مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

التقنيات المستقبلية لأمن المعلومات وحماية البيانات

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 20 – 24 / 7 / 2025.

مقدمة :

في ظل التطور السريع للتكنولوجيا وظهور تهديدات سيبرانية جديدة ومتقدمة، تتطلب حماية المعلومات والبيانات تبني تقنيات مستقبلية أكثر تقدمًا لتعزيز الأمان الإلكتروني. إن التصدي للهجمات السيبرانية المتطورة يتطلب مواكبة أحدث الابتكارات في مجال أمن المعلومات، مثل الذكاء الاصطناعي، التشفير المتقدم، وتكنولوجيا البلوك تشين. هذا البرنامج التدريبي "التقنيات المستقبلية لأمن المعلومات وحماية البيانات" يهدف إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتطبيق تقنيات حديثة ومتطورة لحماية الأنظمة والبيانات في بيئات العمل المعقدة والمترابطة.

أهداف الورشة:

- فهم التحديات الأمنية الناشئة في العصر الرقمي.
- التعرف على أحدث التقنيات المستقبلية في مجال أمن المعلومات وحماية البيانات (مثل الذكاء الاصطناعي، البلوك تشين، الحوسبة الكمومية).
- إتقان مهارات استخدام هذه التقنيات في الكشف عن التهديدات والاستجابة لها.
- تطوير استراتيجيات فعالة لحماية البيانات والمعلومات الحساسة.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين.
- التعامل مع حوادث الاختراق الأمني واستعادة البيانات.
- تطبيق المعرفة المكتسبة في تطوير حلول أمنية مبتكرة.

محتويات الورشة:

اليوم التدريبي الأول:

التحديات الأمنية في العصر الرقمي

- أنواع التهديدات السيبرانية الحديثة (مثل هجمات الفدية، التصيد الاحتيالي، هجمات سلسلة التوريد).
- التحديات التي تواجه أمن المعلومات في العصر الرقمي (مثل التطور السريع للتكنولوجيا، زيادة حجم البيانات، الهجمات المتطورة).
- أهمية تبني التقنيات المستقبلية في مواجهة هذه التحديات.
- ورشة عمل: تحليل حالة اختراق أمني وتحديد نقاط الضعف.

اليوم التدريبي الثاني:

الذكاء الاصطناعي في الأمن السيبراني

- تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات والاستجابة لها.
- تعلم الآلة في تحليل السلوك واكتشاف الأنماط الشاذة.
- استخدام معالجة اللغة الطبيعية في تحليل التهديدات وتصنيفها.
- ورشة عمل: تطبيق أدوات الذكاء الاصطناعي في تحليل سجلات الأحداث الأمنية.

اليوم التدريبي الثالث:

البلوك تشين وأمن البيانات

- مفهوم البلوك تشين ومزاياه في أمن البيانات (مثل اللامركزية، الشفافية، عدم القابلية للتغيير).
- تطبيقات البلوك تشين في حماية البيانات والتحقق من الهوية.
- التحديات والفرص المتعلقة باستخدام البلوك تشين في أمن المعلومات.
- ورشة عمل: تصميم تطبيق بسيط قائم على البلوك تشين لتأمين البيانات.

اليوم التدريبي الرابع:

الحوسبة الكمومية وأمن التشفير

- مفهوم الحوسبة الكمومية وتأثيرها المحتمل على التشفير التقليدي.
- تطوير خوارزميات تشفير مقاومة للحوسبة الكمومية.
- التحديات والفرص المتعلقة بأمن التشفير في عصر الحوسبة الكمومية.
- ورشة عمل: استعراض أحدث التطورات في مجال التشفير الكمي.

اليوم التدريبي الخامس:

استراتيجيات الأمن السيبراني المستقبلية

- أفضل الممارسات في أمن المعلومات وحماية البيانات في العصر الرقمي.
- تطوير استراتيجيات شاملة للأمن السيبراني.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي.
- التعامل مع حوادث الاختراق الأمني واستعادة البيانات.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.