

الدورة المتقدمة في الأمن السيبراني وإدارة المخاطر
السيبرانية

UK Traininig

PARTNER



الدورة المتقدمة في الأمن السيبراني وإدارة المخاطر السيبرانية

المقدمة

في ظل التحولات الرقمية المتسارعة والتطورات التقنية الكبيرة، أصبحت التهديدات السيبرانية تمثل تحديًا حقيقيًا تواجهه المؤسسات بمختلف أحجامها وقطاعاتها. لم يعد الأمن السيبراني خيارًا تقنيًا فقط، بل أصبح جزءًا أساسيًا من استراتيجيات المؤسسات لحماية المعلومات والبيانات الحساسة وضمان استمرارية الأعمال. تهدف هذه الدورة التدريبية الشاملة إلى تزويد المشاركين بالمعرفة والمهارات الأساسية والمتقدمة في مجال الدفاع السيبراني، مع التركيز على منهجيات إدارة المخاطر وتحليل التهديدات الحديثة. تجمع الدورة بين الجوانب النظرية والتطبيقية من خلال محاكاة سيناريوهات واقعية وتطبيقات عملية، مما يمكن المشاركين من تطوير قدراتهم بشكل فعال وبناء بيئة عمل أكثر أمانًا واستقرارًا.

أهداف الدورة

- بنهاية هذه الدورة، سيكون المشاركون قادرين على:
- بناء وقيادة استراتيجية متكاملة للأمن السيبراني داخل المؤسسة.
- تقييم المخاطر السيبرانية وتحديد أولويات المعالجة.
- تطبيق ضوابط أمان فعالة بناءً على أفضل الممارسات العالمية.
- اكتساب مهارات عملية من خلال سيناريوهات حقيقية ومحاكاة.

محتوى الدورة

اليوم الأول: مقدمة في الأمن السيبراني والمخاطر

- مقدمة في الأمن السيبراني وأهميته في البيئة الحديثة.
- العلاقة بين الأمن السيبراني وإدارة المخاطر المؤسسية.
- نظرة عامة على التهديدات السيبرانية الحديثة.
- مقدمة حول دورة حياة إدارة المخاطر السيبرانية.

UK Training

PARTNER



اليوم الثاني: تصنيف وتحليل التهديدات السيبرانية

- أنواع التهديدات والهجمات السيبرانية.
- تحليل التهديدات الداخلية والخارجية.
- دراسات حالة لهجمات كبرى على منظمات عالمية.
- تحليل الأثر.

اليوم الثالث: تقييم الثغرات وتقدير المخاطر

- تقنيات كشف الثغرات.
- تحديد الأصول الحرجة داخل المؤسسة.
- أدوات تحليل المخاطر مصفوفة المخاطر — الاحتمالية مقابل الأثر.
- دراسة عملية: تقييم مخاطر مشروع تقني.

اليوم الرابع: بناء السياسات والإجراءات الأمنية

- كيفية تطوير سياسات أمن معلومات فعالة.
- دور السياسات في الحد من المخاطر.
- إعداد الإجراءات التشغيلية القياسية.
- ربط السياسات الأمنية باستراتيجية إدارة المخاطر.

اليوم الخامس: أمن الشبكات والبنية التحتية

- مبادئ تصميم الشبكات الآمنة.
- إدارة والتحكم في الوصول إلى الشبكات.
- تقسيم الشبكات وتطبيق الجدران النارية.
- دمج أنظمة كشف ومنع التسلل.

UK Training

PARTNER



اليوم السادس: أمن البيانات، التشفير، وإدارة الوصول

- حماية البيانات أثناء النقل والتخزين.
- تقنيات وأساليب التشفير وأنواعه.
- إدارة الوصول وتحديد الصلاحيات.
- المصادقة متعددة العوامل وإدارة الهوية.

اليوم السابع: إدارة الحوادث السيبرانية والاستجابة لها

- منهجية التعامل مع الحوادث السيبرانية.
- خطوات التحقيق والتحليل.
- تسجيل الحوادث والإبلاغ عنها.
- إعداد خطة الاستجابة للحوادث.

اليوم الثامن: استمرارية الأعمال والتعافي من الكوارث

- تطوير خطة استمرارية الأعمال.
- إعداد خطة التعافي من الكوارث.
- دمج الأمن السيبراني في خطط الطوارئ.
- تمرين محاكاة عملي للاستجابة للأزمات.

اليوم التاسع: إدارة المخاطر السيبرانية الاستراتيجية

- دمج إدارة المخاطر ضمن الحوكمة المؤسسية.
- المعايير والأطر مثل ISO 27005 و NIST RMF.
- دور القيادة العليا في دعم استراتيجية الأمن السيبراني.
- المراجعات الدورية للمخاطر وتحديث السياسات.

UK Training

PARTNER



اليوم العاشر: مراجعة شاملة وتطبيق عملي

- تطبيق عملي شامل مختبر محاكاة الأمن السيبراني.
- تحليل حالة حقيقية وبناء خطة أمن سيبراني متكاملة.
- تقديم مشاريع الفرق ومناقشة نتائج التقييم.
- الختام وتوزيع الشهادات.

لماذا تحضر هذه الدورة: الإيجابيات

- تركيز قوي على التطبيق العملي من خلال معامل المحاكاة ودراسات الحالة الواقعية.
- تطوير مهارات متقدمة في تحليل المخاطر وصياغة استراتيجيات وقائية.
- تمكين المشاركين من التعامل مع الحوادث السيبرانية والاستجابة بفعالية.
- إعداد المشاركين للامتحان للمعايير والسياسات العالمية في الأمن السيبراني.
- تعزيز قدرات القيادة والتخطيط الاستراتيجي داخل الفرق التقنية والمؤسسات.

الخاتمة

بنهاية هذه الدورة، يكون المشاركون قد اكتسبوا خبرة شاملة تؤهلهم للتعامل مع مختلف تحديات الأمن السيبراني بثقة وكفاءة. ستمكنهم المهارات المكتسبة من بناء استراتيجيات حماية فعالة وتطوير بيئة عمل أكثر أمانًا واستقرارًا داخل مؤسساتهم. كما تسهم هذه الدورة في رفع مستوى الوعي الأمني وتعزيز ثقافة الأمن السيبراني بين الأفراد والفرق التقنية، لتصبح المؤسسات أكثر استعدادًا لمواجهة التهديدات المستقبلية وحماية أصولها الرقمية.

UK Training

PARTNER

