مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الأمن السيبراني وحماية البنية التحتية الحساسة

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 12 – 16 / 01 / 2025.

مقدمة :

تُشكل البنية التحتية الحساسة في المؤسسات الحكومية (مثل شبكات الكهرباء، و انظمة الاتصالات، و الخدمات المالية (عصبًا حيويًا لِلحفاظ على استمرارية الخدمات الحكومية و حماية الامن الوطني .و مع التطور المُتسارع لِلهجمات السيبرانية و تنوع اهدافها، تبرز أهمية تعزيز الامن السيبراني و حماية هذه البنية من الاختراقات و التعطيل.

يهدف هذا البرنامج التدريبي الى تزويد المشاركين بالمعرفة و المهارات اللازمة لِحماية البنية التحتية الحساسة في المؤسسات الحكومية من الهجمات السيبرانية .سيركز البرنامج على استعراض مجموعة واسعة من المواضيع، مثل انواع التهديدات السيبرانية)بما فيها البرمجيات الخبيثة و هجمات الحرمان من الخدمة(، و تقنيات الحماية و الوقاية)مثل جدران الحماية و انظمة كشف التسلل(، و ادارة الازمات السيبرانية، و التعاون و تبادل المعلومات بين المؤسسات الحكومية .كما سيتناول البرنامج افضل الممارسات في مجال حوكمة الامن السيبراني و ادارة المخاطر، و كيفية بناء قدرات وطنية قوية في مجال الامن السيبراني .و سيُقدم البرنامج ايضًا تمارين محاكاة و دراسات حالة واقعية لتعزيز فهم المشاركين و تطبيق المعارف المكتسبة في بيئات عمل مُحاكية.

أهداف الورشة:

- فهم مبادئ الامن السيبراني و أهميته في حماية البنية التحتية الحساسة في المؤسسات الحكومية .
- التعرف على مختلف انواع التهديدات السيبرانية و أساليب الهجوم .
- اتقان مهارات الحماية و الوقاية من الهجمات السيبرانية و تطبيق افضل الممارسات .
- ادارة الازمات السيبرانية و التعامل مع الاختراقات الامنية بِكفاءة و فعالية .
- تطبيق افضل الممارسات في مجال حوكمة الامن السيبراني و ادارة المخاطر .
- بناء قدرات وطنية قوية في مجال الامن السيبراني و تطوير الكوادر الوطنية .
- تعزيز التعاون و تبادل المعلومات بين المؤسسات الحكومية لِمواجهة التهديدات السيبرانية.

محتويات الورشة:

اليوم الاول:

مقدمة في الامن السيبراني

- مبادئ الامن السيبراني و أهميته في العصر الرقمي.
- مفهوم البنية التحتية الحساسة و اهميتها الاستراتيجية.
- انواع التهديدات السيبرانية و اهدافها.
- ورشة عمل :تحديد الاصول و البيانات الحرجة في البنية التحتية الحساسة.

اليوم الثاني:

التهديدات السيبرانية و اساليب الهجوم

- انواع التهديدات السيبرانية)البرمجيات الخبيثة، هجمات الحرمان من الخدمة، التصيد.(
- اساليب الهجوم السيبراني و تقنيات الاختراق.
- ثغرات الامن السيبراني و كيفية استغلالها.
- تمرين محاكاة :تحليل هجوم سيبراني و تحديد اساليب الهجوم المستخدمة.

اليوم الثالث: الحماية والوقاية من الهجمات السيبرانية

- تقنيات و ادوات الحماية من الهجمات السيبرانية)جدران الحماية، انظمة كشف التسلل.(
- امن الشبكات و الانظمة و التطبيقات.
- امن البيانات و تشفيرها و حمايتها.
- ورشة عمل :تطبيق تقنيات الحماية و الوقاية على نظام مُحاكى.

اليوم الرابع: ادارة الازمات السيبرانية

- مراحل ادارة الازمات السيبرانية و خطوات الاستجابة.
- خطط الاستجابة للحوادث السيبرانية و اجراءات التعامل مع الاختراقات.
- التحقيق في الهجمات السيبرانية و جمع الادلة.
- تمرين محاكاة :التعامل مع حادث سيبراني و تطبيق خطة الاستجابة.

اليوم الخامس: حوكمة الامن السيبراني و التعاون

- مبادئ حوكمة الامن السيبراني و افضل الممارسات.
- ادارة مخاطر الامن السيبراني و وضع السياسات.
- التعاون و تبادل المعلومات بين المؤسسات.
- جلسة نقاش :تطوير استراتيجية وطنية للأمن السيبراني و حماية البنية التحتية الحساسة.

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.