مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

أمن المعلومات وتحليل التهديدات السيبرانية في المؤسسات الحكومية

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 7 – 11 / 12 / 2025.

مقدمة :

تُشكل أمن المعلومات خط الدفاع الأول للمؤسسات الحكومية في العصر الرقمي، حيث تُعتمد على التكنولوجيا في جميع العمليات و الخدمات .و مع التطور المُتسارع لِلهجمات السيبرانية و تنوع أساليبها، تبرز أهمية الابتكار في تقنيات أمن المعلومات و تحليل التهديدات لِحماية البيانات الحساسة و ضمان استمرارية العمل الحكومي.

يهدف هذا البرنامج التدريبي إلى تزويد المشاركين بأحدث المعارف و المهارات في مجال أمن المعلومات و تحليل التهديدات السيبرانية .سيركز البرنامج على استعراض مجموعة واسعة من المواضيع، مثل أحدث أنواع التهديدات السيبرانية، و تقنيات الحماية المُتقدمة)بما فيها الذكاء الاصطناعي و التعلم الآلي(، و أساليب الاستجابة للحوادث و التحقيق الجنائي الرقمي .كما سيتناول البرنامج أفضل الممارسات في مجال حوكمة أمن المعلومات و إدارة المخاطر، و كيفية بناء فرق استجابة للحوادث فعّالة، و تعزيز التعاون و تبادل المعلومات بين المؤسسات الحكومية .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 المعلومات و أهميته في حماية المؤسسات الحكومية في العصر الرقمي .
- التعرف على أحدث أنواع التهديدات السيبرانية و أساليب الهجوم المُتطورة .
- إتقان مهارات تحليل التهديدات و تقييم المخاطر الأمنية .
- تطبيق تقنيات الحماية المُتقدمة)مثل الذكاء الاصطناعي و التعلم الآلي (لِمنع و الكشف عن الهجمات .
- إدارة الحوادث السيبرانية و التحقيق فيها باستخدام أحدث الأساليب و الأدوات .
- تطبيق أفضل الممارسات في مجال حوكمة أمن المعلومات و إدارة المخاطر .
- تعزيز التعاون و تبادل المعلومات بين المؤسسات الحكومية لِمواجهة التهديدات السيبرانية

محتويات الورشة:

اليوم الاول :

مُقدمة في أمن المعلومات و التهديدات السيبرانية

- مبادئ أمن المعلومات و أهم المفاهيم)سرية المعلومات، سلامة المعلومات، توافر المعلومات.(
- أحدث أنواع التهديدات السيبرانية)الهجمات المُستهدفة، البرمجيات الخبيثة المُتقدمة، هجمات الفدية.(
- أساليب الهجوم السيبراني و تقنيات الاختراق)الهندسة الاجتماعية، ثغرات الأمن.(
- **ورشة عمل :**تحليل هجوم سيبراني و تحديد أساليب الهجوم المُستخدمة و الأهداف المُستهدفة.

اليوم الثاني:

تحليل التهديدات و تقييم المخاطر

- مناهج و أدوات تحليل التهديدات السيبرانية .(Threat Intelligence)
- تقييم المخاطر الأمنية و تحديد الأصول الحرجة و نقاط الضعف.
- استخدام منصات تحليل التهديدات و مشاركة المعلومات الأمنية.
- **تمرين محاكاة :**تطبيق أدوات تحليل التهديدات و تقييم المخاطر على سيناريو مُحدد.

اليوم الثالث:

تقنيات الحماية المُتقدمة

- أنظمة منع التسلل و الكشف عن الاختراقات .(IPS/IDS)
- تقنيات الذكاء الاصطناعي و التعلم الآلي في الكشف عن و منع الهجمات السيبرانية.
- أمن الشبكات و الأنظمة و التطبيقات و القواعد البيانية.
- **ورشة عمل :**تطبيق تقنيات الحماية المُتقدمة على نظام مُحاكى لِمنع هجمات سيبرانية.

اليوم الرابع:

الاستجابة للحوادث و التحقيق الجنائي الرقمي

- مراحل إدارة الحوادث السيبرانية و خطوات الاستجابة)احتواء الهجوم، استعادة البيانات.(
- التحقيق الجنائي الرقمي و جمع الأدلة الرقمية و تحليلها.
- أدوات و تقنيات التحقيق الجنائي الرقمي)تحليل البرمجيات الخبيثة، استعادة الملفات المُحذوفة.(
- **تمرين محاكاة :**التعامل مع حادث سيبراني و تطبيق مهارات التحقيق الجنائي الرقمي.

اليوم الخامس :حوكمة أمن المعلومات و التعاون

- مبادئ حوكمة أمن المعلومات و أفضل الممارسات .(ISO 27001)
- إدارة مخاطر أمن المعلومات و وضع السياسات و الإجراءات الأمنية.
- التعاون و تبادل المعلومات بين المؤسسات الحكومية و فرق الاستجابة للحوادث.
- **جلسة نقاش :**تطوير استراتيجية أمن سيبراني وطنية و تعزيز التعاون في مجال أمن المعلومات

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.