مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

أمن البنى التحتية الحيوية: حماية الشبكات من الهجمات المتقدمة

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 12 – 16 / 01 / 2025.

مقدمة :

في ظل التهديدات السيبرانية المتزايدة وتطور الهجمات الإلكترونية التي تستهدف البنى التحتية الحيوية، أصبح من الضروري على الحكومات تطوير استراتيجيات فعّالة لحماية الشبكات والأنظمة الحساسة. البنى التحتية الحيوية تشمل العديد من القطاعات الحيوية مثل الطاقة، المياه، الاتصالات، والنقل، التي تعد الأساس لعمل الحكومات والمجتمعات. تتطلب حماية هذه الأنظمة الحساسة تقنيات متقدمة وأساليب مبتكرة للتصدي للهجمات السيبرانية وتعزيز الأمن. يهدف برنامج "أمن البنى التحتية الحيوية: حماية الشبكات من الهجمات المتقدمة" إلى تزويد المشاركين بالمهارات والمعرفة اللازمة لحماية الأنظمة الحيوية من التهديدات المتقدمة، وضمان استمرارية العمل بأمان.

أهداف الورشة:

- فهم مفهوم البنى التحتية الحيوية وأهميتها.
- التعرف على التهديدات السيبرانية المتقدمة التي تستهدف البنى التحتية الحيوية.
- إتقان مهارات تقييم المخاطر الأمنية وتحديد نقاط الضعف.
- تصميم وتنفيذ استراتيجيات الأمن السيبراني الفعالة لحماية البنى التحتية الحيوية.
- التعرف على أحدث التقنيات والأدوات المستخدمة في الأمن السيبراني.
- تطوير خطط الاستجابة للحوادث الأمنية والتعافي منها.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين.

محتويات الورشة:

اليوم التدريبي الأول:

البنى التحتية الحيوية والتهديدات السيبرانية

- مفهوم البنى التحتية الحيوية وأنواعها (الطاقة، المياه، النقل، الاتصالات).
- أهمية حماية البنى التحتية الحيوية.
- أنواع التهديدات السيبرانية المتقدمة (الهجمات المستهدفة، البرمجيات الخبيثة المتقدمة، هجمات الحرمان من الخدمة).
- ورشة عمل: تحليل حالة اختراق أمني في بنية تحتية حيوية وتحديد نقاط الضعف.

اليوم التدريبي الثاني:

تقييم المخاطر الأمنية

- مفهوم تقييم المخاطر الأمنية وأهميته.
- منهجيات تقييم المخاطر (مثل NIST، ISO 27005).
- تحديد الأصول الحرجة وتقييم نقاط الضعف.
- تقدير احتمالية وتأثير الهجمات السيبرانية.
- ورشة عمل: تطبيق منهجية تقييم المخاطر على بنية تحتية حيوية.

اليوم التدريبي الثالث:

استراتيجيات الأمن السيبراني

- مبادئ الأمن السيبراني (السرية، التكامل، التوافر).
- تصميم وتنفيذ استراتيجيات الأمن السيبراني الفعالة.
- أمن الشبكات وأمن التطبيقات وأمن البيانات.
- أفضل الممارسات في الأمن السيبراني.
- ورشة عمل: تطوير استراتيجية أمن سيبراني لبنية تحتية حيوية.

اليوم التدريبي الرابع:

التقنيات والأدوات

- أحدث التقنيات والأدوات المستخدمة في الأمن السيبراني (مثل جدران الحماية، أنظمة الكشف عن الاختراق، تحليل السلوك، 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.

اليوم التدريبي الخامس:

الاستجابة للحوادث والتعافي

- أهمية وجود خطة للاستجابة للحوادث الأمنية والتعافي منها.
- مراحل الاستجابة للحوادث (الكشف، الاحتواء، الاستئصال، التعافي).
- التحقيق الجنائي الرقمي.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي.
- ورشة عمل: تطوير خطة للاستجابة للحوادث الأمنية في بنية تحتية حيوية.

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.