Global Horizon
TRAINING CENTER

دورة:
إدارة المخاطر والتعامل مع التهديدات السيبرانية

22 - 26 نوفمبر 2026

القاهرة (مصر)

إدارة المخاطر والتعامل مع التهديدات السيبرانية

رمز الدورة: IT13153 تاريخ الإنعقاد: 22 - 26 نوفمبر 2026 دولة الإنعقاد: القاهرة (مصر) - رسوم الإشتراك: Euro

مقدمة

في ظل التطور السريع للتقنيات الرقمية واعتماد المؤسسات بشكل متزايد على الأنظمة الإلكترونية، أصبحت التهديدات السيبرانية من أبرز المخاطر التي تواجه المنظمات في مختلف القطاعات. تهدف هذه الدورة، التي صممتها Horizon Global Training Center، إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتحديد التهديدات السيبرانية وتقييم مخاطرها، ووضع خطط استجابة فعالة تضمن استمرارية الأعمال وحماية الأصول الرقمية.

أهداف البرنامج

- التعرف على مفهوم إدارة المخاطر السيبرانية وأهميته.
- تحليل أنواع التهديدات والهجمات السيبرانية الشائعة.
- تطبيق منهجيات تقييم وتحليل المخاطر.
- تطوير خطط استجابة للحوادث والتعافي من الأزمات.
- فهم الأطر والمعايير الدولية الخاصة بأمن المعلومات مثل NIST، ISO 27001.

الفئة المستهدفة

- مسؤولو أمن المعلومات وتقنية المعلومات.
- مدراء المخاطر والامتثال.
- مسؤولو الحوكمة الإلكترونية.
- المدراء التنفيذيون المهتمون بالأمن السيبراني.
- جميع العاملين في أقسام الحماية الرقمية والتحول الرقمي.

الأثر المؤسسي

- تعزيز قدرة المؤسسة على التنبؤ بالمخاطر السيبرانية والتعامل معها.

- تقوية منظومة أمن المعلومات بما يضمن استمرارية العمل.
- تحسين الالتزام بالمعايير والتشريعات الخاصة بحوكمة أمن المعلومات.
- تقليل الخسائر الناتجة عن الاختراقات أو الأعطال الأمنية.

المحاور التدريبية

اليوم الأول: أساسيات إدارة المخاطر السيبرانية

- مفهوم أمن المعلومات والمخاطر السيبرانية.
- الفرق بين التهديدات، الثغرات، المخاطر، والتأثير.
- الإطار العام لإدارة المخاطر السيبرانية.
- العوامل التنظيمية والتقنية المؤثرة على المخاطر.

اليوم الثاني: التهديدات السيبرانية وتحليل الهجمات

- أنواع الهجمات السيبرانية البرمجيات الخبيثة، التصيد، الحرمان من الخدمة، إلخ.
- تحليل طرق وأساليب المهاجمين Chain Kill Cyber.
- أدوات وتقنيات تحليل التهديدات.
- مؤشر الاختراق ومؤشر التهديدات.

اليوم الثالث: تقييم وتحليل المخاطر السيبرانية

- منهجيات تقييم المخاطر ISO 27005، NIST SP 800-30.
- تصنيف الأصول وتحديد أولويات الحماية.
- تحليل الأثر المحتمل والاحتمالية.
- سجل المخاطر وخطط المعالجة.

اليوم الرابع: استراتيجيات الحد من المخاطر والتعامل مع الحوادث

- آليات التخفيف من المخاطر والرقابة الفنية والإدارية.
- الاستجابة للحوادث السيبرانية وخطة الطوارئ.
- تشكيل فرق الاستجابة للحوادث CSIRT.
- التدريب على سيناريوهات هجومية.

اليوم الخامس: الامتثال والمعايير الدولية واستمرارية الأعمال

- الأطر المعيارية لأمن المعلومات ISO 27001، NIST، COBIT.
- العلاقة بين إدارة المخاطر وأمن المعلومات.
- خطة استمرارية الأعمال والتعافي من الكوارث DRP/BCP.
- تقييم الأداء وتطوير استراتيجية أمنية مستدامة.