البروشور التعريفي للدورة

إدارة المخاطر السيبرانية

دورة متقدمة في تحديد المخاطر السيبرانية وتقديرها كمياً بصورة مبسطة، وبناء سجل مخاطرها، وإدارة مخاطر الأطراف الثالثة، ورفع التقارير إلى مجلس الإدارة.

الكود	HT-IT-109
التصنيف	تقنية المعلومات والأمن السيبراني
المدة	أسبوع واحد
المستوى	متقدم
المدينة	أمستردام

مقدمة

عبارة مثل "خطر اختراق مرتفع" لا تساعد مجلس الإدارة على المفاضلة بين استثمارين؛ فالقرار يحتاج إلى سيناريوهات واضحة وتقديرات للخسارة المحتملة ضمن نطاقات، مهما كانت تقريبية.

الأهداف

- صياغة سيناريوهات مخاطر سيبرانية ترتبط بأصول وعمليات محددة
- بناء سجل مخاطر سيبرانية يربط كل خطر بالضوابط والمالك والخطر المتبقي
- تقدير تكرار الأحداث وحجم الخسائر ضمن نطاقات بطريقة كمية مبسطة
- تقييم المخاطر السيبرانية للموردين والأطراف الثالثة ومتابعتها
- عرض المخاطر السيبرانية على مجلس الإدارة بلغة مالية واضحة

لمن هذه الدورة

- مديرو المخاطر السيبرانية وأمن المعلومات
- مديرو المخاطر المؤسسية المسؤولون عن ملف المخاطر التقنية
- مسؤولو إدارة مخاطر الموردين والتعاقدات التقنية
- مستشارو المخاطر ومعدو تقارير المخاطر للجان المجلس

المهارات التي ستكتسبها

- صياغة سيناريوهات المخاطر السيبرانية
- التقدير الكمي للمخاطر
- تقييم مخاطر الأطراف الثالثة
- إعداد تقارير المخاطر للمجلس

مخرجات التعلم

- إعداد سجل مخاطر سيبرانية لعشرة سيناريوهات مع الضوابط والمالكين والخطر المتبقي
- تقدير الخسارة السنوية المحتملة لسيناريو واحد ضمن نطاق وعرض منحنى تجاوز الخسارة
- تصميم نموذج لتصنيف الموردين حسب مستوى المخاطر السيبرانية ومتطلبات تقييم كل فئة
- إعداد تقرير من صفحتين لمجلس الإدارة عن أبرز المخاطر السيبرانية وخيارات معالجتها

محاور الدورة

اليوم الأول: المخاطر السيبرانية في سياق المؤسسة

- ربط المخاطر السيبرانية بإطار المخاطر المؤسسية وقابلية المخاطر المعتمدة
- العلاقة بين الأصل والتهديد والثغرة والأثر

- تحديد المخاطر بالسيناريوهات انطلاقاً من العمليات الحرجة

اليوم الثاني: سجل المخاطر السيبرانية

- كتابة بيان خطر واضح يتضمن السبب والحدث والأثر
- الخطر الكامن والمتبقي وربط الضوابط بفئات NIST CSF 2.0
- الملكية وقرارات قبول المخاطر وتحديث السجل

اليوم الثالث: أسس التقدير الكمي

- حدود المصفوفات النوعية ومتى يفيد التقدير الكمي
- تقدير تكرار الحدث وحجم الخسارة بنطاقات وتقديرات الخبراء المعايرة
- محاكاة مونت كارلو المبسطة ومنحنى تجاوز الخسارة

اليوم الرابع: مخاطر الأطراف الثالثة

- تصنيف الموردين حسب الوصول إلى البيانات والأنظمة وأهمية الخدمة
- استبيانات العناية الواجبة والأدلة المطلوبة والبنود التعاقدية الأمنية
- المتابعة المستمرة ومخاطر التركز لدى مزودي الخدمات السحابية

اليوم الخامس: المعالجة والتقارير إلى المجلس

- خيارات المعالجة ومقارنة كلفة الضوابط بالخسارة المتوقعة واعتبارات التأمين السيبراني
- مؤشرات المخاطر الرئيسية وتصميم تقرير المجلس
- مشروع تطبيقي: تقرير لمجلس الإدارة عن أبرز السيناريوهات السيبرانية لمؤسسة المشارك مقدرة ضمن نطاقات مع توصيات المعالجة

منهجية التدريب

ورشة لصياغة سيناريوهات مخاطر انطلاقاً من عمليات المشاركين الحرجة
تمارين معايرة التقدير يختبر فيها المشاركون دقة نطاقاتهم
تشغيل نموذج Excel معد مسبقاً لمحاكاة مونت كارلو على سيناريو محدد
عرض تقرير المخاطر أمام لجنة مخاطر محاكاة تطرح أسئلة المجلس

الشهادة

يحصل المشارك على شهادة حضور من Harbor Training Center عند إتمام الدورة.

المواعيد القادمة

المدينة	الموعد	اللغة	الرسوم
أمستردام	8 – 12 فبراير 2027	EN	EUR 6,100
أمستردام	9 – 13 أغسطس 2027	AR	EUR 6,100

الرسوم للمشارك الواحد.

تواصل معنا

البريد info@harbor4training.com

للتسجيل والتفاصيل، امسح الرمز أو زر الرابط:

https://harbor4training.com/ar/courses/cyber-risk-management