Global Horizon
TRAINING CENTER

دورة:

أمن المعلومات

30 يونيو - 11 يوليو 2025

كوالالمبور (ماليزيا)

أمن المعلومات

رمز الدورة: IT12945 تاريخ الإنعقاد: 30 يونيو - 11 يوليو 2025 دولة الإنعقاد: كوالالمبور (ماليزيا) - رسوم الإشتراك: 9000 Euro

المقدمة:

أمن المعلومات يُعد من أهم المجالات التي تضمن حماية المعلومات الرقمية في العصر الحالي، حيث أصبح الحفاظ على سرية وسلامة وتوافر المعلومات أمرًا حيويًا للشركات والمؤسسات. تواجه المؤسسات تحديات متزايدة مع التهديدات السيبرانية والهجمات التي تستهدف البنية التحتية المعلوماتية. تهدف هذه الدورة إلى تمكين المشاركين من فهم شامل لأمن المعلومات وتزويدهم بالمهارات اللازمة لتطبيق تدابير الحماية الملائمة.

أهداف البرنامج:

- تقديم فهم شامل لمبادئ وأساسيات أمن المعلومات.
- تعزيز القدرة على تقييم وإدارة المخاطر الأمنية.
- تعليم المشاركين كيفية تطوير سياسات أمنية فعالة.
- تمكين المشاركين من اكتشاف ومعالجة التهديدات السيبرانية.
- استعراض الأدوات والتقنيات الحديثة المستخدمة في أمن المعلومات.

الكفاءات المكتسبة:

- فهم أساسيات وتقنيات أمن المعلومات.
- تطوير استراتيجيات وسياسات أمن المعلومات.
- القدرة على تقييم المخاطر الأمنية ومعالجتها.
- استخدام الأدوات الأمنية لحماية المعلومات.
- التمكن من التعامل مع الحوادث الأمنية والاستجابة لها.

الجمهور المستهدف:

- محترفو تكنولوجيا المعلومات.
- مدراء الأمن السيبراني.
- مدراء المشاريع التقنية.
- متخصصو الحوكمة والمخاطر والامتثال GRC.
- كل من يرغب في تعزيز معرفته بأمن المعلومات.

المحاور التدريبية:

اليوم الأول: مدخل إلى أمن المعلومات

- تعريف أمن المعلومات وأهميته.
- أبعاد أمن المعلومات السرية، السلامة، التوافر.
- تهديدات أمن المعلومات الحديثة والتحديات.
- حالات دراسية حول اختراقات أمن المعلومات.

اليوم الثاني: إدارة المخاطر الأمنية

- تعريف المخاطر الأمنية وأنواعها.
- كيفية تقييم المخاطر وإدارتها.
- استراتيجيات التخفيف من المخاطر.
- أمثلة على إدارة المخاطر في مؤسسات كبيرة.

اليوم الثالث: السياسات والإجراءات الأمنية

- تطوير سياسات أمن المعلومات.
- كيفية تطبيق الإجراءات الأمنية داخل المؤسسة.
- الأدوار والمسؤوليات في فريق الأمن.
- أفضل الممارسات لإنشاء بيئة عمل آمنة.

اليوم الرابع: الأمن السيبراني والاستجابة للحوادث

- مفهوم الأمن السيبراني وأهميته.
- تحليل الحوادث الأمنية وكيفية الاستجابة لها.
- خطط الطوارئ والاستمرارية.
- دراسات حالة حول الاستجابة للحوادث.

اليوم الخامس: تقنيات حماية البيانات

- التشفير وأنواعه.
- حماية البيانات أثناء النقل والتخزين.
- تقنيات التوثيق والمصادقة.

- إدارة الوصول وحماية البيانات الشخصية.

اليوم السادس: البرمجيات الخبيثة والتهديدات الداخلية

- أنواع البرمجيات الخبيثة فيروسات، ديدان، برامج الفدية.
- كيفية اكتشاف وإزالة البرمجيات الخبيثة.
- تهديدات الداخل: الأسباب وكيفية الوقاية.
- استراتيجيات لحماية الأنظمة من التهديدات الداخلية.

اليوم السابع: أمن الشبكات

- المبادئ الأساسية لأمن الشبكات.
- تقنيات الجدران النارية وأنظمة كشف التسلل IPS/IDS.
- تأمين الاتصالات والبيانات المتنقلة.
- دراسة حالات حول الهجمات الشبكية والحلول.

اليوم الثامن: الامتثال والمعايير الدولية لأمن المعلومات

- معايير ISO 27001 و27002.
- الامتثال التنظيمي لأمن المعلومات.
- سياسات الحوكمة والأطر القانونية.
- أمثلة على الامتثال لأمن المعلومات في المؤسسات.

اليوم التاسع: أمن الحوسبة السحابية

- التحديات الأمنية في بيئات الحوسبة السحابية.
- حماية البيانات في السحابة.
- إدارة الهويات والوصول في السحابة.
- استعراض حالات حول أمن الحوسبة السحابية.

اليوم العاشر: التوجهات المستقبلية في أمن المعلومات

- التهديدات المستقبلية وأمن المعلومات.
- الذكاء الاصطناعي وأثره على أمن المعلومات.
- الابتكارات في الحماية السيبرانية.

- استراتيجيات تعزيز أمن المعلومات في المستقبل.