مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الأمن السحابي: تأمين البيانات والعمليات في بيئات الحوسبة السحابية الحكومية

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 2 – 6 / 11 / 2025.

مقدمة :

في ظل التحول الرقمي المتسارع، أصبحت الحوسبة السحابية جزءًا أساسيًا من البنية التحتية الرقمية للحكومات. تقدم الحوسبة السحابية مرونة أكبر وقدرات متقدمة لتخزين ومعالجة البيانات، إلا أنها تجلب معها تحديات أمنية تتعلق بحماية البيانات الحساسة، وتأمين العمليات الحكومية التي تعتمد على هذه التقنيات. "الأمن السحابي: تأمين البيانات والعمليات في بيئات الحوسبة السحابية الحكومية" هو برنامج تدريبي يهدف إلى تزويد المشاركين بالمعرفة والأدوات اللازمة لحماية البيانات الحكومية وإدارة العمليات الحساسة بشكل آمن ضمن البيئات السحابية. يتم التركيز على أفضل الممارسات الأمنية العالمية لتأمين البنية التحتية السحابية ومنع التهديدات السيبرانية التي قد تستهدف هذه الأنظمة.

أهداف الورشة:

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

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى الحوسبة السحابية

- مفهوم الحوسبة السحابية وأنواعها (عامة، خاصة، هجينة).
- مزايا وتحديات استخدام الحوسبة السحابية في القطاع الحكومي.
- نماذج الخدمات السحابية (IaaS، PaaS، SaaS) وتطبيقاتها في الحكومة.
- ورشة عمل: تحليل حالة استخدام للحوسبة السحابية في جهة حكومية 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، تهديدات داخلية).
- التحديات الخاصة بأمن البيانات والخصوصية في السحابة.
- مفهوم أمن البيانات المشتركة (Shared Responsibility Model) وتحديد مسؤوليات كل طرف.
- ورشة عمل: تقييم المخاطر الأمنية في بيئة حوسبة سحابية حكومية افتراضية.

اليوم التدريبي الثالث:

استراتيجيات الأمن السحابي

- 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 والعمليات الحكومية 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، CASB).
- 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 الموظفين الحكوميين.
- 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.