مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الشبكات الذكية وحماية البيانات في المؤسسات

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 10 – 14 / 8 / 2025.

مقدمة :

تشكل الشبكات الذكية العمود الفقري للتقنيات الحديثة التي تعتمد عليها المؤسسات في تحسين الأداء وتعزيز الكفاءة. توفر الشبكات الذكية قدرات متقدمة لإدارة البيانات والتواصل السلس بين الأجهزة المختلفة، لكنها في نفس الوقت تعرض المؤسسات لتحديات أمنية جديدة تتعلق بحماية البيانات الحساسة وضمان سرية المعلومات. في ظل التهديدات السيبرانية المتزايدة، أصبح من الضروري على المؤسسات تطبيق استراتيجيات فعالة لحماية بياناتها وشبكاتها الذكية. يهدف برنامج "الشبكات الذكية وحماية البيانات في المؤسسات" إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لإدارة الشبكات الذكية بفعالية وحماية البيانات من التهديدات السيبرانية المتقدمة.

أهداف الورشة:

- فهم مفهوم الشبكات الذكية ومكوناتها الرئيسية.
- التعرف على فوائد ومزايا استخدام الشبكات الذكية في المؤسسات.
- تحليل التحديات الأمنية التي تواجه الشبكات الذكية.
- إتقان مهارات تصميم وتنفيذ استراتيجيات أمنية فعالة للشبكات الذكية.
- التعرف على أحدث التقنيات والأدوات المستخدمة في أمن الشبكات الذكية.
- تطوير خطط الاستجابة للحوادث الأمنية والتعافي منها في سياق الشبكات الذكية.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى الشبكات الذكية

- مفهوم الشبكات الذكية ومكوناتها الرئيسية (أجهزة الاستشعار، تحليلات البيانات، الأتمتة).
- فوائد ومزايا استخدام الشبكات الذكية في المؤسسات (الكفاءة، التحكم، الأمان).
- تطبيقات الشبكات الذكية في مختلف القطاعات (الصناعة، الطاقة، النقل، المدن الذكية).
- ورشة عمل: تحليل حالة استخدام للشبكات الذكية في مؤسسة وتحديد الفوائد والتحديات.

اليوم التدريبي الثاني:

التحديات الأمنية في الشبكات الذكية

- أنواع المخاطر الأمنية في الشبكات الذكية (الوصول غير المصرح به، هجمات الحرمان من الخدمة، اختراق البيانات، التلاعب بالأجهزة).
- نقاط الضعف المحتملة في الشبكات الذكية.
- مفهوم أمن التصميم (Security by Design) وأهميته في الشبكات الذكية.
- ورشة عمل: تقييم المخاطر الأمنية في شبكة ذكية افتراضية.

اليوم التدريبي الثالث:

استراتيجيات أمن الشبكات الذكية

- مبادئ الأمن السيبراني (السرية، التكامل، التوافر).
- تصميم وتنفيذ استراتيجيات الأمن السيبراني الفعالة للشبكات الذكية.
- أمن الأجهزة، أمن الشبكات، أمن البيانات، أمن التطبيقات في سياق الشبكات الذكية.
- أفضل الممارسات في أمن الشبكات الذكية.
- ورشة عمل: تطوير استراتيجية أمن سيبراني لشبكة ذكية.

اليوم التدريبي الرابع:

التقنيات والأدوات

- أحدث التقنيات والأدوات المستخدمة في أمن الشبكات الذكية (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 للشبكات الذكية.

اليوم التدريبي الخامس:

الاستجابة للحوادث والتعافي

- أهمية وجود خطة للاستجابة للحوادث الأمنية والتعافي منها في سياق الشبكات الذكية.
- مراحل الاستجابة للحوادث (الكشف، الاحتواء، الاستئصال، التعافي).
- التحقيق الجنائي الرقمي في حوادث الشبكات الذكية.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين.
- ورشة عمل: تطوير خطة للاستجابة للحوادث الأمنية في شبكة ذكية.

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.