مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

أمن إنترنت الأشياء في الخدمات: تحديات وحلول

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 16 – 20 / 2 / 2025.

مقدمة :

إنترنت الأشياء (IoT) تعدّ من أبرز التقنيات الحديثة التي أحدثت تحولًا جذريًا في طريقة تقديم الخدمات الحكومية والتجارية. تتصل الأجهزة والمستشعرات بالإنترنت وتجمع البيانات لتوفير خدمات ذكية وفعّالة. مع توسع الاعتماد على هذه التقنية، تنشأ تحديات أمنية متزايدة تتعلق بحماية البيانات الشخصية وضمان أمان الشبكات التي تربط هذه الأجهزة. يهدف برنامج "أمن إنترنت الأشياء في الخدمات: تحديات وحلول" إلى تزويد المشاركين بفهم شامل للتحديات الأمنية المتعلقة بإنترنت الأشياء، وتعلم الحلول والتقنيات المتقدمة لحماية الأنظمة المتصلة وتعزيز الأمان في البيئات المختلفة.

أهداف الورشة:

- المسؤولون الحكوميون المعنيون بتطوير الخدمات المعتمدة على تقنيات إنترنت الأشياء.
- فرق تكنولوجيا المعلومات والأمن السيبراني في المؤسسات التي تستخدم إنترنت الأشياء.
- مزودو الخدمات التقنية والحلول الأمنية لإنترنت الأشياء.
- المستشارون والمتخصصون في أمن الشبكات والأنظمة المتصلة.
- الأكاديميون والباحثون المهتمون بتكنولوجيا إنترنت الأشياء وأمنها.
- مسؤولو المخاطر والإدارة في الشركات التي تعتمد على إنترنت الأشياء في تقديم الخدمات.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى إنترنت الأشياء

- مفهوم إنترنت الأشياء ومكوناته (الأجهزة، الشبكات، البيانات، التطبيقات).
- تطبيقات إنترنت الأشياء في مختلف الخدمات (المدن الذكية، الصحة، النقل، الصناعة).
- مزايا وتحديات استخدام إنترنت الأشياء.
- ورشة عمل: تحليل حالة استخدام لإنترنت الأشياء في خدمة معينة وتحديد الفوائد والتحديات.

اليوم التدريبي الثاني:

المخاطر والتحديات الأمنية

- أنواع المخاطر الأمنية في إنترنت الأشياء (الوصول غير المصرح به، هجمات الحرمان من الخدمة، اختراق البيانات، التزييف والاحتيال).
- التحديات الخاصة بأمن إنترنت الأشياء (التنوع، التوزيع، القدرة المحدودة للأجهزة).
- مفهوم أمن التصميم (Security by Design) وأهميته في إنترنت الأشياء.
- ورشة عمل: تقييم المخاطر الأمنية في نظام إنترنت الأشياء افتراضي.

اليوم التدريبي الثالث:

استراتيجيات الأمن السيبراني

- مبادئ الأمن السيبراني (السرية، التكامل، التوافر).
- تصميم وتنفيذ استراتيجيات الأمن السيبراني الفعالة لإنترنت الأشياء.
- أمن الأجهزة، أمن الشبكات، أمن البيانات، أمن التطبيقات.
- أفضل الممارسات في أمن إنترنت الأشياء.
- ورشة عمل: تطوير استراتيجية أمن سيبراني لنظام إنترنت الأشياء.

اليوم التدريبي الرابع:

التقنيات والأدوات

- أحدث التقنيات والأدوات المستخدمة في أمن إنترنت الأشياء (مثل التشفير، المصادقة، التحكم في الوصول، الكشف عن التهديدات، الذكاء الاصطناعي في الأمن السيبراني).
- كيفية اختيار وتطبيق التقنيات والأدوات المناسبة.
- أهمية التحديث المستمر للتقنيات الأمنية.
- ورشة عمل: تجربة عملية على إحدى أدوات الأمن السيبراني لإنترنت الأشياء.

اليوم التدريبي الخامس:

الاستجابة للحوادث والتعافي

- أهمية وجود خطة للاستجابة للحوادث الأمنية والتعافي منها في سياق إنترنت الأشياء.
- مراحل الاستجابة للحوادث (الكشف، الاحتواء، الاستئصال، التعافي).
- التحقيق الجنائي الرقمي في حوادث إنترنت الأشياء.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين المستخدمين ومقدمي الخدمات.
- ورشة عمل: تطوير خطة للاستجابة للحوادث الأمنية في نظام إنترنت الأشياء.

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.