مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

أمن الاتصالات وحماية الشبكات في المؤسسات الحكومية الحساسة.

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 07 – 11 / 12 / 2025.

مقدمة :

تُشكل الاتصالات و الشبكات عصبًا حيويًا لِعمل المؤسسات الحكومية الحساسة، حيث تُدير الخدمات الحكومية الأساسية و تُخزن كميات هائلة من البيانات الحساسة .و تُشكل الهجمات السيبرانية و عمليات التجسس و التسريب تهديدًا مُتزايدًا لِهذه الشبكات، مما قد يُؤدي إلى تعطيل الخدمات الحكومية، و سرقة البيانات، و الإضرار بالأمن الوطني .و لذلك، تُعدّ حماية شبكات الاتصالات في المؤسسات الحكومية الحساسة من أهم أولويات الأمن السيبراني و الأمن الوطني.

يهدف هذا البرنامج التدريبي إلى تزويد المشاركين بالمعرفة و المهارات اللازمة لِحماية شبكات الاتصالات في المؤسسات الحكومية الحساسة من مختلف التهديدات .سيركز البرنامج على استعراض مجموعة واسعة من المواضيع، مثل مبادئ أمن الاتصالات و أنواع التهديدات)بما فيها التجسس و التسريب و التخريب(، و تقنيات الحماية و الوقاية)مثل التشفير و جدران الحماية و أنظمة كشف التسلل(، و إدارة الأزمات و الاستجابة للحوادث، و التعاون و تبادل المعلومات بين المؤسسات الحكومية .كما سيتناول البرنامج أفضل الممارسات في مجال أمن الاتصالات و حوكمة أمن المعلومات، و كيفية بناء فرق استجابة للحوادث فعّالة، و تطوير الكوادر الوطنية في هذا المجال .و سيُقدم البرنامج أيضًا تمارين محاكاة و دراسات حالة واقعية لتعزيز فهم المشاركين و تطبيق المعارف المكتسبة في بيئات عمل مُحاكية.

أهداف الورشة:

- فهم مبادئ أمن الاتصالات و أهميته في حماية المؤسسات الحكومية الحساسة .
- التعرف على مختلف أنواع التهديدات و المخاطر التي تُهدد شبكات الاتصالات الحكومية .
- إتقان مهارات الحماية و الوقاية من التهديدات و تطبيق أفضل الممارسات الأمنية .
- إدارة الأزمات و الاستجابة للحوادث الأمنية بِكفاءة و فعالية لِتقليل الضرر .
- تطبيق أفضل الممارسات في مجال أمن الاتصالات و حوكمة أمن المعلومات .
- بناء فرق استجابة للحوادث فعّالة و قادرة على التعامل مع التهديدات بِسرعة .
- تعزيز التعاون و تبادل المعلومات بين المؤسسات الحكومية لِمواجهة التهديدات بِشكل مُشترك

محتويات الورشة:

اليوم الأول:

مُقدمة في أمن الاتصالات و حماية الشبكات

- مبادئ أمن الاتصالات و أهميته في العصر الرقمي و علاقته بِالأمن الوطني.
- مفهوم حماية الشبكات و أهم التشريعات و القوانين ذات الصلة)مثل قوانين الخصوصية و الأمن السيبراني.(
- أنواع التهديدات و المخاطر)التجسس، التسريب، التخريب، الهجمات السيبرانية، الأخطاء البشرية.(
- ورشة عمل :تحديد الأصول و البيانات الحرجة في شبكات الاتصالات الحكومية و تقييم مستوى حمايتها.

اليوم الثاني:

التشفير و أمن الشبكات

- مبادئ و أساليب التشفير و أنواع خوارزميات التشفير)التشفير المُتماثل، التشفير غير المُتماثل.(
- تطبيقات التشفير في حماية الاتصالات و البيانات)بروتوكولات VPN، .SSL/TLS).
- أمن الشبكات و الخوادم و أجهزة التوجيه و المُفاتيح و نقاط الوصول اللاسلكية.
- تمرين محاكاة :تطبيق تقنيات التشفير و تأمين شبكة اتصالات مُحاكية.

اليوم الثالث:

أنظمة كشف و منع التسلل

- أنظمة كشف التسلل (IDS)و أنظمة منع التسلل (IPS)و كيفية عملها و استخدامها.
- تحليل سجلات الأحداث و رصد الأنشطة المُريبة على شبكات الاتصالات.
- أدوات و تقنيات مراقبة و تحليل حركة الشبكة لِكشف الهجمات و التهديدات.
- ورشة عمل :تحليل بيانات و سجلات أحداث شبكة اتصالات مُحاكية لِكشف هجمات و أنشطة مُريبة.

اليوم الرابع:

إدارة الأزمات و الاستجابة للحوادث

- مراحل إدارة الأزمات و خطوات الاستجابة)الكشف، الاحتواء، التحقيق، المعالجة، التعافي.(
- خطط الاستجابة للحوادث الأمنية و إجراءات التعامل مع الاختراقات و إدارة الأدلة الرقمية.
- التحقيق في الهجمات السيبرانية و جمع الأدلة الرقمية و التعاون مع الجهات الأمنية.
- تمرين محاكاة :التعامل مع حادث أمني على شبكة اتصالات و تطبيق خطة الاستجابة لِاحتواء الضرر

اليوم الخامس:

حوكمة أمن الاتصالات و التعاون و التقييم

- مبادئ حوكمة أمن الاتصالات و أفضل الممارسات)مثل معايير ISO 27001و NIST).
- إدارة مخاطر أمن الاتصالات و وضع السياسات و الإجراءات الأمنية و التدقيق الأمني.
- التعاون و تبادل المعلومات بين المؤسسات الحكومية و الجهات الأمنية لِمواجهة التهديدات بِشكل مُشترك.
- بناء فرق استجابة للحوادث (CERTs)و تطوير آليات التنسيق و التواصل أثناء الأزمات.
- جلسة ختامية :مناقشة التحديات و الفرص المُستقبلية في مجال أمن الاتصالات و حماية الشبكات في المؤسسات الحكومية الحساسة.
- تقييم أداء المشاركين في البرنامج التدريبي و قياس مُستوى فهمهم للمواضيع و المهارات المُكتسبة

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.