مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

تحليل الجرائم الإلكترونية ومكافحة الهجمات السيبرانية المتقدمة.

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 21 – 25 / 09 / 2025.

مقدمة :

تُشكل الجرائم الإلكترونية و الهجمات السيبرانية المُتقدمة تهديدًا مُتزايدًا للمؤسسات الحكومية و الأفراد و الأمن الوطني، حيث تُستخدم أساليب مُعقدة و تقنيات مُتطورة لِلسرقة و التخريب و التجسس و تعطيل الخدمات .و تتطلب مكافحة هذه الجرائم امتلاك القدرة على تحليلها و فهم أساليبها و تطوير استراتيجيات فعّالة لِلحماية و الوقاية و الرد على الهجمات.

يهدف هذا البرنامج التدريبي إلى تزويد المشاركين بالمعرفة و المهارات اللازمة لِتحليل الجرائم الإلكترونية و مكافحة الهجمات السيبرانية المُتقدمة .سيركز البرنامج على استعراض مجموعة واسعة من المواضيع، مثل أنواع الجرائم الإلكترونية و الهجمات السيبرانية، و أساليب التحقيق الجنائي الرقمي، و تقنيات الحماية و الوقاية)بما فيها الذكاء الاصطناعي و التعلم الآلي(، و إدارة الأزمات السيبرانية، و التعاون و تبادل المعلومات بين المؤسسات الحكومية .كما سيتناول البرنامج أفضل الممارسات في مجال الأمن السيبراني، 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 مفهوم الجرائم الإلكترونية و الهجمات السيبرانية المُتقدمة و أثرها على الأفراد و المؤسسات و الدول .
- التعرف على مختلف أنواع الجرائم الإلكترونية و الهجمات السيبرانية و أساليب تنفيذها .
- إتقان مهارات التحقيق الجنائي الرقمي و جمع و تحليل الأدلة الإلكترونية .
- تطبيق تقنيات الحماية و الوقاية من الهجمات السيبرانية باستخدام أحدث الأساليب و الأدوات .
- إدارة الأزمات السيبرانية و التعامل مع الاختراقات الأمنية بِكفاءة و فعالية .
- تطبيق أفضل الممارسات في مجال الأمن السيبراني و حوكمة أمن المعلومات .
- تعزيز التعاون و تبادل المعلومات بين المؤسسات الحكومية و الجهات الأمنية لِمواجهة التهديدات السيبرانية..

محتويات الورشة:

اليوم الأول:

مُقدمة في الجرائم الإلكترونية و الهجمات السيبرانية

- مفهوم الجرائم الإلكترونية و الهجمات السيبرانية و أنواعها و أهدافها و تأثيرها.
- الإطار القانوني و التشريعي لِمُكافحة الجرائم الإلكترونية في الدولة.
- أمثلة على جرائم إلكترونية و هجمات سيبرانية و دراسة أسباب وقوعها و نتائجها.
- ورشة عمل :تحديد الأصول و البيانات الحرجة في مؤسسة حكومية و تقييم مخاطر الأمن السيبراني.

اليوم الثاني:

تحليل الجرائم الإلكترونية و أساليب الهجوم

- أنواع الجرائم الإلكترونية)الاحتيال، الابتزاز، التشهير، التجسس، التخريب.(
- أساليب الهجوم السيبراني و تقنيات الاختراق)الهندسة الاجتماعية، ثغرات الأمن السيبراني، البرمجيات الخبيثة.(
- أدوات و تقنيات التحقيق الجنائي الرقمي)جمع الأدلة، تحليل البرمجيات الخبيثة، استعادة البيانات.(
- تمرين محاكاة :تحليل جريمة إلكترونية و تحديد أساليب الهجوم المُستخدمة و كيفية جمع الأدلة.

اليوم الثالث:

مكافحة الهجمات السيبرانية المُتقدمة

- أنواع الهجمات السيبرانية المُتقدمة)الهجمات المُستهدفة، هجمات سلسلة التوريد، التزييف العميق.(
- تقنيات الحماية و الوقاية من الهجمات السيبرانية)جدران الحماية، أنظمة كشف التسلل، الذكاء الاصطناعي.(
- أمن الشبكات و الخوادم و قواعد البيانات و التطبيقات و الأجهزة المُتصلة.
- ورشة عمل :تطبيق تقنيات الحماية و الوقاية على نظام مُحاكى لِمنع هجمات سيبرانية مُختلفة.

اليوم الرابع:

إدارة الأزمات السيبرانية و الاستجابة للحوادث

- مراحل إدارة الأزمات السيبرانية و خطوات الاستجابة)الكشف، الاحتواء، التحقيق، المعالجة، التعافي.(
- خطط الاستجابة للحوادث السيبرانية 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 و تطبيق خطة الاستجابة لِاحتواء الضرر و استعادة البيانات

اليوم الخامس:

التعاون و تبادل المعلومات و أفضل الممارسات

- أهمية التعاون و تبادل المعلومات بين المؤسسات الحكومية و الجهات الأمنية و القطاع الخاص لِمواجهة التهديدات السيبرانية.
- بناء الشراكات و فرق الاستجابة للحوادث (CERTs)و تبادل المعلومات عن التهديدات و الثغرات الأمنية.
- أفضل الممارسات في مجال الأمن السيبراني و حوكمة أمن المعلومات و التوعية بمخاطر الجرائم الإلكترونية.
- تطوير استراتيجية وطنية لِلأمن السيبراني و حماية البنية التحتية الحرجة و البيانات الحساسة.
- جلسة ختامية :مناقشة التحديات و الفرص المُستقبلية في مجال مكافحة الجرائم الإلكترونية و الهجمات السيبرانية.

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.