مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الاستجابة السريعة للحوادث السيبرانية المتقدمة

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 9 – 13 / 3 / 2025.

مقدمة :

تعد الحوادث السيبرانية المتقدمة من أكبر التهديدات التي تواجه المؤسسات الحكومية والخاصة على حد سواء، نظرًا لتزايد تعقيد الهجمات الإلكترونية وتطور التقنيات المستخدمة فيها. إن الاستجابة السريعة والفعالة للحوادث السيبرانية تلعب دورًا حاسمًا في تقليل الأضرار وحماية البيانات الحساسة. يتطلب ذلك وجود فرق مدربة قادرة على اكتشاف الهجمات بسرعة، تحديد نقاط الضعف، وتنفيذ استراتيجيات فعّالة للتعافي. يهدف برنامج "الاستجابة السريعة للحوادث السيبرانية المتقدمة" إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لإدارة الاستجابة الفعالة للحوادث السيبرانية المعقدة، مع التركيز على أفضل الممارسات العالمية في هذا المجال.

أهداف الورشة:

- فهم طبيعة التهديدات السيبرانية المتقدمة وأساليب الهجوم الحديثة.
- إتقان مهارات الكشف عن الحوادث السيبرانية وتحليلها باستخدام أدوات متقدمة.
- تطوير القدرة على اتخاذ قرارات سريعة وفعالة في ظل ضغوط الأزمات الأمنية.
- تنفيذ استراتيجيات احتواء وعزل الهجمات ومنع انتشارها.
- استعادة الأنظمة والبيانات المتضررة بأسرع وقت ممكن.
- تحليل الأحداث الأمنية واستخلاص الدروس المستفادة لتطوير خطط الوقاية.
- بناء فرق استجابة للحوادث السيبرانية فعالة وقادرة على التعامل مع التهديدات المتطورة.

محتويات الورشة:

اليوم التدريبي الأول:

التهديدات السيبرانية المتقدمة

- أنواع الهجمات السيبرانية المتقدمة (APT، هجمات الفدية، هجمات سلسلة التوريد، الهندسة الاجتماعية).
- أساليب وطرق الهجوم الحديثة.
- أدوات وتقنيات المخترقين.
- ورشة عمل: تحليل حالة اختراق أمني متقدم وتحديد أساليب الهجوم المستخدمة.

اليوم التدريبي الثاني:

الكشف عن الحوادث وتحليلها

- أهمية الكشف المبكر عن الحوادث السيبرانية.
- أدوات وتقنيات الكشف عن التهديدات (SIEM، EDR، NDR).
- تحليل السجلات والبيانات للكشف عن الأنشطة المشبوهة.
- التحقيق الجنائي الرقمي (Digital Forensics).
- ورشة عمل: استخدام أدوات التحليل الجنائي الرقمي لتحليل حادثة أمنية.

اليوم التدريبي الثالث:

الاحتواء والاستجابة

- استراتيجيات احتواء وعزل الهجمات ومنع انتشارها.
- إدارة الأزمات الأمنية واتخاذ القرارات السريعة.
- التواصل الفعال مع أصحاب المصلحة خلال الأزمة.
- توثيق الحادثة وتقديم التقارير.
- ورشة عمل: تطوير خطة استجابة لحادثة أمنية وتطبيقها على سيناريو واقعي.

اليوم التدريبي الرابع:

التعافي من الحوادث

- أهمية استعادة الأنظمة والبيانات المتضررة بأسرع وقت ممكن.
- تقنيات استعادة البيانات والأنظمة.
- التحقق من سلامة الأنظمة بعد الاستعادة.
- تقييم فعالية خطة الاستجابة وتحديد مجالات التحسين.
- ورشة عمل: تطوير خطة للتعافي من الكوارث وتطبيقها على سيناريو واقعي.

اليوم التدريبي الخامس:

بناء فرق الاستجابة والتطوير المستمر

- أهمية بناء فرق استجابة للحوادث السيبرانية فعالة.
- مهارات وقدرات أعضاء فريق الاستجابة.
- التدريب والتطوير المستمر لأعضاء الفريق.
- التعاون مع جهات خارجية (مثل CERTs) في الاستجابة للحوادث.
- 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.