مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

تقنيات الحوسبة السحابية الآمنة

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 8 – 12 / 6 / 2025.

مقدمة :

مع تزايد اعتماد المؤسسات والحكومات على تقنيات الحوسبة السحابية لتحسين الأداء وتوفير الموارد، تأتي التحديات الأمنية كعنصر رئيسي يجب التعامل معه بفعالية. تقنيات الحوسبة السحابية الآمنة تُعد من أهم الحلول التي تساهم في حماية البيانات والتطبيقات من التهديدات السيبرانية المتزايدة. الحفاظ على سرية المعلومات، حماية الخصوصية، وضمان الامتثال للمعايير الأمنية تعتبر من المهام الأساسية لأي نظام حوسبة سحابية. يهدف برنامج "تقنيات الحوسبة السحابية الآمنة" إلى تزويد المشاركين بالمعرفة والأدوات اللازمة لتأمين البيئات السحابية وضمان حماية البيانات الحساسة.

أهداف الورشة:

- فهم مفهوم الحوسبة السحابية وأنواعها ومزاياها.
- التعرف على المخاطر والتحديات الأمنية المتعلقة بالحوسبة السحابية.
- إتقان مهارات تقييم المخاطر الأمنية ووضع استراتيجيات فعالة للحماية.
- فهم مفهوم أمن البيانات المشتركة (Shared Responsibility Model) بين مزود الخدمة السحابية والعميل.
- التعرف على أحدث التقنيات والأدوات المستخدمة في أمن الحوسبة السحابية.
- تطوير سياسات وإجراءات لضمان الامتثال للمعايير واللوائح الأمنية.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين المستخدمين.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى الحوسبة السحابية

- مفهوم الحوسبة السحابية وأنواعها (عامة، خاصة، هجينة).
- مزايا وتحديات استخدام الحوسبة السحابية.
- نماذج الخدمات السحابية (IaaS، PaaS، SaaS).
- ورشة عمل: تحليل حالة استخدام للحوسبة السحابية وتحديد الفوائد والتحديات.

اليوم التدريبي الثاني:

المخاطر والتحديات الأمنية

- أنواع المخاطر الأمنية في الحوسبة السحابية (الوصول غير المصرح به، فقدان البيانات، هجمات الحرمان من الخدمة، اختراق الحسابات).
- التحديات الخاصة بأمن البيانات والخصوصية في السحابة.
- مفهوم أمن البيانات المشتركة (Shared Responsibility Model).
- ورشة عمل: تقييم المخاطر الأمنية في بيئة حوسبة سحابية افتراضية.

اليوم التدريبي الثالث:

استراتيجيات الأمن السيبراني

- مبادئ الأمن السيبراني (السرية، التكامل، التوافر).
- تصميم وتنفيذ استراتيجيات الأمن السيبراني الفعالة في السحابة.
- أمن الشبكات وأمن التطبيقات وأمن البيانات في بيئة الحوسبة السحابية.
- أفضل الممارسات في أمن الحوسبة السحابية.
- ورشة عمل: تطوير استراتيجية أمن سيبراني لحماية البيانات والأنظمة في السحابة.

اليوم التدريبي الرابع:

التقنيات والأدوات

- أحدث التقنيات والأدوات المستخدمة في أمن الحوسبة السحابية (مثل التشفير، إدارة الهوية والوصول، مراقبة الأمن، الكشف عن التهديدات، أمن البنية التحتية كخدمة).
- كيفية اختيار وتطبيق التقنيات والأدوات المناسبة.
- أهمية التحديث المستمر للتقنيات الأمنية.
- ورشة عمل: تجربة عملية على إحدى أدوات الأمن السيبراني في السحابة.

اليوم التدريبي الخامس:

الامتثال والوعي الأمني

- الإطار القانوني والتنظيمي لأمن البيانات والخصوصية في [اسم الدولة].
- تطوير سياسات وإجراءات لضمان الامتثال للمعايير واللوائح الأمنية.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين المستخدمين.
- التدريب والتوعية المستمرة بأفضل الممارسات الأمنية.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.
- إعداد خطط عمل فردية لتطبيق المعرفة المكتسبة.

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.