مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

استراتيجيات التكيف مع الهجمات السيبرانية المعقدة في القطاع العام

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 23 – 27 / 11 / 2025.

مقدمة :

مع تصاعد وتيرة الهجمات السيبرانية وتطور أساليب الاختراق، تواجه المؤسسات الحكومية تحديات متزايدة في حماية البنية التحتية الرقمية والبيانات الحساسة. تعتمد الهجمات السيبرانية المعقدة على استراتيجيات متقدمة، مثل الهجمات المستمرة المتقدمة (APT)، والهجمات متعددة المراحل التي تستهدف نقاط الضعف في الأنظمة الحكومية. لضمان حماية الأنظمة والبيانات، يتعين على القطاع العام تبني استراتيجيات فعالة للتكيف مع هذه الهجمات، بما يشمل رصد التهديدات بشكل استباقي، تعزيز الدفاعات الأمنية، وتحسين قدرات الاستجابة. يهدف هذا البرنامج التدريبي "استراتيجيات التكيف مع الهجمات السيبرانية المعقدة في القطاع العام" إلى تزويد المشاركين بالمعرفة والأدوات اللازمة لتطوير استراتيجيات مرنة وفعالة للتصدي لهذه التهديدات.

أهداف الورشة:

- فهم طبيعة الهجمات السيبرانية المعقدة وأساليب الهجوم الحديثة.
- إتقان مهارات تقييم المخاطر الأمنية وتحديد نقاط الضعف.
- تطوير استراتيجيات أمنية مرنة وقابلة للتطوير لمواجهة التهديدات المتغيرة.
- بناء قدرات المؤسسات الحكومية على التكيف والاستجابة السريعة للهجمات.
- تعزيز التعاون وتبادل المعلومات مع الجهات المعنية بالأمن السيبراني.
- تطوير خطط استمرارية الأعمال والتأهب للطوارئ.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي بين الموظفين.

محتويات الورشة:

اليوم التدريبي الأول:

التهديدات السيبرانية المتقدمة

- أنواع الهجمات السيبرانية المعقدة (مثل APT، هجمات الفدية، هجمات سلسلة التوريد، الهندسة الاجتماعية).
- أساليب وطرق الهجوم الحديثة (مثل هجمات zero-day، استغلال الثغرات الأمنية، الهجمات متعددة الأ vectors).
- أدوات وتقنيات المخترقين.
- ورشة عمل: تحليل حالة اختراق أمني متقدم وتحديد أساليب الهجوم المستخدمة.

اليوم التدريبي الثاني:

تقييم المخاطر الأمنية وبناء المرونة

- مفهوم تقييم المخاطر الأمنية وأهميته.
- منهجيات تقييم المخاطر (مثل NIST، ISO 27005).
- تحديد الأصول الحرجة وتقييم نقاط الضعف.
- بناء المرونة في الأنظمة والعمليات.
- ورشة عمل: تطبيق منهجية تقييم المخاطر على نظام حكومي وتحديد نقاط الضعف.

اليوم التدريبي الثالث:

استراتيجيات الأمن السيبراني التكيفية

- مبادئ الأمن السيبراني (السرية، التكامل، التوافر).
- تصميم وتنفيذ استراتيجيات أمنية مرنة وقابلة للتطوير.
- أمن الشبكات وأمن التطبيقات وأمن البيانات.
- أفضل الممارسات في الأمن السيبراني التكيفي.
- ورشة عمل: تطوير استراتيجية أمن سيبراني تكيفية لنظام حكومي.

اليوم التدريبي الرابع:

الاستجابة للحوادث والتعافي

- أهمية وجود خطة للاستجابة للحوادث الأمنية والتعافي منها.
- مراحل الاستجابة للحوادث (الكشف، الاحتواء، الاستئصال، التعافي).
- التحقيق الجنائي الرقمي.
- التعلم من الحوادث السابقة وتحسين خطط الاستجابة.
- ورشة عمل: تطوير خطة للاستجابة للحوادث الأمنية وتطبيقها على سيناريو واقعي.

اليوم التدريبي الخامس:

التعاون وتبادل المعلومات وبناء القدرات

- أهمية التعاون وتبادل المعلومات مع الجهات المعنية بالأمن السيبراني.
- بناء فرق استجابة للحوادث السيبرانية فعالة.
- التدريب والتطوير المستمر للكوادر الأمنية.
- بناء ثقافة الأمن السيبراني وتعزيز الوعي.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.

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.