIG استخدام أدوات تقييم المخاطر، وإعداد مصفوفات تتضمن المنهجية ورش عمل تطبيقية تتيح للمتدربين العوامل المؤثرة، حل المشكلات. يتم المشاركة النشطة والعمل الجماعي Training Center المخاطر، وتطوير خطط تخفيف المخاطر. يشجعBEN تهدف هذه المنهجية إلى تمكين تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى لتعزيز التفكير النقدي وقدرات وكفاءة. بالمعرفة والأدوات اللازمة لإدارة المخاطر المشاركين من العودة إلى مؤسساتهم وهم مجهزون استفادة من الدورة. السيبرانية بفعالية

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

السيبراني الوحدة الأولى: مفاهيم وأسس إدارة مخاطر الأمن

- الاستراتيجي. مقدمة إلى إدارة المخاطر السيبرانية ودورها
- أهمية تقييم المخاطر في تحديد الأولويات الأمنية.
- مفاهيم التهديد، الثغرة، والأثر.
- نماذج إدارة المخاطر (مثل NIST CSF، ISO ٢٧٠٠٥).
- مكونات إطار عمل إدارة المخاطر الشامل.
- التحديات الشائعة في إدارة المخاطر السيبرانية.
- دمج إدارة المخاطر مع أهداف الأعمال.

الوحدة الثانية: تحديد وتقييم المخاطر السيبرانية

- تحديد الأصول الهامة وتقدير قيمتها.
- تحديد التهديدات ونقاط الضعف المحتملة.
- منهجيات تقييم المخاطر (الكمية والنوعية).
- أدوات وتقنيات جمع البيانات للمخاطر.
- تحليل احتمالية وقوع الحوادث.
- تقدير الأثر المالي والتشغيلي والأخلاقي للمخاطر.
- تصنيف المخاطر وتحديد مستوياتها.

المعالجة الوحدة الثالثة: تحليل المخاطر وتطوير استراتيجيات

- تحليل المخاطر بناءً على الاحتمالية والأثر.
- تقنيات تحليل الثغرات الأمنية واختبار الاختراق.
- النقل). خيارات معالجة المخاطر (القبول، التجنب، التخفيف،
- تصميم وتنفيذ الضوابط الأمنية لتقليل المخاطر.
- تطوير خطط الاستجابة للحوادث كجزء من المعالجة.
- تحليل التكلفة والفائدة للضوابط الأمنية.
- بناء خطة شاملة لمعالجة المخاطر.

الوحدة الرابعة: مراقبة المخاطر وإعداد التقارير

- المراقبة المستمرة للمخاطر وتحديد المخاطر الناشئة.
- الرئيسية (KRIs). مؤشرات الأداء الرئيسية (KPIs) ومؤشرات المخاطر
- المصلحة. إعداد تقارير المخاطر للإدارة العليا وأصحاب
- التواصل الفعال حول حالة المخاطر.
- مراجعة وتقييم فعالية خطط معالجة المخاطر.
- إدارة سجلات المخاطر وتحديثها.
- أهمية التغذية الراجعة في دورة إدارة المخاطر.

الوحدة الخامسة: إدارة المخاطر المتقدمة والامتثال

- إدارة مخاطر سلسلة التوريد والأطراف الثالثة.
- إدارة مخاطر الامتثال للوائح (مثل GDPR، CCPA).
- أتمتة إدارة المخاطر (GRC tools).
- التعامل مع المخاطر البشرية والأمن السلوكي.
- الأشياء، الحوسبة السحابية). مخاطر التقنيات الناشئة (الذكاء الاصطناعي، إنترنت
- دراسات حالة متقدمة في إدارة المخاطر السيبرانية.
- التخطيط للمستقبل في مواجهة التهديدات المتغيرة.

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:

الآمن في السيبرانية ليست مجرد وظيفة متفاعلة مع التهديدات، كيف يمكن للمؤسسات أن تضمن أن عملية إدارة المخاطر

البيئة الرقمية؟ بل هي محرك استباقي للابتكار والنمو

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

مما يميزها عن الدورات التي إدارة مخاطر الأمن السيبراني: التقييم، التحليل، تتميز هذه الدورة بتركيزها الشامل والعميق على في المنهجيات والأدوات التي تمكن المشاركين تقدم نظرة سطحية. نحن لا نكتفي بتقديم المفاهيم، بل والمعالجة الشاملة، تعتمد الدورة على نهج عملي مكثف، يتضمن دراسات حالة من تطبيق إدارة المخاطر بفعالية في مؤسساتهم. نتعمق المتقدم، المقدم بممارسة تقييم المخاطر، وتحليلها، وصياغة خطط واقعية وورش عمل تفاعلية، مما يسمح للمتدربين التحديات والحلول في هذا المجال من BIG BEN Training Center، أن يكون المشاركون معالجتها. يضمن المحتوى الأكاديمي على المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا الحيوي. هذه الدورة لا تهدف فقط إلى تزويد على دراية بأحدث مرونة الأمن. حماية أصول مؤسساتهم واتخاذ قرارات مستنيرة لتعزيز خبراء في إدارة المخاطر السيبرانية، قادرين