مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

تطبيقات الأمن السيبراني في البيئات الحكومية المعتمدة على إنترنت الأشياء (IoT).

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 7 – 11 / 12 / 2025.

مقدمة :

الأشياء (IoT) من أبرز التطورات التي ساهمت في تحسين العمليات والخدمات الحكومية من خلال الاتصال الذكي بين الأجهزة وتحليل البيانات الضخمة. ومع ذلك، فإن الاعتماد المتزايد على هذه التقنيات يعرض الحكومات لمجموعة جديدة من التهديدات السيبرانية التي يمكن أن تستغل الثغرات الأمنية في الشبكات والأجهزة المتصلة. يتطلب تأمين البيئات الحكومية التي تعتمد على إنترنت الأشياء تطبيق استراتيجيات أمنية متقدمة لحماية البيانات والأنظمة من الهجمات السيبرانية المعقدة. يهدف هذا البرنامج التدريبي "تطبيقات الأمن السيبراني في البيئات الحكومية المعتمدة على إنترنت الأشياء (IoT)" إلى تزويد المشاركين بالمهارات والمعرفة اللازمة لتأمين الأجهزة والشبكات المتصلة بالإنترنت في البيئات الحكومية.

أهداف الورشة:

- فهم مفهوم إنترنت الأشياء وتطبيقاته في الخدمات الحكومية.
- التعرف على المخاطر والتحديات الأمنية المتعلقة بإنترنت الأشياء في البيئات الحكومية.
- إتقان مهارات تقييم المخاطر الأمنية وتحديد نقاط الضعف في أنظمة إنترنت الأشياء الحكومية.
- تصميم وتنفيذ استراتيجيات الأمن السيبراني الفعالة لحماية أجهزة وبيانات إنترنت الأشياء في الحكومة.
- التعرف على أحدث التقنيات والأدوات المستخدمة في أمن إنترنت الأشياء في القطاع الحكومي.
- تطوير خطط الاستجابة للحوادث الأمنية والتعافي منها في سياق إنترنت الأشياء الحكومية.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين الحكوميين ومستخدمي الخدمات.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى إنترنت الأشياء في الحكومة

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

اليوم التدريبي الثاني:

المخاطر والتحديات الأمنية

- أنواع المخاطر الأمنية في إنترنت الأشياء في البيئات الحكومية (الوصول غير المصرح به، هجمات الحرمان من الخدمة، اختراق البيانات، التلاعب بالأجهزة، انتهاك الخصوصية).
- التحديات الخاصة بأمن إنترنت الأشياء في الحكومة (التنوع، التوزيع، القدرة المحدودة للأجهزة، حساسية البيانات).
- مفهوم أمن التصميم (Security by Design) وأهميته في إنترنت الأشياء الحكومية.
- ورشة عمل: تقييم المخاطر الأمنية في نظام إنترنت الأشياء حكومي افتراضي.

اليوم التدريبي الثالث:

استراتيجيات الأمن السيبراني

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

اليوم التدريبي الرابع:

التقنيات والأدوات

- أحدث التقنيات والأدوات المستخدمة في أمن إنترنت الأشياء في البيئات الحكومية (مثل التشفير، المصادقة، التحكم في الوصول، تقسيم الشبكة، 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 الحكومية.
- مراحل الاستجابة للحوادث (الكشف، الاحتواء، الاستئصال، التعافي).
- التحقيق الجنائي الرقمي في حوادث إنترنت الأشياء.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين الحكوميين ومستخدمي الخدمات.
- ورشة عمل: تطوير خطة للاستجابة للحوادث الأمنية في نظام إنترنت الأشياء حكومي.

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.