مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

إدارة الأمن السيبراني في البنى التحتية الحيوية.

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 23 – 27 / 03 / 2025.

مقدمة :

تتزايد أهمية الأمن السيبراني في ظل التطور التكنولوجي المتسارع، وخاصة في البنى التحتية الحيوية التي تشكل عصب الحياة لأي دولة .فأمن شبكات الطاقة، والمياه، والمواصلات، والاتصالات، وغيرها من القطاعات الحيوية، أصبح ضرورة ملحة لحماية المجتمعات من التهديدات السيبرانية المتزايدة .يأتي هذا البرنامج التدريبي المتقدم "إدارة الأمن السيبراني في البنى التحتية الحيوية "ليقدم مقاربة شاملة وحديثة لإدارة وتأمين هذه البنى، مع التركيز على أحدث التقنيات و الاستراتيجيات في هذا المجال .يهدف البرنامج إلى تزويد المشاركين بالمعرفة و المهارات اللازمة لحماية البنى التحتية الحيوية من الهجمات السيبرانية، و ضمان استمرارية عملها بكفاءة و فاعلية.

أهداف الورشة:

- فهم مفهوم الأمن السيبراني و أهميته في حماية البنى التحتية الحيوية .
- التعرف على أنواع التهديدات السيبرانية التي تستهدف البنى التحتية الحيوية .
- تحليل نقاط الضعف في البنى التحتية الحيوية و تقييم المخاطر المحتملة .
- تطبيق أفضل الممارسات و الاستراتيجيات في مجال إدارة الأمن السيبراني .
- استخدام أحدث الأدوات و التقنيات في كشف و صد الهجمات السيبرانية .
- تطوير خطط استجابة فعالة للحوادث السيبرانية .
- بناء كوادر مؤهلة في مجال الأمن السيبراني للبنى التحتية الحيوية.

محتويات الورشة:

اليوم الأول:

- **مقدمة في الأمن السيبراني للبنى التحتية الحيوية :**

مفهوم الأمن السيبراني و أهميته.

أنواع البنى التحتية الحيوية و خصائصها.

التحديات و المخاطر السيبرانية التي تواجه البنى التحتية الحيوية.

- **التهديدات السيبرانية و أساليب الهجوم :**

أنواع الهجمات السيبرانية)البرمجيات الخبيثة، هجمات الحرمان من الخدمة، التصيد الاحتيالي، وغيرها.(

أساليب الهجوم و تقنيات الاختراق المستخدمة من قبل المهاجمين.

أمثلة على هجمات سيبرانية استهدفت بنى تحتية حيوية.

اليوم الثاني:

- **تأمين شبكات البنى التحتية الحيوية :**

هندسة الأمن السيبراني لشبكات البنى التحتية الحيوية.

بروتوكولات الأمان و تقنيات التشفير.

جدران الحماية و أنظمة كشف و منع التسلل.

- **حماية البيانات و الأنظمة في البنى التحتية الحيوية :**

تأمين قواعد البيانات و الأنظمة الحساسة.

إدارة الهويات و التحكم في الوصول.

النسخ الاحتياطي و استعادة البيانات.

اليوم الثالث:

- **الاستجابة للحوادث السيبرانية و إدارتها :**

خطوات الاستجابة للحوادث السيبرانية.

تحليل أسباب الحوادث و جمع الأدلة الجنائية الرقمية.

التعامل مع وسائل الإعلام و إدارة الأزمة.

- **استمرارية الأعمال و التعافي من الكوارث :**

تطوير خطط استمرارية الأعمال و التعافي من الكوارث.

اختبار خطط الاستجابة و التأكد من فعاليتها.

ضمان استمرارية الخدمات الحيوية في حالات الطوارئ.

اليوم الرابع:

- **التقنيات الحديثة في الأمن السيبراني :**

الذكاء الاصطناعي و تعلم الآلة في الأمن السيبراني.

تحليل البيانات الضخمة و اكتشاف التهديدات المتقدمة.

تقنيات الأمن السيبراني في بيئات السحابة الحاسوبية.

- **إدارة الأمن السيبراني و الحوكمة :**

أطر عمل و معايير الأمن السيبراني.

إدارة المخاطر و تقييم الامتثال.

بناء ثقافة الأمن السيبراني في المؤسسات.

اليوم الخامس:

- **ورشة عمل و تمارين تطبيقية :**

محاكاة هجمات سيبرانية و تطبيق مهارات الاستجابة للحوادث.

تحليل حالات دراسية و مناقشة أفضل الممارسات.

تطوير خطط أمن سيبراني للبنى التحتية الحيوية.

- **اختبار و تقييم المهارات :**

اختبارات نظرية و عملية لتقييم المهارات المكتسبة خلال البرنامج.

مناقشة التحديات و تقديم المشورة و الإرشاد للمشاركين

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.